Страновой отчет: политические инициативы и законы Китая, касающиеся интернета

Вени Марковски (Veni Markovski) и
Алексей Трепыхалин (Alexey Trepykhalin)
31 января 2022
GE-010 (обновленная редакция)

СОДЕРЖАНИЕ

Введение

В настоящем документе охвачены политические инициативы и законодательные/нормативные акты, касающиеся интернета, выдвинутые в Китае за период с 16 декабря 2015 года по 5 ноября 2021 года. Это гарантирует наличие у сообщества ICANN необходимой информации для лучшего понимания обсуждений, которые ведутся в ООН, МСЭ и других учреждениях ООН.

Этот документ входит в состав серии регулярных отчетов по конкретным странам, содержащих обзор деятельности, относящейся к экосистеме интернета и миссии ICANN. Мониторинг таких инициатив — одна из основных обязанностей отдела корпорации ICANN по взаимодействию с правительствами и межправительственными организациями (GE), чтобы держать все сообщество ICANN в курсе вопросов, имеющих важное значение для глобального единого функционально совместимого интернета и его системы уникальных идентификаторов[1].

Как и предыдущие документы GE, настоящий отчет составлен на основе текстов первоисточников, касающихся политики и технологий интернета, в том числе таких, как система доменных имен (DNS), адреса интернет-протокола (IP) и параметры протокола. Кроме того, данный документ опирается на соответствующие тексты, заявления и нормативно-правовые положения, определяющие позицию Китая по тем же вопросам в Организации Объединенных Наций (ООН), Международном союзе электросвязи (МСЭ) и на внутригосударственном уровне.

Внешнеполитические заявления и инициативы Китая

16 декабря 2015 года в своем выступлении на церемонии открытия второй Всемирной конференции по вопросам интернета в Учжэне[2], президент Китайской Народной Республики, Си Цзиньпин, сказал: «...международное сообщество должно укреплять диалог и сотрудничество на основе взаимного уважения и доверия, содействовать преобразованию глобальной системы управления интернетом и совместно работать над развитием мирного, безопасного, открытого и коллективного киберпространства и созданием многосторонней, демократической и прозрачной глобальной системы управления интернетом»[3].

Президент Си заявил, что для достижения этой цели «уважение к киберсуверенитету» отдельных стран и участие в «международном управлении киберпространством на

[1] «План операционной деятельности и финансовый план ICANN», стр. 47, корпорация ICANN, декабрь 2020 года, https://www.icann.org/en/system/files/files/draft-op-financial-plan-fy21-25-opplan-fy21-20dec19-en.pdf.

[2] Всемирная конференция по вопросам интернета ежегодно проводится в городе Учжэнь, провинция Чжэцзян, Управлением по вопросам киберпространства Китая и народным правительством провинции Чжэцзян http://www.wuzhenwic.org/2020-10/15/c_547699.htm. Настоящий документ переведен на несколько языков исключительно в информационных целях. Оригинальный текст (на китайском языке) доступен здесь: https://www.wicwuzhen.cn/.

[3] Комментарии Е.П. Си Цзиньпина, президента Китайской Народной Республики, на церемонии открытия второй Всемирной конференции по вопросам интернета, Учжэнь, 16 декабря 2015 года https://www.fmprc.gov.cn/eng/wjdt_665385/zyjh_665391/201512/t20151224_678467.html.

равной основе» должны стать одним из четырех основополагающих принципов[4]. Президент Си также добавил: «Для международного управления киберпространством следует использовать многосторонний подход с многосторонним участием. Он должен опираться на консультации между всеми сторонами при эффективном использовании функций различных участников, в том числе правительств, международных организаций, интернет-компаний, технических сообществ, неправительственных организаций и отдельных граждан. Односторонний подход недопустим. Решения не должны приниматься единственной стороной в приказном порядке или в результате обсуждения несколькими сторонами в узком кругу. Все страны должны активизировать связи и обмен, улучшить механизм диалога и консультаций по вопросам киберпространства, а также изучить и сформулировать глобальные правила управления интернетом, чтобы глобальная система управления интернетом стала более справедливой и рациональной, более сбалансированным способом отражала стремления и интересы большинства стран»[5].

7 марта 2016 года на заседании Правительственного консультативного комитета (GAC) ICANN представитель Китая подчеркнул, что «четыре принципа и пять предложений», выдвинутых президентом Си в 2016 году на второй Всемирной конференции по вопросам интернета в Учжэне, «дают нам (неразборчиво) представление о суждениях и позициях Китая по вопросу управления интернетом»[6].

27 апреля 2016 года Китай опубликовал Национальную стратегию кибербезопасности[7], поясняющую важность «укрепления международного сотрудничества в киберпространстве» для страны. В связи с этим в стратегии конкретизируется, что такое сотрудничество должно «способствовать реформированию глобальной системы управления интернетом» и «интернационализации управления интернет-адресами, серверами доменных имен и другими аналогичными основными ресурсами». В стратегии также была выражена поддержка того, чтобы «Организация Объединенных Наций играла ведущую роль, содействовала разработке международных общепризнанных норм для киберпространства, а также международного договора о борьбе с терроризмом в киберпространстве, созданию механизмов правовой помощи для борьбы с киберпреступностью, углублению международного сотрудничества в таких областях, как политика и законодательство, технологические инновации, стандарты и нормы, реагирование на чрезвычайные ситуации, защита критической информационной инфраструктуры и т. д». Кроме того, в ней содержался призыв «создать многостороннюю, демократическую и прозрачную систему международного управления интернетом».

[4] Комментарии Е.П. Си Цзиньпина.
[5] Комментарии Е.П. Си Цзиньпина.
[6] МАРРАКЕШ — Правительственное совещание GAC на высоком уровне, 7 марта 2016 года, ICANN55 | Марракеш, Марокко, стр. 86 https://gac.icann.org/transcripts/public/transcript-icann55-gac-hl-governmental-meeting-2016-03-07.pdf.
[7] China Copyright and Media, Национальная стратегия безопасности в киберпространстве, обновленная редакция от 27 декабря 2016 года, https://chinacopyrightandmedia.wordpress.com/2016/12/27/national-cyberspace-security-strategy/. Настоящий документ переведен на несколько языков исключительно в информационных целях. Оригинальный текст (на китайском языке) доступен здесь: http://www.cac.gov.cn/2016-12/27/c_1120195926.htm.

2 марта 2017 года Китай опубликовал Международную стратегию сотрудничества в киберпространстве[8]. В ней говорится, что «Китай будет предпринимать активные усилия для реформирования организационной структуры Форума по управлению интернетом ООН, чтобы дать ему возможность играть более заметную роль в управлении интернетом, укрепить его способность принятия решений, обеспечить надежное финансирование и ввести открытые и прозрачные процедуры избрания его членов и представления отчетов». Международная стратегия сотрудничества в киберпространстве также гласит, что Китай «будет участвовать в международных дискуссиях по вопросу о справедливом распределении и управлении критическими интернет-ресурсами» и «будет энергично содействовать реформированию ICANN, чтобы сделать ее по-настоящему независимой международной организацией, расширить ее представленность и повысить открытость и прозрачность принятия решений и ведения деятельности»[9].

20 апреля 2018 года на Национальной рабочей конференции по кибербезопасности и информатизации в Пекине президент Си сказал, что «реформирование глобальной системы управления интернетом станет в дальнейшем общей тенденцией и общим стремлением». Он добавил: «Следует упорно стремиться к управлению киберпространством на многосторонней основе при участии многих заинтересованных сторон, давая возможность выполнять свои функции всем видам субъектов, включая правительства, международные организации, интернет-предприятия, техническое сообщество, гражданские организации и отдельных граждан. Мы также должны одновременно продвигать управление киберпространством в рамках ООН и добиться лучших результатов в плане предоставления возможности играть позитивную роль самым разным негосударственным субъектам»[10].

9 июля 2019 года в материалах, отправленных Рабочей группе открытого состава (РГОС) по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности, Китай отметил: «Страны должны общими силами построить многостороннюю демократическую и прозрачную глобальную систему управления интернетом. Организация, которой поручено управление критическими ресурсами, такими как корневые серверы, должна быть реально независима от любого государства для обеспечения широкого участия и совместного принятия решений всеми странами»[11].

В апреле 2020 года Китай направил следующее предложение относительно предварительного проекта отчета РГОС ООН, в котором заявил: «Ввиду того, что мы ограничены во времени, следует также постараться избежать включения в отчет понятий,

---

[8] Международная стратегия сотрудничества в киберпространстве, China Daily, 2 марта 2017 года, https://www.chinadaily.com.cn/kindle/2017-03/02/content_28409210.htm. Настоящий документ переведен на несколько языков исключительно в информационных целях. Оригинальный текст (на китайском языке) доступен здесь: http://www.china.org.cn/chinese/2017-03/07/content_40424606.htm.

[9] Международная стратегия сотрудничества в киберпространстве, China Daily, 2 марта 2017 года.

[10] New America, перевод: Речь Си Цзиньпина 20 апреля на Национальной рабочей конференции по кибербезопасности и информатизации, 30 апреля 2018 года, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-xi-jinpings-april-20-speech-national-cybersecurity-and-informatization-work-conference/. Настоящий документ переведен на несколько языков исключительно в информационных целях. Оригинальный текст (на китайском языке) доступен здесь: http://www.xinhuanet.com/politics/2018-04/21/c_1122719810.htm.

[11] Материалы, отправленные Китаем Рабочей группе открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности, 7 июля 2019 года, https://s3.amazonaws.com/unoda-web/wp-content/uploads/2019/09/china-submissions-oewg-en.pdf.

относительно которых еще не достигнут глобальный консенсус (таких как «публичное ядро»)», а также: «На предыдущих двух сессиях стороны, в том числе Китай, выдвинули десятки конструктивных предложений по таким вопросам, как киберсуверенитет, безопасность цепочки поставок, защита критически важной инфраструктуры, отказ от односторонних санкций и борьба с кибертерроризмом. Надеемся, что эти предложения могут быть включены в отчет»[12].

8 сентября 2020 года Министерство иностранных дел Китая опубликовало Глобальную инициативу по защите данных, в которой рассмотрело необходимость улучшения межгосударственного сотрудничества в области защиты данных, борьбы с киберпреступностью и т. д. В этом документе предлагается, чтобы «правительства, международные организации, компании отрасли ИКТ[13], технические сообщества, гражданские организации, физические лица и все остальные субъекты приложили согласованные усилия для обеспечения защиты данных в соответствии с принципом широких консультаций, совместного вклада и общей пользы». Документ призывает государства, помимо прочего: «обеспечивать защиту данных на комплексной, объективной и доказательной основе, а также поддерживать открытую, безопасную и стабильную цепочку поставок глобальных продуктов и услуг ИКТ»[14].

В марте 2021 года на ежегодной конференции законодательного органа «Две сессии» был принят 14-й пятилетний план и долгосрочные цели до 2035 года. В главе 18 этого документа («Создание хорошей цифровой экосистемы») раздел 4 («Содействовать формированию сообщества с общим будущим в киберпространстве) гласит: «Развивать международный обмен и сотрудничество в киберпространстве и содействовать выработке международных правил для цифрового пространства и киберпространства в рамках Организации Объединенных Наций как основного канала и Устава ООН как основных принципов. Содействовать созданию многосторонней, демократической и прозрачной глобальной системы управления интернетом и созданию более справедливой и рациональной сетевой инфраструктуры и механизма управления ресурсами»[15].

---

[12] Предложение Китая относительно предварительного проекта отчета РГОС, 16 апреля 2020 года (датировано на основании свойств PDF-файла), https://front.un-arm.org/wp-content/uploads/2020/04/china-contribution-to-oewg-pre-draft-report-final.pdf .

[13] ИКТ — информационные и коммуникационные технологии, UNTERM — терминологическая база данных ООН, https://unterm.un.org/unterm/display/record/imo/na?OriginalId=551772be82184a22adaeb86841e335e6.

[14] Глобальная инициатива по защите данных, сайт Министерства иностранных дел Китая, 8 сентября 2020 года, https://www.fmprc.gov.cn/mfa_eng/wjb_663304/zzjg_663340/jks_665232/kjfywj_665252/202009/t20200908_599773.htmlhttps://www.fmprc.gov.cn/mfa_eng/wjb_663304/zzjg_663340/jks_665232/kjfywj_665252/202009/t20200908_599773.html и статья «Китай запускает глобальную инициативу по защите данных в ответ на политизацию вопросов защиты данных», Reuters, 7 сентября 2020 года, https://www.reuters.com/article/wangyi-global-digital-security-0908-idCNKBS25Z0AJ. Настоящий документ переведен на несколько языков исключительно в информационных целях. Оригинальный текст (на китайском языке) доступен здесь: https://www.fmprc.gov.cn/chn/pds/ziliao/tytj/t1827469.htm.

[15] Guancha, «14-й пятилетний план» и описание долгосрочных целей до 2035 года (полный текст), 13 марта 2021 года, https://www.guancha.cn/politics/2021_03_13_583945_5.shtml.

10 марта 2021 года Китай на заседании РГОС в ООН заявил: «Государства должны участвовать в управлении и распределении международных интернет-ресурсов на равной основе»[16].

29 июня 2021 года Китай и Российская Федерация сделали совместное заявление, продлив действие двустороннего Договора о добрососедстве, дружбе и сотрудничестве. В совместном заявлении они согласились «подтвердить свою приверженность укреплению международной информационной безопасности как на двустороннем, так и на многостороннем уровне» и подчеркнули «свое единство по вопросам, связанным с управлением интернетом, которое охватывает обеспечение равноправного участия всех государств в глобальном управлении сетью, повышение их роли в этом процессе и сохранение суверенного права государств регулировать национальный сегмент интернета. Россия и Китай подчеркивают необходимость повышения роли Международного союза электросвязи и расширения представленности двух стран в его руководящих органах»[17].

1 ноября 2021 года Российская Федерация представила свой проект текста[18] предлагаемой Конвенции ООН о борьбе с киберпреступностью и объявила, что этот текст подготовлен совместно с Китаем[19,20].

5 ноября 2021 года Китай внес свои предложения на первом заседании Специального комитета (АНС)[21]. Помимо прочего, он заявил: «Государствам-членам предлагается ввести уголовную ответственность за взлом и разрушение объектов, систем, данных или критической информационной инфраструктуры ИКТ. Это может включать несанкционированный доступ к компьютерным информационным системам, незаконное вмешательство в работу компьютерных информационных систем, незаконное приобретение компьютерных данных, незаконное посягательство на компьютерные данные, нарушение критической информационной инфраструктуры и тому подобное».

---

[16] Рабочая группа открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности, третья основная сессия, 8–12 марта 2021 года, Резюме председателя РГОС, рабочий документ заседания, 10 марта 2021 года, A/AC.290/2021/CRP.3*, https://front.un-arm.org/wp-content/uploads/2021/03/Chairs-Summary-A-AC.290-2021-CRP.3-technical-reissue.pdf.

[17] Посольство Российской Федерации в Соединенном Королевстве Северной Ирландии и Великобритании, совместное заявление Российской Федерации и Китайской Народной Республики по случаю двадцатой годовщины существования Договора о добрососедстве, дружбе и сотрудничестве между Российской Федерацией и Китайской Народной Республикой, 28 июня 2021 года, https://www.rusemb.org.uk/fnapr/7007. Настоящий документ переведен на несколько языков исключительно в информационных целях. Оригинальный текст (на китайском языке) доступен здесь: http://www.xinhuanet.com/2021-06/28/c_1127606620.htm.

[18] Конвенция ООН о противодействии использованию информационных и коммуникационных технологий в преступных целях, 27 июля 2021 года, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Comments/RF_28_July_2021_-_E.pdf .

[19] Статья «Скоро начнется создание новой конвенции ООН о борьбе с киберпреступностью», fm4.orf.at, https://fm4.orf.at/stories/3019118/ .

[20] Константинос Комаитис (Konstantinos Komaitis), Twitter-аккаунт, 1 ноября 2021 года и 19 января 2022 года, https://twitter.com/i/web/status/1455217317504327683.

[21] Предложения Китая по вопросу рамок, целей и структуры (элементов) Конвенции ООН о противодействии использованию ИКТ в преступных целях: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/Comments/Chinas_Suggestions_on_the_Scope_Objectives_and_Structure_AHC_ENG.pdf.

Внутригосударственные заявления, законодательные и нормативные акты

1 июля 2015 года был принят Закон о национальной безопасности. Он гласит (ст. 59): «Государство создает системы и механизмы управления для проверки и контроля национальной безопасности, проводит проверку национальной безопасности в отношении иностранных коммерческих инвестиций, специальных товаров и технологий, продуктов и услуг информационных технологий интернета, проектов, затрагивающих вопросы национальной безопасности, а также в отношении других важных вопросов и видов деятельности, которые оказывают или могут оказать влияние на национальную безопасность»[22]. Статья 25 этого закона гласит: «Государство создает национальную систему защиты сетевой и информационной безопасности, [...] расширяет управление сетями, защищает суверенитет, безопасность и интересы в области развития киберпространства».
1 июня 2017 года вступил в силу Закон о кибербезопасности (CSL). Согласно этому закону государство отвечает за «содействие формированию мирного, безопасного, открытого и коллективного киберпространства и создание многосторонней, демократической и прозрачной системы управления интернетом». В законе также есть положение о хранении интернет-данных внутри страны «на материковой части Китая». Статья 31 закона определяет рамки критической информационной инфраструктуры, которые охватывают «многоуровневую систему защиты связи общего пользования и информационных услуг, энергетики, транспорта, водных ресурсов, финансов, общественных служб, электронного правительства и другой критической информационной инфраструктуры». Статья 37 закона гласит: «когда из-за коммерческих требований действительно необходимо передать их [личную информацию и важные данные] за пределы материковой части, они [операторы критической информационной инфраструктуры] должны принять меры по оценке безопасности, сформулированные совместно государственными ведомствами по вопросам кибербезопасности и информатизации и компетентными ведомствами Государственного совета; если законами и административными нормами предусмотрено иное, требуется соблюдать указанные положения»[23]. (Соответствующие положения приведены в Приложении 1 к настоящему документу.)

24 августа 2017 года Министерство промышленности и информационных технологий Китая (MIIT) опубликовало пересмотренные Меры по управлению доменными именами в интернете. [24] (Соответствующие положения приведены в Приложении 2 к настоящему документу.)

---

[22]China Law Translate, Закон Китайской Народной Республики о национальной безопасности, 1 июля 2015 года, https://www.chinalawtranslate.com/en/2015nsl/. Настоящий документ переведен на несколько языков исключительно в информационных целях. Оригинальный текст (на китайском языке) доступен здесь: http://www.gov.cn/zhengce/2015-07/01/content_2893902.htm.
[23] New America, перевод: Закон Китайской Народной Республики о кибербезопасности (вступил в силу 1 июня 2017 года), 29 июня 2018 года, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/. Настоящий документ переведен на несколько языков исключительно в информационных целях. Оригинальный текст (на китайском языке) доступен здесь: http://www.cac.gov.cn/2016-11/07/c_1119867116.htm.
[24] Министерство промышленности и информационных технологий, Меры по управлению доменными именами в интернете, 24 августа 2017 года https://www.chinalawtranslate.com/en/internet-domain-name-management-measures/. Настоящий

29 января 2018 MIIT объявило о том, что на основании статьи 5 вышеупомянутых новых мер оно внесло изменения в систему доменных имен китайского сегмента интернета[25]. (Соответствующие положения приведены в Приложении 3 к настоящему документу.)

13 июня 2019 года в статье 2 документа «Меры по оценке безопасности трансграничной передачи личной информации» было предложено: «Сетевые операторы, которые предоставляют личную информацию, собранную в процессе деятельности на материковой части Китайской Народной Республики (в дальнейшем это именуется отправкой личной информации), должны выполнять оценку безопасности в соответствии с настоящими Мерами. Если в результате оценки безопасности будет установлено, что отправка личной информации может повлиять на национальную безопасность или нанести вред общественным интересам или что сложно обеспечить эффективную защиту личной информации, такая информация не должна покидать территорию страны. В случаях, когда у государства есть другие положения об отправке личной информации, применяются указанные положения»[26].
10 июня 2021 года, на 29-й сессии Постоянного комитета Всекитайского собрания народных представителей 13-го созыва был принят Закон о защите данных (DSL)[27]. (См. соответствующие тексты в Приложении 4 к настоящему документу.)

30 июля 2021 года были опубликованы новые Нормы обеспечения безопасности критической информационной инфраструктуры (после их принятия Государственным советом Китая 27 апреля 2021 года). Эти нормы определяют рамки критической информационной инфраструктуры, содержат положения об «отраслях и секторах» для дополнительной детализации этих рамок и определяют требования к отчетности этих организаций перед центральными органами власти в киберпространстве в случае «особенно серьезных инцидентов кибербезопасности», таких как «относительно широкомасштабная»

документ переведен на несколько языков исключительно в информационных целях. Оригинальный текст (на китайском языке) доступен здесь: http://www.cac.gov.cn/2017-09/28/c_1121737753.htm.

[25] По состоянию на 19 августа 2021 года URL китайского ресурса не работает, на английском языке: https://www.chinalawtranslate.com/en/chinese-internet-domain-name-system/. Настоящий документ переведен на несколько языков исключительно в информационных целях. Оригинальный текст (на китайском языке) доступен здесь: http://xn--eqrt2g.xn--vuq861b/#.

[26] New America, перевод: Новый проект правил трансграничной передачи личной информации за пределы Китая, 13 июня 2019 года, «Меры по оценке безопасности отправки личной информации (проект для обсуждения)», 13 июня 2019 года, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-new-draft-rules-cross-border-transfer-personal-information-out-china/. Настоящий документ переведен на несколько языков исключительно в информационных целях. Оригинальный текст (на китайском языке) доступен здесь: http://www.cac.gov.cn/2019-06/13/c_1124613618.htm.

[27] Inside Privacy, неофициальный перевод Covington: Меры по оценке безопасности трансграничной передачи личной информации (проект для обсуждения)», 13 июня 2019 года, https://www.insideprivacy.com/wp-content/uploads/sites/51/2019/06/Measures-for-Security-Assessment-of-the-Cross-Border-Transfer-of-Personal-Information_bilingual.pdf, и New America, перевод: Новый проект правил трансграничной передачи личной информации за пределы Китая «Меры по оценке безопасности отправки личной информации (проект для обсуждения)», июнь 2019 года https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-new-draft-rules-cross-border-transfer-personal-information-out-china/. Настоящий документ переведен на несколько языков исключительно в информационных целях. Оригинальный текст (на китайском языке) доступен здесь: http://www.cac.gov.cn/2019-06/13/c_1124613618.htm.

утечка личной информации[28]. Нормы вступили в силу 1 сентября 2021 года. (Соответствующие статьи норм приведены в Приложении 6 к настоящему документу.)

20 августа 2021 года Постоянный комитет Всекитайского собрания народных представителей КНР принял Закон о защите личной информации (PIPL). Этот закон вступил в силу 1 ноября 2021 года. Закон «разработан [...] с целью защиты прав и интересов владельцев личной информации, стандартизации деятельности по обработке личной информации и содействия рациональному использованию личной информации». Личная информация «физических лиц пользуется правовой защитой; всем юридическим и физическим лицам запрещено нарушать права и интересы физических лиц в отношении личной информации». Этот закон «распространяется на организации и физических лиц, обрабатывающих личную информацию физических лиц на территории Китайской Народной Республики». «Если при обработке за границей Китайской Народной Республики личной информации физических лиц, находящихся на территории Китайской Народной Республики, имеет место одно из следующих обстоятельств, этот закон также применяется» (1) «когда цель состоит в предоставлении продуктов или услуг физическим лицам на территории страны»; (2) «при анализе или оценке деятельности физических лиц на территории страны»; (3) «в других обстоятельствах, предусмотренных в законах или административных нормах». Закон также содержит определение личной информации и того, что считается ее обработкой: «Личная информация — это все виды информации, записанной с помощью электронных или других средств, которая имеет отношение к идентифицированным или идентифицируемым физическим лицам, исключая информацию после анонимизации. Обработка личной информации включает сбор, хранение, использование, обработку, передачу, предоставление, публикацию, удаление личной информации и тому подобное»[29]. (Полный текст закона приведен в Приложении 5 к настоящему документу).

Заключение

Китай активно участвует во всех важных дискуссиях в ООН, касающихся киберпространства. Международный и национальный вклад Китая может затронуть миссию ICANN. Корпорация ICANN через отдел по взаимодействию с правительствами продолжит предоставление информации сообществу ICANN, когда такие заявления или предложения будут иметь отношение к техническому управлению интернетом или миссии ICANN.

[28] Постановление Государственного совета Китайской Народной Республики № 745, 30 июля 2021 года, http://www.gov.cn/zhengce/content/2021-08/17/content_5631671.htm?trs=1, в переводе DigiChina: https://digichina.stanford.edu/news/translation-critical-information-infrastructure-security-protection-regulations-effective-sept.

[29] Закон Китайской Народной Республики о защите личной информации, (принят 20 августа 2021 года на 30-й сессии Постоянного комитета Всекитайского собрания народных представителей 13-го созыва), http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml

Приложение 1
Закон Китайской Народной Республики о кибербезопасности[30]

Принято 6 ноября 2016 года. Вступает в силу 1 июня 2017 года.

1. Содержание

Глава I. Общие положения

Статья 1. Настоящий закон разработан в целях обеспечения кибербезопасности; защиты суверенитета и национальной безопасности, социальных и общественных интересов в киберпространстве; защиты законных прав и интересов граждан, юридических лиц и других организаций; содействия полноценному развитию информатизации экономики и общества.

Статья 2. Настоящий закон применим к созданию, эксплуатации, техническому обслуживанию и использованию сетей, а также к надзору и управлению в области кибербезопасности на материковой части Китайской Народной Республики.

Статья 3. Государство стремится в равной степени уделять особое внимание развитию кибербезопасности и информатизации и соблюдать принципы активного применения, научного развития, управления в соответствии с законом и обеспечения безопасности. Государство способствует строительству сетевой инфраструктуры и связности, поощряет инновации и применение сетевых технологий, поддерживает подготовку квалифицированных кадров в области кибербезопасности, создает целостную систему для сохранения кибербезопасности и наращивает возможности защиты кибербезопасности.

Статья 4. Государство определяет и постоянно совершенствует стратегию кибербезопасности, разъясняет фундаментальные требования и главные цели обеспечения кибербезопасности и предлагает политику, рабочие задачи и процедуры обеспечения кибербезопасности для ключевых секторов.

Статья 5. Государство принимает меры для мониторинга, предотвращения и снижения рисков и угроз кибербезопасности, возникающих как на материковой части территории Китайской Народной Республики, так и за ее пределами. Государство защищает критическую информационную инфраструктуру от атак, вторжений, вмешательства и уничтожения; государство в предусмотренном законом порядке наказывает за противоправную и преступную деятельность в киберпространстве, сохраняя безопасность и порядок в киберпространстве.

[30] New America, перевод: Закон Китайской Народной Республики о кибербезопасности (вступил в силу 1 июня 2017 года), 29 июня 2018 года, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/. Настоящий документ переведен на несколько языков исключительно в информационных целях. Оригинальный текст (на китайском языке) доступен здесь: http://www.cac.gov.cn/2016-11/07/c_1119867116.htm.

Статья 6. Государство поощряет искреннее, добросовестное, полезное и цивилизованное поведение в сети; оно способствует распространению основных социалистических ценностей, принимает меры по повышению осведомленности всего общества и уровня кибербезопасности и формирует благоприятную среду для совместного участия всего общества в укреплении кибербезопасности.
Статья 7. Государство активно ведет международный обмен и сотрудничество в области управления киберпространством, исследования и разработки сетевых технологий, подготовки стандартов, борьбы с киберпреступностью и противозаконной деятельностью, а также в других аналогичных областях; оно способствует построению мирного, безопасного, открытого и коллективного киберпространства и созданию многосторонней, демократической и прозрачной системы управления интернетом.
Статья 8. Государственные ведомства по кибербезопасности и информатизации отвечают за всестороннее планирование и координацию деятельности по обеспечению кибербезопасности и соответствующей деятельности по надзору и управлению. Ведомства Государственного совета по телекоммуникациям, государственной безопасности и другие компетентные органы отвечают за деятельность по защите кибербезопасности, надзору и управлению в рамках своих обязанностей в соответствии с положениями настоящего закона и соответствующих законов и административных норм. Обязанности по защите кибербезопасности, надзору и управлению компетентных ведомств народных правительств на уровне уездов и выше определяются соответствующими национальными нормами.
Статья 9. Сетевые операторы, которые ведут предпринимательскую деятельность и предоставляют услуги, должны соблюдать законы и административные нормы, уважать общественную мораль, соблюдать коммерческую этику, быть честными и заслуживающими доверия, выполнять обязательства по защите кибербезопасности, соглашаться на надзор со стороны правительства и общественности и нести социальную ответственность.
Статья 10. Создание и эксплуатацию сетей или предоставление услуг через сети необходимо осуществлять: в соответствии с положениями законов и административных норм, а также обязательными требованиями национальных стандартов; принимая технические и другие необходимые меры по защите кибербезопасности и стабильности работы; эффективно реагируя на инциденты кибербезопасности; предотвращая киберпреступления и незаконную деятельность; сохраняя целостность, конфиденциальность и удобство использования данных в сети.
Статья 11. Соответствующие организации интернет-отрасли, согласно своим учредительным договорам, должны укреплять отраслевую самодисциплину, устанавливать нормы поведения в сфере кибербезопасности, направлять своих членов в деле укрепления защиты кибербезопасности в соответствии с законом, повышать уровень защиты кибербезопасности и стимулировать полноценное развитие отрасли.
Статья 12. Государство защищает права граждан, юридических лиц и других организаций на использование сетей в соответствии с законодательством; оно содействует широкому доступу к сети, повышает уровень сетевых услуг, предоставляет безопасные и удобные сетевые услуги обществу и гарантирует законное, упорядоченное и свободное перемещение информации в сети.
Все люди и организации, использующие сети, должны соблюдать Конституцию и законы, поддерживать общественный порядок и уважать общественную мораль; они не должны ставить под угрозу кибербезопасность и не должны использовать интернет для ведения деятельности, угрожающей национальной безопасности, национальной чести и национальным интересам; они не должны подстрекать к подрыву национального суверенитета, ниспровергать социалистическую систему, разжигать сепаратизм, разрушать национальное единство, поддерживать терроризм или экстремизм,

пропагандировать ненависть и дискриминацию на этнической почве, распространять информацию, пропагандирующую насилие и жестокость, информацию порнографического или сексуального характера, создавать или распространять ложную информацию для нарушения экономического или общественного порядка или информацию, которая наносит ущерб репутации, конфиденциальности, интеллектуальной собственности или нарушает остальные законные права и интересы других лиц, а также другие аналогичные нормативные акты.

Статья 13. Государство поощряет исследование и разработку сетевых продуктов и услуг, способствующих здоровому воспитанию несовершеннолетних; государство в предусмотренном законом порядке наказывает за использование сетей для ведения деятельности, которая угрожает психическому и физическому благополучию несовершеннолетних; государство создает для несовершеннолетних безопасную и здоровую сетевую среду.

Статья 14. Все люди и организации имеют право сообщать о поведении, угрожающем кибербезопасности, ведомствам, отвечающим за кибербезопасность и информатизацию, телекоммуникации, государственную безопасность и другим ведомствам. Ведомства, получающие такие сообщения, должны незамедлительно обрабатывать их в соответствии с законом; если эти вопросы не входят в сферу компетенции данного ведомства, сообщения должны незамедлительно передаваться ведомству, которое уполномочено их рассматривать. Соответствующие ведомства должны сохранять конфиденциальность информации, поступившей от осведомителей, и защищать законные права и интересы осведомителей.

Глава II. Обеспечение и стимулирование кибербезопасности

Статья 15. Государство создает и совершенствует систему стандартов обеспечения кибербезопасности. Административные ведомства Государственного совета по стандартизации и другие компетентные ведомства Государственного совета в рамках своих индивидуальных обязанностей должны организовать выработку и своевременный пересмотр соответствующих национальных и отраслевых стандартов для управления кибербезопасностью, а также безопасностью сетевых продуктов, услуг и операций. Государство поддерживает участие предприятий, научно-исследовательских организаций, высших учебных заведений и отраслевых организаций, имеющих отношение к сети, в разработке национальных и отраслевых стандартов в области кибербезопасности.

Статья 16. Государственный совет и народные правительства провинций, автономных районов и городов центрального подчинения обязаны: заниматься комплексным планированием; наращивать объем инвестиций; поддерживать ключевые отрасли и программы, связанные с технологиями обеспечения кибербезопасности; поддерживать исследование и разработку технологий обеспечения кибербезопасности, их применение и популяризацию; продвигать надежные и заслуживающие доверия сетевые продукты и услуги; защищать права на интеллектуальную собственность в области сетевых технологий; поддерживать участие научно-исследовательских институтов и организаций, занимающихся вопросами развития, высших учебных заведений и т. д. в государственных программах инновационного развития технологий обеспечения кибербезопасности.

Статья 17. Государство способствует созданию общественных систем обслуживания для кибербезопасности, поощряя выполнение соответствующими предприятиями и организациями сертификации, тестирования, оценки рисков для кибербезопасности и оказание других аналогичных услуг в области безопасности.

Статья 18. Государство поощряет разработку технологий сетевой защиты и использования данных, поощряя предоставление открытого доступа к ресурсам

с данными общего пользования и содействуя техническим инновациям и экономическому и социальному развитию.
Государство поддерживает инновационные методы управления кибербезопасностью, используя новые сетевые технологии для повышения уровня защиты кибербезопасности.
Статья 19. Народные правительства всех уровней и их соответствующие ведомства должны регулярно вести пропаганду и обучение в области кибербезопасности, а также направлять и стимулировать надлежащее ведение пропагандистской и учебной работы в области кибербезопасности соответствующими подразделениями.
Средства массовой информации должны вести среди общественности целенаправленную пропаганду и обучение в области кибербезопасности.
Статья 20. Государство поддерживает проведение предприятиями и учебными заведениями, такими как высшие учебные заведения и профессиональные училища, теоретического и практического обучения по кибербезопасности, и использует множество методов для подготовки квалифицированных кадров в области кибербезопасности и поощрения взаимодействия между специалистами по кибербезопасности.

Глава III. Безопасность сетевых операций

Раздел 1. Общие положения

Статья 21. Государство вводит в действие многоуровневую систему защиты кибербезопасности [MLPS]. Сетевые операторы должны выполнять следующие обязанности по обеспечению безопасности в соответствии с требованиями этой многоуровневой системы защиты кибербезопасности, чтобы обеспечить в сети отсутствие вмешательства, повреждений или несанкционированного доступа и предотвратить утечку, кражу или фальсификацию сетевых данных:

(1) создать внутренние системы и рабочие правила управления безопасностью, определить круг лиц, отвечающих за кибербезопасность и ввести ответственности за защиту кибербезопасности;

(2) принять технические меры для предотвращения заражения компьютерными вирусами, кибератак, вторжений в сеть и других действий, угрожающих кибербезопасности;

(3) принять технические меры для мониторинга и регистрации режимов функционирования сети и инцидентов кибербезопасности и соблюдать положения по хранению сетевых журналов в течение не менее шести месяцев;

(4) принять такие меры, как установление степени конфиденциальности данных, резервное копирование важных данных и шифрование;

(5) выполнять другие обязательства, предусмотренные законом или административными нормами.

Статья 22. Сетевые продукты и услуги должны удовлетворять соответствующим национальным и обязательным требованиям. Поставщики сетевых продуктов и услуг не должны устанавливать вредоносные программы; обнаружив, что их продукты и услуги имеют бреши в системе безопасности или уязвимости, они должны немедленно принять корректирующие меры, а также следовать положениям о незамедлительном информировании пользователей и компетентных ведомств.
Поставщики сетевых продуктов и услуг должны обеспечивать безопасность своих продуктов и услуг и не должны прекращать принятие мер по поддержанию безопасности в течение согласованного с клиентами срока или периода.
Если сетевой продукт или услуга содержит функцию сбора информации о пользователе, его поставщик должен четко на это указать и получить согласие со стороны пользователя; если это охватывает личную информацию пользователя, поставщик также должен

соблюдать положения настоящего закона и соответствующих законов и административных норм о защите личной информации.

Статья 23. Критическое сетевое оборудование и специализированные продукты, используемые для обеспечения кибербезопасности, должны соответствовать национальным стандартам и обязательным требованиям, и перед продажей или предоставлением должны быть сертифицированы квалифицированной организацией или пройти проверку на соблюдение требований безопасности. Государственные ведомства по кибербезопасности и информатизации вместе с компетентными ведомствами Государственного совета составляют и публикуют каталог критического сетевого оборудования и специализированных продуктов для обеспечения кибербезопасности и содействуют взаимному признанию сертификатов безопасности и результатов проверки безопасности, чтобы избежать дублирования сертификатов и проверок.

Статья 24. Сетевые операторы, предлагающие пользователям доступ к сети и услуги по регистрации доменных имен, доступ к сети через стационарные или мобильные телефоны или услуги по публикации информации или мгновенному обмену сообщениями, должны требовать от пользователей предоставления достоверных данных об их личности при подписании соглашений с пользователями или подтверждении предоставления услуг. Если пользователи не предоставили достоверные данные о своей личности, сетевой оператор не должен предоставлять им соответствующие услуги. Государство реализует стратегию доверия к сетевой идентификации и поддерживает исследование и разработку надежных и удобных технологий электронной аутентификации личности, поощряя взаимное принятие различных способов электронной аутентификации личности.

Статья 25. Сетевые операторы должны составлять планы реагирования на инциденты кибербезопасности и незамедлительно устранять уязвимости в системах, компьютерные вирусы, кибератаки, вторжения в сеть и аналогичные риски кибербезопасности. При возникновении инцидентов кибербезопасности сетевые операторы должны немедленно приступить к выполнению плана реагирования на чрезвычайные ситуации, принять надлежащие корректирующие меры и проинформировать компетентные ведомства согласно соответствующим положениям.

Статья 26. Лица, которые занимаются сертификацией, тестированием, оценкой рисков для обеспечения кибербезопасности или аналогичными видами деятельности — или открыто публикуют информацию о кибербезопасности, например сведения об уязвимости систем, компьютерных вирусах, сетевых атаках или вторжениях, — должны соблюдать соответствующие национальные нормы.

Статья 27. Физические лица и организации не должны незаконно вторгаться в сети других сторон, нарушать нормальное функционирование сетей других сторон, а также воровать сетевые данные или заниматься иной деятельностью, угрожающей кибербезопасности; они не должны предоставлять программы или инструменты, специально используемые для сетевых вторжений, нарушения нормального функционирования сетей и мер защиты, кражи сетевых данных или других действий, угрожающих кибербезопасности; если им достоверно известно, что другие совершат действия, угрожающие кибербезопасности, они не должны предоставлять помощь, такую как техническая поддержка, реклама или оплата расходов.

Статья 28. Сетевые операторы должны оказывать техническую поддержку и содействие органам государственной и национальной безопасности, которые защищают национальную безопасность и расследуют преступную деятельности в соответствии с законом.

Статья 29. Государство поддерживает сотрудничество между сетевыми операторами в таких областях, как сбор, анализ и предоставление информации по кибербезопасности,

ее использование для устранения чрезвычайных ситуаций, расширение возможностей сетевых операторов по охране безопасности.
Соответствующие отраслевые организации должны создать и наладить механизмы стандартизации и координации в области кибербезопасности для своей отрасли, укрепить анализ и оценку кибербезопасности, а также периодически предупреждать о рисках, поддерживать и координировать реагирование участников на риски кибербезопасности.
Статья 30. Информация, полученная ведомствами по кибербезопасности и информатизации и компетентными ведомствами, выполняющими обязанности по защите кибербезопасности, может использоваться только по мере необходимости для защиты кибербезопасности и не должна использоваться для других целей.

Раздел 2. Безопасность работы критической информационной инфраструктуры
Статья 31. Государство реализует основную защиту на основе многоуровневой системы защиты кибербезопасности связи общего пользования и информационных услуг, энергетики, транспорта, водных ресурсов, финансов, общественных служб, электронного правительства и другой критической информационной инфраструктуры, которая в случае уничтожения, потери функциональности или утечки данных может поставить под серьезную угрозу национальную безопасность, национальное и народное благосостояние или общественные интересы. Государственный совет определяет конкретные рамки и меры по охране безопасности критической информационной инфраструктуры.
Государство поощряет добровольное участие операторов сетей, находящихся за [обозначенными] рамками критически важных систем информационной инфраструктуры, в системе защиты критической информационной инфраструктуры.
Статья 32. В соответствии с обязанностями и разделением труда, предусмотренными Государственным советом, ведомства, отвечающие за работу по обеспечению безопасности критической информационной инфраструктуры должны в индивидуальном порядке составлять планы обеспечения безопасности критической информационной инфраструктуры своей отрасли или сектора, а также направлять и контролировать деятельность по обеспечению безопасности функционирования критической информационной инфраструктуры.
Статья 33. Лица, создающие критическую информационную инфраструктуру, должны обеспечить, чтобы она обладала возможностью сохранения стабильности бизнеса и устойчивого функционирования, и обеспечить синхронное планирование, введение и применение технических мер безопасности.
Статья 34. В дополнение к положениям статьи 21 настоящего закона операторы критической информационной инфраструктуры также выполняют следующие обязанности по обеспечению безопасности:
(1) создание специализированных органов по управлению безопасностью, назначение лиц, отвечающих за управление безопасностью, и проверка биографических данных этих ответственных лиц и персонала, занимающего критически важные должности;
(2) периодическое проведение обучения по кибербезопасности, технического обучения и оценки навыков сотрудников;
(3) создание резервных копий для послеаварийного восстановления важных систем и баз данных;
(4) подготовка планов реагирования на инциденты кибербезопасности и организация периодических учебно-тренировочных занятий;
(5) другие обязанности, предусмотренные законом или административными нормами.
Статья 35. Операторы критической информационной инфраструктуры, приобретающие сетевые продукты и услуги, которые могут повлиять на национальную безопасность, должны пройти национальную экспертизу безопасности, организованную

государственными ведомствами по кибербезопасности и информатизации и компетентными ведомствами Государственного совета.
Статья 36. Операторы критической информационной инфраструктуры, приобретающие сетевые продукты и услуги, должны следовать соответствующим положениям и заключить с поставщиком соглашение о безопасности и конфиденциальности, разъясняющее функции и обязанности в области сохранения безопасности и конфиденциальности.
Статья 37. Операторы критической информационной инфраструктуры, которые собирают или создают личную информацию или важные данные во время деятельности на материковой части территории Китайской Народной Республики, должны хранить их на материковой части Китая. Если из-за коммерческих требований действительно необходимо передать их за пределы материковой части, они должны принять меры по оценке безопасности, сформулированные совместно государственными ведомствами по вопросам кибербезопасности и информатизации и компетентными ведомствами Государственного совета; если законами и административными нормами предусмотрено иное, требуется соблюдать указанные положения.
Статья 38. Как минимум, раз в год операторы критической информационной инфраструктуры должны проводить контроль и оценку сетевой безопасности и возможных рисков либо самостоятельно, либо путем привлечения организации, оказывающей услуги в сфере кибербезопасности; операторы CII должны представить отчет по кибербезопасности с изложением обстоятельств контроля и оценки, а также мер по улучшению, в компетентное ведомство, отвечающее за работу по обеспечению безопасности критической информационной инфраструктуры.
Статья 39. Государственные ведомства по кибербезопасности и информатизации должны координировать работу компетентных ведомств по использованию следующих мер по обеспечению безопасности критической информационной инфраструктуры:
(1) Проведение проверок на местах с целью оценки рисков безопасности критической информационной инфраструктуры, предложение мер по улучшению ситуации с возможностью привлечения в случае необходимости организации, оказывающей услуги в сфере кибербезопасности, для проведения проверки и оценки рисков кибербезопасности.
(2) Периодически организация проведения операторами критической информационной инфраструктуры учебно-тренировочных занятий по реагированию на чрезвычайные ситуации, повышающих уровень, координацию и возможности реагирования на инциденты кибербезопасности.
(3) Содействие обмену информацией по кибербезопасности между компетентными ведомствами, операторами критической информационной инфраструктуры, а также компетентными научно-исследовательскими учреждениями и организациями, оказывающими услуги в сфере кибербезопасности.
(4) Оказание технической поддержки и помощи в области управления в чрезвычайной ситуации, послеаварийного восстановления и т. д. при возникновении инцидентов кибербезопасности.

Глава IV. Сетевая информационная безопасность

Статья 40. Сетевые операторы должны строго сохранять конфиденциальность пользовательской информации, которую они собирают, а также создать и наладить системы защиты пользовательской информации.
Статья 41. Сетевые операторы, собирающие и использующие личную информацию, должны соблюдать принципы законности, уместности и необходимости; они должны публиковать правила сбора и использования, четко указывать цели, средства и объем сбора или использования информации и получать согласие лиц, чьи данные собираются.

Сетевые операторы не должны собирать личную информацию, не связанную с предоставляемыми услугами; не должны нарушать положения законов, административных норм или соглашений между сторонами о сборе или использовании личной информации; должны следовать положениям законов, административных норм и соглашений с пользователями при обработке личной информации, которая у них хранится.

Статья 42. Сетевые операторы не должны раскрывать, фальсифицировать или уничтожать личную информацию, которую собирают; в отсутствие согласия лица, чья информация была собрана, личная информация не должна предоставляться другим. Однако это имеет место за исключением случая, когда информация может быть предоставлена, если после обработки невозможно идентифицировать конкретного человека и восстановить его личность.

Сетевые операторы должны принять технические и другие необходимые меры для защиты личной информации, которую собирают, и предотвращения утечки, уничтожения или потери личной информации. В случае, когда происходит или может произойти утечка, уничтожение или потеря личной информации, незамедлительно должны быть приняты корректирующие меры и выполнены действия согласно положениям об оперативном информировании пользователей и компетентных ведомств в соответствии с нормами.

Статья 43. При обнаружении физическими лицами того, что сетевые операторы нарушили положения законов, административных норм или соглашений между сторонами в части сбора или использования личной информации, они имеют право требовать удаления своей личной информации сетевыми операторами; при обнаружении ошибок в личной информации, собранной или сохраненной сетевыми операторами, они имеют право требовать, чтобы сетевые операторы внесли исправления. Сетевые операторы обязаны принимать меры для удаления и исправления.

Статья 44. Физические лица или организации не должны воровать личную информацию или использовать другие незаконные методы ее получения и не должны противозаконно продавать или предоставлять личную информацию другим.

Статья 45. Ведомства, на законном основании исполняющие обязанности по надзору и управлению кибербезопасностью, а также их сотрудники, должны сохранять строгую конфиденциальность личной информации, персональных данных и коммерческих секретов, о которых узнали при выполнении своих обязанностей, и не должны допускать утечку, продажу или незаконное предоставление этой информации другим.

Статья 46. Все физические лица и организации отвечают за использование ими сайтов и не должны создавать сайты или группы для общения с целью мошенничества, совершения уголовных преступлений, создания или продажи запрещенных и контролируемых товаров или других незаконных действий, и сайты не должны использоваться для публикации информации, связанной с мошенничеством, созданием или продажей запрещенных и контролируемых товаров или других незаконных действий.

Статья 47. Сетевые операторы должны укреплять управление информацией, публикуемой пользователями, и при получении сведений о том, что закон или административные нормы запрещают ее публикацию или передачу, они должны немедленно прекратить передачу этой информации, принять меры по обработке, такие как удаление информации, предотвратить распространение этой информации, сохранить соответствующие регистрационные записи и сообщить об этом соответствующим компетентным ведомствам.

Статья 48. Отправленная в электронном виде информация и прикладное программное обеспечение, предоставленные любым физическим лицом или организацией, не должны устанавливать вредоносные программы и не должны содержать информацию, которую законы и административные нормы запрещают публиковать или передавать.

На поставщиков услуг распространения информации в электронном виде и поставщиков услуг загрузки прикладного программного обеспечения возложены обязанности по

управлению безопасностью; если они узнают о том, что их пользователи совершили действия, указанные в предыдущем пункте, они обязаны: принять меры, такие как прекращение предоставления услуг и удаление информации или вредоносных программ; сохранить соответствующие регистрационные записи; сообщить об этом ответствующим компетентным ведомствам.

Статья 49. Сетевые операторы должны создать системы сетевой информационной безопасности для приема жалоб и сообщений, публично раскрывать информацию о способах подачи жалоб или отправки сообщений и оперативно принимать и рассматривать жалобы и сообщения, имеющие отношение к сетевой информационной безопасности. Сетевые операторы должны сотрудничать с ведомствами по кибербезопасности и информатизации и компетентными ведомствами при осуществлении надзора и проведении проверок в соответствии с законом.

Статья 50. Государственные ведомства по кибербезопасности и информатизации и компетентные ведомства выполняют обязанности по надзору и управлению сетевой информационной безопасностью в соответствии с законом; при обнаружении публикации или передачи информации, которая запрещена законами или административными нормами, они обязаны потребовать, чтобы сетевые операторы прекратили передачу, приняли меры по уничтожению, такие как удаление, и сохранили соответствующие регистрационные записи; если описанная выше информация поступает из-за пределов материковой части Китайской Народной Республики, они должны уведомить соответствующую организацию о необходимости принять технические и другие необходимые меры для блокировки передачи.

Глава V. Контроль, раннее предупреждение и реагирование на чрезвычайные ситуации

Статья 51. Государство создает систему мониторинга кибербезопасности, раннего предупреждения и информационного обмена. Государственные ведомства по кибербезопасности и информатизации должны осуществлять общую координацию работы компетентных ведомств для укрепления сбора, анализа и представления информации о кибербезопасности и соблюдать требования норм для унифицированной публикации информации в рамках мониторинга кибербезопасности и раннего предупреждения.

Статья 52. Ведомства, отвечающие за работу по обеспечению безопасности критической информационной инфраструктуры, должны создать и наладить системы мониторинга кибербезопасности, раннего предупреждения и представления информации для соответствующей отрасли или сектора и представлять информацию в рамках мониторинга кибербезопасности и раннего предупреждения в соответствии с нормами.

Статья 53. Государственные ведомства по кибербезопасности и информатизации в координации с компетентными ведомствами создают и налаживают механизмы для оценки рисков кибербезопасности и реагирования на чрезвычайные ситуации, составляют планы реагирования на инциденты кибербезопасности и периодически проводят учебно-тренировочные занятия.

Ведомства, отвечающие за работу по обеспечению безопасности критической информационной инфраструктуры, должны составлять планы реагирования на инциденты кибербезопасности для соответствующей отрасли или сектора и периодически проводить учебно-тренировочные занятия.

В планах реагирования на чрезвычайные ситуации для инцидентов кибербезопасности необходимо ранжировать инциденты кибербезопасности на основе таких факторов, как степень ущерба в результате инцидента и масштаб воздействия, и предусмотреть соответствующие меры по реагированию на чрезвычайные ситуации.

Статья 54. При увеличении риска инцидентов кибербезопасности соответствующие ведомства народных правительств на уровне провинций и выше, действуя в рамках своих полномочий и предусмотренных процедур, должны принять следующие меры с учетом параметров риска кибербезопасности и возможного ущерба:

(1) потребовать, чтобы компетентные ведомства, организации и персонал оперативно собрали и представили соответствующую информацию и усилили мониторинг возникновения рисков кибербезопасности;

(2) организовать проведение компетентными ведомствами, организациями и квалифицированным персоналом анализа и оценки информации о риске кибербезопасности и спрогнозировать вероятность возникновения инцидента, масштаб воздействия и степень ущерба;

(3) распространить предупреждения о риске кибербезопасности для общественности и опубликовать информацию о мерах по предотвращению или снижению ущерба.

Статья 55. При возникновении инцидента кибербезопасности необходимо немедленно приступить к выполнению плана реагирования на чрезвычайные ситуации, провести анализ и оценку инцидента кибербезопасности, потребовать принятия сетевыми операторами технических и других необходимых мер, устранить потенциальные риски безопасности, предотвратить распространение угрозы и незамедлительно опубликовать предупреждения для общественности.

Статья 56. Если при выполнении обязанностей по надзору и управлению в области кибербезопасности компетентные ведомства народных правительств на уровне провинций и выше обнаружат в сетях относительно высокий риск безопасности или инцидент безопасности, они имеют право в рамках своих полномочий и предусмотренных процедур вызвать юридического представителя или ответственное лицо оператора этой сети для опроса. Сетевые операторы должны соблюдать требования по применению процедур, вносить исправления и устранять скрытые опасности.

Статья 57. Внезапные чрезвычайные ситуации или происшествия в сфере производственной безопасности, возникшие в результате инцидентов кибербезопасности, необходимо устранять в соответствии с положениями «Закона Китайской Народной Республики о чрезвычайных ситуациях», «Закона Китайской Народной Республики о безопасности на производстве» и других соответствующих законов и административных норм.

Статья 58. Для удовлетворения потребности в защите национальной безопасности и социального общественного порядка, а также для реагирования на требования общества при возникновении крупных инцидентов безопасности, могут быть приняты временные меры, как предусмотрено или утверждено Государственным советом, в отношении передачи данных по сети в конкретном регионе, например такая передача данных может быть ограничена.

Глава VI. Юридическая ответственность

Статья 59. Если сетевые операторы не выполняют обязанности по защите кибербезопасности, предусмотренные в статьях 21 и 25 настоящего закона, компетентные ведомства направляют им предписания об устранении нарушений и предупреждения; в случае отказа исправить ситуацию, причинения вреда кибербезопасности или других аналогичных последствий взимается штраф от 10 000 до 100 000 юаней; с непосредственно ответственного руководящего персонала взимается штраф от 5000 до 50 000 юаней. Если операторы критической информационной инфраструктуры не выполняют обязанности по защите кибербезопасности, предусмотренные в статьях 33, 34, 36 и 38 настоящего закона, компетентные ведомства направляют им предписания об устранении нарушений и предупреждения; в случае отказа исправить ситуацию, причинения вреда кибербезопасности или других аналогичных последствий взимается

штраф от 100 000 до 1 000 000 юаней; с непосредственно ответственного руководящего персонала взимается штраф от 10 000 до 100 000 юаней.
Статья 60. При нарушении пункта 1 или 2 статьи 22 или пункта 1 статьи 48 настоящего закона любым из перечисленных ниже действий, соответствующие компетентные ведомства должны направлять предписания об устранении нарушений и предупреждения; в случае отказа исправить ситуацию, причинения вреда кибербезопасности или других последствий взимается штраф от 50 000 до 500 000 юаней; с непосредственно ответственных лиц взимается штраф от 10 000 до 100 000 юаней:
(1) установка вредоносных программ;
(2) непринятие незамедлительных мер по устранению брешей в системе безопасности или уязвимостей, которые имеются в продуктах или услугах, или непредставление информации пользователям и отчетности компетентным ведомствам в соответствии с нормами;
(3) неправомерное прекращение обеспечения безопасности продуктов или услуг.
Статья 61. Нарушение сетевыми операторами пункта 1 статьи 24 настоящего закона, когда они не требуют, чтобы пользователи предоставили достоверные данные о своей личности, или оказывают соответствующие услуги пользователям, не предоставившим достоверных данных о своей личности, влечет за собой получение предписания об устранении нарушений от соответствующего компетентного ведомства; в случае отказа исправить ситуацию или серьезных обстоятельств взимается штраф от 50 000 до 500 000 юаней, а соответствующее компетентное ведомство может направить предписание о временной приостановке операций, о приостановке хозяйственной деятельности до устранения нарушений, о закрытии сайтов, об отзыве разрешений на выполнение соответствующих операций или аннулировании лицензий на ведение хозяйственной деятельности; с непосредственно ответственных лиц и другого непосредственно ответственного персонала взимается штраф от 10 000 до 100 000 юаней.
Статья 62. При нарушении статьи 26 настоящего закона в отношении сертификации, тестирования или оценки рисков для обеспечения кибербезопасности или публикации информации о кибербезопасности, например сведений об уязвимости систем, компьютерных вирусах, кибератаках или сетевых вторжениях, направляется предписание об устранении нарушений и предупреждение; в случае отказа исправить ситуацию или серьезных обстоятельств взимается штраф от 10 000 до 100 000 юаней, а соответствующее компетентное ведомство может направить предписание о временной приостановке операций, о приостановке хозяйственной деятельности до устранения нарушений, о закрытии сайтов, об отзыве разрешений на выполнение соответствующих операций или аннулировании лицензий на ведение хозяйственной деятельности; с непосредственно ответственных лиц и другого непосредственно ответственного персонала взимается штраф от 5000 до 50 000 юаней.
Статья 63. Нарушение статьи 27 настоящего закона путем ведения деятельности, наносящей ущерб кибербезопасности, или путем предоставления специализированного программного обеспечения или инструментов для деятельности, наносящей ущерб кибербезопасности, или путем предоставления помощи другим лицам, деятельность которых наносит ущерб кибербезопасности, такой как техническая поддержка, реклама или оплата расходов, если не является преступлением, влечет за собой конфискацию незаконных доходов органами общественной безопасности и лишение свободы на срок до 5 суток, при этом может взиматься штраф от 50 000 до 500 000 юаней; в случае серьезных обстоятельств срок лишения свободы составляет от 5 до 15 суток и может взиматься штраф от 100 000 до 1 000 000 юаней.
Если указанные в предыдущем пункте действия совершены организацией, то органы общественной безопасности конфискуют незаконные доходы и взимают штраф от 100 000 до 1 000 000 юаней, а с непосредственно ответственных лиц и другого

непосредственно ответственного персонала взимается штраф в соответствии с предыдущим пунктом.
При нарушении статьи 27 настоящего закона лицам, на которых органами общественной безопасности наложено административное взыскание, запрещается заниматься управлением кибербезопасностью или занимать ключевые должности в сфере эксплуатации сетей в течение 5 лет; лицам, которым назначено уголовное наказание, пожизненно запрещается работать в сфере управления кибербезопасностью и занимать ключевые должности в сфере эксплуатации сетей.
Статья 64. Нарушение сетевыми операторами и поставщиками сетевых продуктов или услуг пункта 3 статьи 22 или статей 41–43 настоящего закона путем неправомерного использования личной информации, которая защищена в соответствии с законом, влечет за собой получение предписания об устранении нарушений от соответствующего компетентного ведомства и может независимо или одновременно повлечь за собой предупреждения, конфискацию незаконного дохода и/или штраф в 1–10-кратном размере незаконных доходов; при отсутствии незаконных доходов взимается штраф до 1 000 000 юаней, а с непосредственно ответственных лиц и другого непосредственно ответственного персонала взимается штраф от 10 000 до 100 000 юаней; в случае серьезных обстоятельств соответствующее компетентное ведомство может направить предписание о временной приостановке операций, о приостановке хозяйственной деятельности до устранения нарушений, о закрытии сайтов, об отзыве разрешений на выполнение соответствующих операций или аннулировании лицензий на ведение хозяйственной деятельности.
Нарушение статьи 44 настоящего закона путем кражи или использования других незаконных средств для получения, незаконной продажи или незаконного предоставления другим личной информации, если не является преступлением, влечет за собой конфискацию незаконных доходов органами общественной безопасности и штраф в 1–10-кратном размере незаконных доходов, а при отсутствии незаконных доходов взимается штраф до 1 000 000 юаней.
Статья 65. При нарушении операторами критической информационной инфраструктуры статьи 35 настоящего закона путем использования сетевых продуктов или услуг, не прошедших экспертизу безопасности, соответствующее компетентное ведомство направляет предписание о прекращении использования и взимает штраф в 1–10-кратном размере покупной цены; с непосредственно ответственных лиц и другого непосредственно ответственного персонала взимается штраф от 10 000 до 100 000 юаней.
Статья 66. При нарушении операторами критической информационной инфраструктуры статьи 37 настоящего закона путем хранения сетевых данных за пределами материковой части территории или предоставления сетевых данных лицам, находящимся за пределами материковой части территории, соответствующее компетентное ведомство: отправляет предписание об устранении нарушений и предупреждение, конфискует незаконные доходы, взимает штраф от 50 000 до 500 000 юаней и может направить предписание о временной приостановке операций, о приостановке хозяйственной деятельности до устранения нарушений, о закрытии сайтов, об отзыве разрешений на выполнение соответствующих операций или аннулировании лицензий на ведение хозяйственной деятельности. С непосредственно ответственных лиц и другого непосредственно ответственного персонала взимается штраф от 10 000 до 100 000 юаней.
Статья 67. Нарушение статьи 46 настоящего закона путем создания сайта или группы для общения с целью ведения незаконной или преступной деятельности, или путем использования сети для публикации информации, связанной с ведением незаконной или преступной деятельности, если не совершено преступление, влечет за собой лишение свободы органами общественной безопасности на срок до 5 суток, при этом может

взиматься штраф от 10 000 до 15 000 юаней; в случае серьезных обстоятельств срок лишения свободы составляет от 5 до 15 суток и может взиматься штраф от 50 000 до 500 000 юаней. Кроме того, органы общественной безопасности имеют право закрыть сайты и группы для общения, используемые с целью ведения незаконной или преступной деятельности.
Если охваченные в предыдущем пункте действия совершены организацией, то органами общественной безопасности взимается штраф от 100 000 до 500 000 юаней, а с главных ответственных руководителей и другого непосредственно ответственного персонала взимается штраф в соответствии с предыдущим пунктом.
Статья 68. При нарушении сетевыми операторами статьи 47 настоящего закона, когда не прекращена передача информации, передача и публикация которой запрещены законами или административным нормам, не приняты меры по ее уничтожению, например удалению, или не сохранены соответствующие регистрационные записи, соответствующее компетентное ведомство направляет предписание об устранении нарушений и предупреждение, а также конфискует незаконный доход; в случае отказа исправить ситуацию или серьезных обстоятельств взимается штраф от 100 000 до 500 000 юаней и может быть направлено предписание о временной приостановке операций, о приостановке хозяйственной деятельности до устранения нарушений, о закрытии сайтов, об отзыве разрешений на выполнение соответствующих операций или аннулировании лицензий на ведение хозяйственной деятельности; с непосредственно ответственных лиц и другого непосредственно ответственного персонала взимается штраф от 10 000 до 100 000 юаней.
Невыполнение поставщиками электронных информационных услуг и поставщиками услуг загрузки прикладного программного обеспечения своих обязанностей по управлению безопасностью, предусмотренных в пункте 2 статьи 48 настоящего закона, влечет за собой наказание в соответствии с положениями предыдущего пункта.
Статья 69. Сетевым операторам, нарушающим положения настоящего закона путем любого из перечисленных ниже действий, соответствующие компетентные ведомства направляют предписание об устранении нарушений; в случае отказа исправить ситуацию или серьезных обстоятельств взимается штраф от 50 000 до 500 000 юаней, а с непосредственно ответственного руководящего и другого персонала взимается штраф от 10 000 до 100 000 юаней:
(1) невыполнение требований компетентных ведомств о принятии мер по уничтожению, таких как прекращение распространения или удаление информации, которую законы или административные нормы запрещают публиковать или распространять;
(2) отказ или воспрепятствование осуществлению компетентными ведомствами законного надзора и проверки;
(3) неоказание технической поддержки и помощи органам общественной и государственной безопасности.
Статья 70. Публикация или передача информации, запрещенная пунктом 2 статьи 12 настоящего закона или другими законами или административными нормами, карается в соответствии с положениями соответствующих законов и административных норм.
Статья 71. Действия, нарушающие положения настоящего закона, должны регистрироваться в досье социального рейтинга и разглашаться согласно соответствующим законам и административным нормам.
Статья 72. Если предусмотренные настоящим законом обязанности по защите кибербезопасности не выполняются сетевыми операторами, которые являются государственными организациями и находятся в ведении правительства, вышестоящая организация или компетентные организации направляют предписание об устранении

нарушений; на непосредственно ответственных руководителей и другой непосредственно ответственный персонал налагаются взыскания.
Статья 73. При нарушении ведомствами по кибербезопасности и информатизации и другими компетентными ведомствами положений статьи 30 настоящего закона путем нецелевого использования личной информации, полученной при выполнении обязанностей по защите кибербезопасности, на непосредственно ответственных лиц и другой непосредственно ответственный персонал налагаются взыскания.
На персонал ведомств по кибербезопасности и информатизации и других компетентных ведомств, который пренебрегает своими обязанностями, злоупотребляет полномочиями, проявляет фаворитизм, если это не является преступлением, налагаются взыскания в соответствии с законом.
Статья 74. Если нарушения положений настоящего закона наносят ущерб другим лицам, виновные несут гражданскую ответственность в соответствии с законом.
Если нарушения положений настоящего закона приводят к нарушению общественного порядка, налагаются административные взыскания в соответствии с законом; если имеется состав преступления, виновные несут уголовную ответственность в соответствии с законом.
Статья 75. Если иностранные учреждения, организации или физические лица совершают атаки, вторжения, вмешательство, наносят ущерб или ведут другую деятельность, которая угрожает критической информационной инфраструктуре Китайской Народной Республики и приводит к серьезным последствиям, виновные должны понести юридическую ответственность в соответствии с законом; входящие в состав Государственного совета ведомства по общественной безопасности и компетентные ведомства также имеют право принять решение о наложении ареста на активы учреждения, организации или физического лица или применить другие необходимые меры наказания.

Глава VII. Дополнительные положения

Статья 76. Приведенная ниже терминология имеет в настоящем законе следующие значения:
(1) «Сеть» [网络, также «кибер»] — система, состоящая из компьютеров или других информационных терминалов и сопутствующего оборудования, которая используется для сбора, хранения, передачи, обмена и обработки информации в соответствии с определенными правилами и процедурами.
(2) «Кибербезопасность» [网络安全, также «сетевая безопасность»] — принятие необходимых мер для предотвращения кибератак, вторжений, вмешательства, разрушения и незаконного использования, а также неожиданных аварий, обеспечение такого состояния сетей, в котором они работают стабильно и надежно, а также обеспечение возможности того, чтобы сетевые данные были полными, конфиденциальными и пригодными для использования.
(3) «Сетевые операторы» [网络运营者] — владельцы и администраторы сетей и поставщики сетевых услуг.
(4) «Сетевые данные» [网络数据] — все виды электронных данных, которые собираются, хранятся, передаются, обрабатываются и создаются в сетях.
(5) «Личная информация» [个人 息息] — все виды информации, записанной в электронном виде или с помощью других средств, которая сама по себе или в совокупности с другой информацией достаточна для того, чтобы установить личность физического лица, в том числе «полные имена, даты рождения, национальные идентификационные номера, личная биометрическая информация, адреса, телефоны физических лиц и т. д.

Статья 77. При защите эксплуатационной безопасности сетей, где хранится или обрабатывается информация, касающаяся государственной тайны, необходимо соблюдать настоящий закон, а также положения законов и административных норм, относящиеся к сохранению секретности.
Статья 78. Правила обеспечения безопасности военных сетей устанавливаются Центральным военным советом.
Статья 79. Настоящий закон вступает в силу 1 июня 2017 года**.**

Приложение 2
Министерство промышленности и информационных технологий Китая, Меры по управлению доменными именами в интернете[31] (выдержки)

Статья 3 мер предписывала Министерству промышленности и информационных технологий выполнять следующие «основные задачи по надзору и управлению в области услуг для доменных имен на всей территории страны: (1) выработка правил и политики управления доменными именами в интернете; (2) создание интернет-системы доменных имен и планирование развития ресурсов доменных имен; (3) управление отечественными операторами корневых серверов доменных имен и органами регистрации и администрирования доменных имен; (4) несение ответственности за управление сетевой и информационной безопасностью системы доменных имен; (5) защита личной информации и законных прав и интересов пользователей в соответствии с законом; (6) несение ответственности за международную координацию в области доменных имен; (7) управление отечественными службами разрешения доменных имен; (8) управление другими видами деятельности, касающимися услуг для доменных имен».
Статья 10 мер предусматривала, что «лица, подающие заявку на создание корневого сервера доменных имен или организации-оператора корневого сервера доменных имен, должны отвечать следующим условиям: (1) корневой сервер доменных имен должен быть установлен на территории страны и должен соответствовать планам развития интернета и требованиям по обеспечению безопасной и стабильной работы системы доменных имен».
Статья 11. Лица, подающие заявку на создание органа регистрации и администрирования доменных имен, должны отвечать следующим условиям:
(1) система управления доменными именами верхнего уровня должна быть создана на территории страны, а используемые доменные имена верхнего уровня должны соответствовать законам и нормам, а также требованиям по обеспечению безопасной и стабильной работы системы доменных имен;
(2) [они должны] быть юридическими лицами, законно созданными на территории страны; указанное юридическое лицо и его основные инвесторы, ключевой оперативный и управленческий персонал должны иметь хороший социальный рейтинг;
(3) наличие безупречных планов профессионального развития и технологических схем, а также помещений, финансов и квалифицированных кадров, подходящих для ведения деятельности по управлению доменным именем верхнего уровня, наряду с наличием систем управления информацией, соответствующих требованиям органа управления телекоммуникациями;
(4) наличие полного набора средств управления сетевой и информационной безопасностью, включая руководящий персонал, структуры управления сетевой и информационной безопасностью, планы и процедуры действий в экстренных ситуациях и соответствующие технические и управленческие меры;
(5) наличие возможности выполнять верификацию личности и защиту личной информации пользователей, возможности обеспечить долгосрочное оказание услуг,

[31] Министерство промышленности и информационных технологий, Меры по управлению доменными именами в интернете, 24 августа 2017 года https://www.chinalawtranslate.com/en/internet-domain-name-management-measures/ (неофициальный перевод). Настоящий документ переведен на несколько языков исключительно в информационных целях. Оригинальный текст (на китайском языке) доступен здесь: http://www.cac.gov.cn/2017-09/28/c_1121737753.htm.

а также полного набора механизмов прекращения обслуживания;

(6) наличие полноценных структур управления услугами регистрации доменных имен и механизмов надзора за органами регистрации доменных имен;
(7) выполнение других требований, предусмотренных законами и административными нормами.
Статья 12. Лица, подающие заявку на создание органа по оказанию услуг регистрации доменных имен, должны отвечать следующим условиям:
(1) система оказания услуг по регистрации доменных имен, регистрационная база данных и системы разрешения имен должны быть созданы на территории страны;
(2) [они должны] быть юридическими лицами, законно созданными на территории страны; указанное юридическое лицо и его основные инвесторы, ключевой оперативный и управленческий персонал должны иметь хороший социальный рейтинг;
(3) наличие помещений, финансов и квалифицированных кадров, подходящих для оказания услуг по регистрации доменных имен, наряду с наличием систем управления информацией, соответствующих требованиям органа управления телекоммуникациями;
(4) наличие возможности выполнять верификацию личности и защиту личной информации пользователей, возможности обеспечить долгосрочное оказание услуг, а также полного набора механизмов прекращения обслуживания;
(6) наличие полного набора средств управления сетевой и информационной безопасностью, включая руководящий персонал, структуры управления сетевой и информационной безопасностью, планы и процедуры действий в экстренных ситуациях и соответствующие технические и управленческие меры.
(7) выполнение других требований, предусмотренных законами и административными нормами.
Статья 13. Лица, подающие заявку на создание корневого сервера доменных имен и организации-оператора корневого сервера доменных имен или органа управления регистрацией доменных имен должны представить материалы заявки в Министерство промышленности и информационных технологий. Лица, подающие заявку на создание органа по оказанию услуг регистрации доменных имен, должны представить материалы заявки в местное ведомство по управлению телекоммуникациями провинции, автономного района или муниципалитета.
Материалы заявки должны содержать:
(1) основные сведения об организации-заявителе;
(2) сертификационные документы, подтверждающие возможность эффективного управления услугами для доменных имен, в том числе сертификаты на соответствующие системы и помещения, документы с описанием возможностей обслуживания и управленческих структур, а также соглашения с другими организациями;
(3) структуры и меры по обеспечению сетевой и информационной безопасности;
(4) документы, подтверждающие репутацию организации-заявителя;
(5) письменное обязательство вести бизнес честно и в соответствии с законом, подписанное правомочным представителем».
Статья 37. «При предоставлении услуг разрешения доменных имен запрещено самовольно искажать данные, используемые для разрешения имен. Разрешение доменного имени не должно быть злонамеренно перенаправлено какой-либо организацией или физическим лицом на IP-адреса других лиц».
Статья 41 мер гласит: «Когда это необходимо для обеспечения национальной безопасности или ликвидации чрезвычайных ситуаций, организации-операторы корневых серверов доменных имен, органы управления регистрацией доменных имен и органы по оказанию услуг регистрации доменных имен должны подчиняться единому командованию

и координации со стороны органов управления телекоммуникациями и выполнять требования органов управления телекоммуникациями».
Статья 46. «Органы управления телекоммуникациями должны создать структуры для регистрации деловой репутации организаций-операторов корневых серверов доменных имен, органов управления доменными именами и органов по оказанию услуг регистрации доменных имен и вносить в досье этих организаций сведения о нарушении настоящих мер, а также наложенных административных взысканиях».

Приложение 3
Система доменных имен в китайском сегменте интернета[32] (выдержки)

I. В нашей стране доменные имена всех уровней в интернете могут состоять из букв (A–Z, a–z, при этом прописные и строчные буквы эквивалентны), цифр (0–9), дефиса (-) и китайских иероглифов; во всех доменах в качестве соединительного элемента должна использоваться точка (.), а в доменных именах всех уровней на китайском языке в качестве соединительных элементов должны использоваться либо точки, либо знак пунктуации, используемый в качестве точки в китайской системе письма (。).

II. Помимо доменов верхнего уровня «.CN» и «.中国» в нашей национальной системе доменных имен интернета создано несколько доменов верхнего уровня на английском и китайском языке. Среди них домены верхнего уровня «政务» [.gov] и «.公益» [.org, буквальный перевод: «общественные интересы»] являются специализированными доменами верхнего уровня на китайском языке, которые предназначены для партийных и правительственных групп и органов страны и других государственных структур всех уровней и для некоммерческих организаций. Схема нашей национальной системы доменов интернета представлена здесь: «http://中国互联网域名体系.中国», «http://中国互联网域名体系.政务» или «http://中国互联网域名体系.信息».

III. В национальном домене верхнего уровня «.CN» создано два типа доменов второго уровня: «домены категорий» и «домены административных районов». Создано девять «доменов категорий», а именно: «政务» используется для партийных и государственных групп и органов на всех уровнях партийной системы и других государственных структур; «公益» используется для некоммерческих организаций; «GOV» используется для государственных органов; «ORG» используется для некоммерческих организаций; «AC» используется для научно-исследовательских учреждений; «COM» используется для промышленных, коммерческих, финансовых и других предприятий; «EDU» используется для образовательных учреждений; «MIL» используется для оборонных учреждений страны; «NET» используется для организаций, предоставляющих интернет-услуги. Создано тридцать четыре «домена административных районов», которые предназначены для использования организациями каждой из провинций, автономных регионов, городов центрального подчинения и специальных административных районов страны [...].

IV. Разрешено подавать заявки на прямую регистрацию доменных имен второго уровня в национальных доменах верхнего уровня «.CN» и «.中国».

[32] Перевод China Law, Система доменных имен в китайском сегменте интернета, 5 марта 2018 года https://www.chinalawtranslate.com/en/chinese-internet-domain-name-system/ (неофициальный перевод). Настоящий документ переведен на несколько языков исключительно в информационных целях. Оригинальный текст (на китайском языке) доступен здесь: http://xn--eqrt2g.xn--vuq861b/#.

Приложение 4
Закон Китайской Народной Республики о безопасности данных (DSL)[33] (выдержки)

Статья 3. Для целей настоящего закона термин «данные» относится к любой записи информации в электронной или любой другой форме.
- Обработка данных включает, помимо прочего, сбор, хранение, использование, обработку, передачу, предоставление и раскрытие данных.
- Безопасность данных означает обеспечение эффективной защиты и законного использования данных путем принятия необходимых мер, а также способность гарантировать постоянную безопасность данных.

Статья 7. Государство должно защищать связанные с данными права и интересы физических лиц и организаций, поощрять законное, грамотное и эффективное использование данных, обеспечивать упорядоченный и соответствующий закону свободный поток данных, а также способствовать развитию цифровой экономики, где данные являются ключевым фактором.

Статья 11. Государство должно активно осуществлять международный обмен и сотрудничество в таких областях, как управление безопасностью данных, разработка и использование данных, участвовать в выработке соответствующих международных правил и стандартов безопасности данных и содействовать безопасному и свободному трансграничному потоку данных.

Статья 14. Государство должно осуществлять стратегию Большие Данные, содействуя созданию инфраструктуры данных, а также поощряя и поддерживая инновационное применение данных во всех отраслях и областях.

Статья 17. Государство должно способствовать формированию системы стандартов в области разработки, технологий использования и безопасности данных. Ведомства Государственного совета по стандартизации и другие компетентные ведомства Государственного совета должны в рамках своих соответствующих обязанностей организовать выработку и надлежащий пересмотр стандартов в области технологий и продуктов для разработки и использования данных, а также для безопасности данных. Государство должно поддерживать участие предприятий, социальных групп, учебных и научно-исследовательских учреждений и т. д. в подготовке таких стандартов.

Статья 21. Данные о национальной безопасности, жизненно важных направлениях национальной экономики, важных аспектах жизни людей, основных общественных интересах и прочие являются основными данными государства, для которых должна применяться более строгая система управления.

Статья 25. Государство должно применять экспортный контроль в соответствии с законом в отношении данных, являющихся контролируемыми товарами, для сохранения национальной безопасности и выполнения международных обязательств.

Статья 26. Если какая-либо страна или регион вводит дискриминационные запреты, ограничения или другие аналогичные меры против КНР в отношении инвестиций или торговли, связанных с данными и технологиями разработки и использования данных,

[33] Закон Китайской Народной Республики о безопасности данных, 11 июня 2021 года, в переводе, который представлен здесь: https://www.secrss.com/articles/31844 (неофициальный перевод), оригинальная публикация представлена здесь: http://www.cac.gov.cn/2021-06/11/c_1624994566919140.htm). Настоящий документ переведен на несколько языков исключительно в информационных целях. Оригинальный текст (на китайском языке) доступен здесь: http://www.cac.gov.cn/2021-06/11/c_1624994566919140.htm.

КНР имеет право принять равные контрмеры против этой страны или региона, исходя из реальных обстоятельств.
Статья 27. При обработке данных с использованием информационных сетей, таких как интернет, обязанности по обеспечению безопасности данных должны выполняться на основе многоуровневой системы защиты кибербезопасности.
Статья 31. Положения Закона КНР о кибербезопасности применяются к управлению безопасностью при экспорте за пределы [материковой части] территории данных, собранных или созданных операторами критической информационной инфраструктуры на [материковой части] территории КНР; меры по управлению безопасностью при экспорте за пределы материковой части территории важных данных, собранных или созданных другими операторами данных на [материковой части] территории КНР, должны быть сформулированы Государственным управлением интернет-информации совместно с компетентными ведомствами Государственного совета.
Статья 32. Все организации и физические лица при сборе данных должны использовать законные и уместные способы и не должны получать данные путем кражи или другими незаконными способами. Если законы или административные нормы содержат положения о цели или объеме сбора и использования данных, данные должны собираться и использоваться в рамках цели и объема, предусмотренных такими законами и административными нормами.
Статья 33. Организации-посредники по транзакциям с данными при предоставлении услуг должны требовать от поставщиков данных указывать источники данных, проверять личности обеих сторон транзакции и сохранять регистрационные записи о проверке и транзакции.
Статья 36. Компетентные государственные органы КНР должны обрабатывать запросы о предоставлении данных, поступившие от иностранных судебных или правоохранительных органов, в соответствии с положениями законов и международных договоров или соглашений, которые заключила или к которым присоединилась КНР, или на основе принципа равноправия и взаимной выгоды. Без одобрения компетентных государственных органов КНР организации или физические лица на [материковой части] территории КНР не должны предоставлять данные, хранящиеся на [материковой части] территории КНР, иностранным судебным или правоохранительным органам.
Статья 38. Если государственным органам необходимо собирать или использовать данные для выполнения своих предписанных законом обязанностей, они должны собирать или использовать данные в объеме, необходимом для выполнения своих предписанных законом обязанностей, и в соответствии с требованиями и процедурами, предусмотренными законами и административными нормами; они должны, в соответствии с законом, сохранять конфиденциальность данных, к которым получили доступ в ходе выполнения своих обязанностей, таких как сведения о частной жизни, личная информация, коммерческая тайна и конфиденциальная деловая информация, и не должны разглашать такие данные или незаконно предоставлять их другим.
Статья 40. Если государственные органы поручают другим создавать или обслуживать системы электронного правительства или хранить и обрабатывать данные о деятельности государственных органов, эти органы должны пройти строгие процедуры утверждения и контролировать выполнение доверенными сторонами своих обязательств по обеспечению безопасности данных. Доверенная сторона должна выполнять свои обязательства по обеспечению безопасности данных в соответствии с положениями законов, нормативных актов и договорных соглашений и не должна хранить, использовать, разглашать или предоставлять другим данные о деятельности государственных органов без разрешения.

Статья 44. Если компетентные органы регулирования при выполнении своих обязанностей по надзору и управлению в отношении безопасности данных обнаруживают наличие серьезных рисков безопасности при обработке данных, они имеют право в рамках своих полномочий и предусмотренных процедур проводить переговоры с соответствующими организациями и физическими лицами и требовать соблюдения процедур, исправления ситуации и устранения скрытых угроз.
Статья 49. В случае невыполнения государственными органами своих обязательств по обеспечению безопасности данных, предусмотренных настоящим законом, на непосредственно ответственных руководителей и другой непосредственно ответственный персонал налагаются взыскания в соответствии с законом.
Статья 52. Если нарушения положений настоящего закона наносят ущерб другим лицам, виновные несут гражданскую ответственность в соответствии с законом.

Приложение 5
Закон Китайской Народной Республики о защите личной информации[34]

(принят 20 августа 2021 года на 30-й сессии Постоянного комитета Всекитайского собрания народных представителей 13-го созыва)

Глава I. Общие положения

Статья 1. Настоящий закон разработан на основе Конституции с целью защиты прав и интересов владельцев личной информации, стандартизации деятельности по обработке личной информации и содействия рациональному использованию личной информации.
Статья 2. Личная информация физических лиц пользуется правовой защитой; всем юридическим и физическим лицам запрещено нарушать права и интересы физических лиц в отношении личной информации.
Статья 3. Закон распространяется на деятельность по обработке личной информации физических лиц на территории Китайской Народной Республики».
Если при обработке за границей Китайской Народной Республики личной информации физических лиц, находящихся на территории Китайской Народной Республики, имеет место одно из следующих обстоятельств, этот закон также применяется:

1. когда цель состоит в предоставлении продуктов или услуг физическим лицам на территории страны;
2. при анализе или оценке деятельности физических лиц на территории страны;
3. в других обстоятельствах, предусмотренных в законах или административных нормах.

Статья 4. Личная информация — это все виды информации, записанной с помощью электронных или других средств, которая имеет отношение к идентифицированным или идентифицируемым физическим лицам, исключая информацию после анонимизации. Обработка личной информации включает сбор, хранение, использование, обработку, передачу, предоставление, публикацию, удаление личной информации и тому подобное.

[34] Закон Китайской Народной Республики о защите личной информации, (принят 20 августа 2021 года на 30-й сессии Постоянного комитета Всекитайского собрания народных представителей 13-го созыва), http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml, в переводе DigiChina: https://digichina.stanford.edu/news/translation-personal-information-protection-law-peoples-republic-china-effective-nov-1-2021

Статья 5. При обработке личной информации необходимо соблюдать принципы законности, уместности, необходимости и честности. Запрещается обрабатывать личную информацию вводящими в заблуждение, мошенническими, принудительными или другими аналогичными способами.
Статья 6. Обработка личной информации должна иметь четкую и разумную цель и должна быть напрямую связана со своей целью. При обработке необходимо использовать способ, оказывающий наименьшее влияние на индивидуальные права и интересы.
Личную информацию необходимо собирать в ограниченном объеме, который минимально необходим для достижения цели обработки. Сбор чрезмерно большого количества личной информации запрещен.
Статья 7. При обработке личной информации необходимо соблюдать принципы открытости и прозрачности, раскрывая правила обработки личной информации и четко указывая цель, способ и объем обработки.
Статья 8. При обработке личной информации необходимо обеспечить качество личной информации и избежать неблагоприятных последствий для индивидуальных прав и интересов из-за недостоверной или неполной личной информации.
Статья 9. Операторы личной информации несут ответственность за свою деятельность по обработке личной информации и принятие необходимых мер для обеспечения безопасности личной информации, которую они обрабатывают.
Статья 10. Всем организациям и физическим лицам запрещено незаконно собирать, использовать, обрабатывать или передавать личную информацию других лиц, незаконно продавать, покупать, предоставлять или раскрывать личную информацию других лиц или наносить ущерб национальной безопасности или общественным интересам при обработке личной информации.
Статья 11. Государство создает структуру защиты личной информации для предотвращения действий, наносящих ущерб правам и интересам субъектов личной информации, и наказания за такие действия, для усиления пропаганды и обучения в области защиты личной информации, а также для содействия формированию благоприятной среды для защиты личной информации, при совместном участии правительства, предприятий, компетентных общественных организаций и широких слоев населения.
Статья 12. Государство энергично участвует в разработке международных правил [или норм] защиты личной информации, стимулирует международный обмен и сотрудничество в области защиты личной информации и способствует взаимному признанию другими странами, регионами и международными организациями правил [или норм], стандартов и т. д. защиты личной информации.

Глава II. Правила обработки личной информации

Раздел 1. Общие положения

Статья 13. Операторы личной информации имеют право обрабатывать личную информацию только при наличии одного из следующих обстоятельств:

1. получено согласие физического лица;
2. когда это необходимо для заключения или выполнения договора, в котором физическое лицо является одной из заинтересованных сторон, или когда это необходимо для управления кадровыми ресурсами в соответствии с законно сформулированными трудовыми правилами и структурами и заключенными на законных основаниях коллективными договорами;
3. когда это необходимо для выполнения предписанных законом функций и обязанностей или обязательств;

4. когда это необходимо для реагирования на внезапные происшествия в сфере общественного здравоохранения, для защиты жизни и здоровья физических лиц или для защиты их собственности в чрезвычайных ситуациях;
5. при обработке личной информации в разумном объеме для создания новостных репортажей, контроля общественного мнения и других аналогичных мероприятий, отвечающих общественным интересам;
6. при обработке в разумном объеме и в соответствии с положениями настоящего закона личной информации, раскрытой физическими лицами по собственной инициативе или уже раскрытой на законных основаниях иным способом;
7. другие обстоятельства, предусмотренные в законах и административных нормах.

При обработке личной информации в соответствии с другими соответствующими положениями настоящего закона необходимо получить индивидуальное согласие. Однако получение индивидуального согласия не требуется при выполнении условий, перечисленных в пунктах 2–7 выше.

Статья 14. Если личная информация обрабатывается на основе индивидуального согласия, физические лица должны давать указанное согласие при полном понимании последствий в добровольном и недвусмысленном заявлении. Если законы или административные нормы предусматривают необходимость получения отдельного согласия или письменного согласия для обработки личной информации, требуется соблюдать указанные положения.

При изменении цели или способа обработки личной информации, или категорий обрабатываемой личной информации, согласие физического лица необходимо получить снова.

Статья 15. Если личная информация обрабатывается на основе индивидуального согласия, физические лица имеют право отозвать свое согласие. Операторы личной информации должны предоставить удобный способ отзыва согласия.

Отзыв физическим лицом своего согласия не влияет на правомочность действий по обработке личной информации, выполненных на основе индивидуального согласия до его отзыва.

Статья 16. Операторы личной информации не имеют права отказаться от предоставления продуктов или услуг на основании того, что физическое лицо не дает или отзывает согласие на обработку своей личной информации, за исключением случаев, когда обработка личной информации необходима для предоставления продуктов или услуг.

Статья 17. Операторы личной информации должны перед ее обработкой открыто сообщить физическим лицам следующие правдивые, точные и полные сведения ясным и понятным языком:

1. название или личное имя и контактные данные оператора личной информации;
2. цель и способы обработки личной информации, категории обрабатываемой личной информации и срок хранения;
3. способы и процедуры осуществления физическими лицами своих прав, предусмотренных в настоящем законе;
4. другие сведения, которые должны быть предоставлены в соответствии с законами или административными нормами.

При изменении сведений, перечисленных в предыдущем абзаце, физических лиц необходимо уведомить о таком изменении.

Если операторы личной информации предоставляют сведения по вопросам, указанным в пункте 1, путем составления правил обработки личной информации, необходимо опубликовать [раскрыть] эти правила и обеспечить удобство их чтения и сохранения.

Статья 18. Операторам личной информации разрешается при обработке личной информации не предоставлять физическим лицам сведения по вопросам, указанным

в пункте 1 предыдущей статьи, в обстоятельствах, когда согласно законам или административным нормам необходимо сохранить конфиденциальность или отсутствует необходимость уведомления.
В чрезвычайных обстоятельствах, когда необходимость защиты жизни и здоровья физических лиц или их собственности не позволяет своевременно уведомить физических лиц, операторы личной информации должны уведомить их после завершения чрезвычайных обстоятельств.
Статья 19. За исключением случаев, когда законы или административные нормы предусматривают иное, срок хранения личной информации не должен превышать периода, минимально необходимого для достижения цели обработки личной информации.
Статья 20. Если двое или более операторов личной информации совместно принимают решение о цели и способе обработки личной информации, они должны достигнуть соглашения по вопросу прав и обязанностей каждого оператора. Однако указанное соглашение не влияет на право физических лиц требовать соблюдения положений настоящего закона каждым оператором личной информации.
Если операторы, совместно обрабатывающие личную информацию, ущемляют права и интересы в отношении личной информации, что наносит ущерб, они несут совместную ответственность в соответствии с законом.
Статья 21. Если операторы личной информации поручают обработку личной информации другим, они должны заключить с доверенным лицом соглашение, в котором указываются цель, срок и способ порученной обработки, категории личной информации, меры защиты, а также права и обязанности обеих сторон и т. д., и должны осуществлять надзор за деятельностью доверенного лица по обработке личной информации.
Доверенные лица должны обрабатывать личную информацию в соответствии с этим соглашением; они не имеют права при обработке личной информации выходить за рамки указанных в соглашении целей или способов обработки и т. д. Если договор поручения не вступает в силу, недействителен, аннулирован или расторгнут, доверенное лицо обязано вернуть личную информацию оператору личной информации или удалить и не имеет права хранить ее.
В отсутствие согласия оператора личной информации доверенное лицо не имеет права перепоручить обработку личной информации другим лицам.
Статья 22. При возникновении необходимости передать личную информацию вследствие слияния, разделения, прекращения существования, объявления о банкротстве и других аналогичных причин операторы личной информации должны сообщить физическим лицам название или личное имя и контактные данные стороны, получающей информацию. Сторона, получающая информацию, должна продолжить выполнение обязанностей оператора личной информации. В случае изменения стороной, получающей информацию, первоначальной цели или способа обработки, необходимо снова направить физическому лицу уведомление в соответствии с положениями настоящего закона.
Статья 23. Если операторы личной информации предоставляют обрабатываемую ими личную информацию другим операторам, они должны сообщить физическим лицам название или личное имя получателя, его контактные данные, цель и способ обработки и категории личной информации, а также получить от каждого физического лица индивидуальное согласие. Получатели должны обрабатывать личную информацию в рамках вышеупомянутых целей и способов обработки, категорий личной информации и т.д. При изменении получателями первоначальной цели или способов обработки, они снова должны получить согласие физического лица.
Статья 24. Если операторы личной информации используют личную информацию для автоматизированного принятия решений, они должны гарантировать прозрачность принятия решений, справедливость и правомерность результата обработки, и они не

имеют права необоснованно применять дифференцированный подход к физическим лицам в отношении условий торговли, таких как торговая цена и т. д.
Лица, осуществляющие push-доставку информации или коммерческие продажи физическим лицам с помощью автоматизированных методов принятия решений, должны одновременно предусмотреть возможность не учитывать индивидуальные характеристики или предоставить физическому лицу удобный способ отказа.
Если использование автоматизированного принятия решений оказывает сильное влияние на права и интересы физического лица, оно имеет право требовать от операторов личной информации разъяснений по данному вопросу, а также имеет право отказаться от принятия решений оператором личной информации исключительно с помощью автоматизированных методов.
Статья 25. Операторы личной информации не имеют права раскрывать личную информацию, которую обрабатывают, кроме случаев, когда они получили отдельное согласие.
Статья 26. Установка в общественных местах оборудования для фотосъемки или распознавания личности должна осуществляться в соответствии с требованиями по обеспечению общественной безопасности и с соблюдением соответствующих государственных норм; при этом должны устанавливаться четкие опознавательные указатели. Собранные фотографии людей и информация о персональных отличительных особенностях может использоваться только в целях обеспечения общественной безопасности; ее запрещено использовать для других целей, кроме случаев, когда получено отдельное согласие физических лиц.
Статья 27. Операторы личной информации могут в разумном объеме обрабатывать личную информацию, уже раскрытую физическим лицом по собственной инициативе или раскрытую на законных основаниях иным способом, кроме случаев, когда физическое лицо явно возражает против этого. Если обработка уже раскрытой личной информации оказывает сильное влияние на индивидуальные права и интересы, оператор личной информации должен получить согласие физического лица в соответствии с положениями настоящего закона.

Раздел 2. Регламент обработки конфиденциальной личной информации

Статья 28. Конфиденциальная личная информация — это личная информация, которая в случае ее утечки или незаконного использования может легко причинить ущерб достоинству физических лиц, серьезный ущерб личной безопасности или безопасности имущества, в том числе информация о биометрических характеристиках, религиозных убеждениях, присвоенном особом статусе, здоровье, финансовых счетах, отслеживании местоположения и т.п., а также информация о несовершеннолетних в возрасте до 14 лет.
Операторы личной информации имеют право обрабатывать конфиденциальную личную информацию только при наличии конкретной цели и необходимости, приняв строгие меры защиты.
Статья 29. Для обработки конфиденциальной личной информации необходимо получить отдельное согласие физического лица. Если законы или административные нормы предусматривают необходимость получения письменного согласия на обработку конфиденциальной личной информации, требуется соблюдать указанные положения.
Статья 30. Операторы личной информации, которые занимаются обработкой конфиденциальной личной информации, в дополнение к сведениям, указанным в пункте 1 статьи 17 настоящего закона, также должны сообщить физическим лицам о необходимости такой обработки и ее влиянии на права и интересы физического лица, за исключением случаев, когда настоящим законом разрешено не уведомлять физических лиц.

Статья 31. Если операторы личной информации обрабатывают личную информацию несовершеннолетних в возрасте до 14 лет, они должны получить согласие одного из родителей или другого опекуна несовершеннолетнего.
Для обработки личной информации несовершеннолетних в возрасте до 14 лет операторы личной информации должны сформулировать специальные правила обработки.
Статья 32. Если законы или административные нормы предусматривают необходимость получения соответствующих распорядительных лицензий или вводят другие ограничения, относящиеся к обработке конфиденциальной личной информации, требуется соблюдать указанные положения.

Раздел 3. Особые положения об обработке личной информации государственными органами

Статья 33. Настоящий закон распространяется на деятельность государственных органов по обработке личной информации; в случаях, когда данный раздел содержит конкретные положения, применяются положения данного раздела.
Статья 34. Государственные органы, обрабатывающие личную информацию для исполнения своих предписанных законом функций и обязанностей, должны действовать в соответствии с полномочиями и процедурами, предусмотренными в законах или административных нормах; они не имеют права выходить за рамки того, что необходимо для исполнения их предписанных законом функций и обязанностей.
Статья 35. Государственные органы, обрабатывающие личную информацию для исполнения предписанных законом функций и обязанностей, должны выполнять обязательства в отношении уведомления, кроме случаев, когда имеют место обстоятельства, указанные в пункте 1 статьи 18 настоящего закона, или тогда, когда уведомление будет препятствовать исполнению государственным органом его предписанных законом функций и обязанностей.
Статья 36. Личная информация, обрабатываемая государственными органами, должна храниться на материковой части территории Китайской Народной Республики. Если действительно необходимо предоставить ее за границей, необходимо провести оценку безопасности. Разрешено обращаться к компетентным органам власти с просьбой оказать поддержку и помощь в проведении оценки безопасности.
Статья 37. Положения настоящего закона об обработке личной информации государственными органами распространяются на обработку личной информации для исполнения предписанных законом функций и обязанностей организациями, которые в установленном законом и нормами порядке уполномочены исполнять функции по связям с общественностью.

Глава III. Правила трансграничной передачи личной информации

Статья 38. Если операторам личной информации действительно необходимо передать личную информацию за границу Китайской Народной Республики из-за коммерческих или других аналогичных требований, должно быть выполнено одно из следующих условий:

1. прохождение оценки безопасности, организованной государственным ведомством по кибербезопасности и информатизации в соответствии со статьей 40 настоящего закона;
2. прохождение сертификации защиты личной информации, выполненной специализированным органом в соответствии с положениями государственного ведомства по кибербезопасности и информатизации;

3. заключение договора с иностранным получателем информации в соответствии со стандартным договором, разработанным государственным ведомством по кибербезопасности и информатизации, в котором согласованы права и обязанности обеих сторон;
4. другие условия, предусмотренные в законах или административных нормах или государственным ведомством по кибербезопасности и информатизации.

Если международные договора или соглашения, которые заключила или к которым присоединилась Китайская Народная Республика, содержат соответствующие положения, такие как условия передачи личной информации за границу Китайской Народной Республики, указанные положения могут быть приведены в исполнение. Операторы личной информации должны принять необходимые меры, чтобы обеспечить соблюдение иностранными получателями личной информации стандарта защиты личной информации, установленного в настоящем законе.

Статья 39. Если операторы личной информации передают личную информацию за границу Китайской Народной Республики, они должны сообщить физическому лицу название или личное имя иностранного получателя, его контактные данные, цель и способы обработки и категории личной информации, а также способы и процедуры осуществления физическими лицами своих прав, предусмотренных в настоящем законе применительно к иностранному получателю и другим аналогичным вопросам, и получить отдельное согласие физического лица.

Статья 40. Операторы критической информационной инфраструктуры и операторы личной информации, обрабатывающие личную информацию в объеме, который достиг значения, установленного государственным ведомством по кибербезопасности и информатизации, должны хранить личную информацию, собранную и созданную на территории Китайской Народной Республики, в пределах национальной юрисдикции. Если им необходимо передать ее за границу, то они должны пройти оценку безопасности, организованную государственным ведомством по кибербезопасности и информатизации; если законы или административные нормы и положения государственного ведомства по кибербезопасности и информатизации позволяют не проводить оценку безопасности, требуется соблюдать указанные положения.

Статья 41. Компетентные органы Китайской Народной Республики, согласно соответствующим законам и международными договорам или соглашениями, которые заключила или к которым присоединилась Китайская Народная Республика, или на основе принципа равноправия и взаимной выгоды, должны обрабатывать запросы о предоставлении личной информации, хранящейся на территории страны, поступившие от иностранных судебных или правоохранительных органов. Без одобрения компетентных органов Китайской Народной Республики операторы личной информации не имеют права предоставлять личную информацию, хранящуюся на материковой части территории Китайской Народной Республики, иностранным судебным или правоохранительным органам.

Статья 42. Если действия иностранных организаций или физических лиц, занимающихся обработкой личной информации, нарушают права и интересы граждан Китайской Народной Республики в отношении личной информации или наносят ущерб национальной безопасности или общественным интересам Китайской Народной Республики, государственное ведомство по кибербезопасности и информатизации имеет право включить их в список, ограничивающий или запрещающий предоставление личной информации, вынести предупреждение и принять меры, например ограничить или запретить предоставление им личной информации и т. д.

Статья 43. Если какая-либо страна или регион вводит дискриминационные запреты, ограничения или другие аналогичные меры против Китайской Народной Республики в области защиты личной информации, Китайская Народная Республика имеет право принять ответные меры против этой страны или региона, исходя из реальных обстоятельств.

Глава IV. Права физических лиц в отношении обработки личной информации

Статья 44. Физические лица имеют право быть осведомленными и право принимать решения в отношении своей личной информации, а также имеют право ограничить обработку своей личной информации другими или отказаться от нее, если законами или административными нормами не предусмотрено иное.

Статья 45. Физические лица имеют право ознакомиться со своей личной информацией и получить ее копию у операторов личной информации, за исключением обстоятельств, указанных в пункте 1 статьи 18 или в статье 35 настоящего закона.

Если физическое лицо направило запрос об ознакомлении со своей личной информацией или получении ее копии, оператор личной информации должен своевременно ее предоставить.

Если физическое лицо направило запрос о передаче его личной информации выбранному оператору личной информации, который удовлетворяет условиям государственного ведомства по кибербезопасности и информатизации, оператор личной информации должен предоставить канал для ее передачи.

Статья 46. Если физическое лицо обнаружило, что его личная информация недостоверная или неполная, оно имеет право потребовать исправления или дополнения его личной информации оператором личной информации. При получении от физического лица требования исправить или дополнить его личную информацию, операторы личной информации должны проверить личную информацию и своевременно внести необходимые исправления или дополнения.

При получении от физического лица требования исправить или дополнить его личную информацию, операторы личной информации должны проверить личную информацию и своевременно внести необходимые исправления или дополнения.

Статья 47. Операторы личной информации должны самостоятельно удалить личную информацию при возникновении одного из перечисленных ниже обстоятельств; если оператор личной информации не удалил ее, физические лица имеют право требовать ее удаления:

1. цель обработки достигнута, ее невозможно достичь, или [личная информация] больше не нужна для достижения целей обработки;
2. операторы личной информации прекращают предоставление продуктов или услуг, или истек срок хранения информации;
3. физическое лицо отзывает согласие;
4. оператор личной информации обрабатывал личную информацию в нарушение законов, административных норм или соглашений;
5. другие обстоятельства, предусмотренные законами или административными нормами.

Если не истек срок хранения, предусмотренный законами или административными нормами, или удаление личной информации технически сложно реализовать, операторы личной информации прекращают все операции по обработке личной информации, за исключением хранения и принятия необходимых мер по обеспечению безопасности.

Статья 48. Физические лица имеют право требовать от оператора личной информации разъяснения правил обработки личной информации.
Статья 49. В случае смерти физического лица его ближайший родственник имеет право в своих собственных законных интересах осуществлять права, предусмотренные в данной главе, для ознакомления с личной информацией умершего, ее копирования, исправления, удаления и т. д., кроме случаев, когда это противоречит воле физического лица, выраженной до его смерти.
Статья 50. Операторы личной информации должны создать удобные механизмы для принятия и обработки заявлений, поступающих от физических лиц в рамках осуществления их прав. При отклонении запросов на осуществление прав физических лиц они должны объяснить причину.
При отклонении запросов на осуществление прав физических лиц операторами личной информации, физические лица имеют право подать иск в народный суд в соответствии с законом.

Глава V. Обязанности оператора личной информации

Статья 51. Операторы личной информации должны, с учетом цели и способов обработки личной информации, категорий личной информации, а также влияния на права и интересы физических лиц, возможно существующих рисков безопасности и т. д., принять перечисленные ниже меры в целях обеспечения соответствия обработки личной информации положениям законов и административных норм и предотвращения несанкционированного доступа, а также утечки, искажения или потери личной информации:

2. формирование внутренних структур управления и правил деятельности;
3. внедрение процедур управления личной информацией в зависимости от ее категории;
4. принятие соответствующих технических мер безопасности, таких как шифрование, деидентификация и т. д.;
5. введение целесообразных рабочих пределов обработки личной информации и регулярное теоретическое и практическое обучение персонала;
6. подготовка и организация осуществления планов реагирования на инциденты безопасности, касающиеся личной информации;
7. другие меры, предусмотренные в законах или административных нормах.

Статья 52. Операторы личной информации, обрабатывающие личную информацию в объеме, который достиг значения, установленного государственным ведомством по кибербезопасности и информатизации, должны назначить сотрудника по защите личной информации, на которого возлагается ответственность за надзор над деятельностью по обработке личной информации, принятие мер защиты и т. д.
Операторы личной информации должны раскрыть способы связи с сотрудниками по защите личной информации и сообщить личные имена и контактные данные этих должностных лиц ведомствам, исполняющим функции и обязанности по защите личной информации.
Статья 53. В случаях, предусмотренных в пункте 2 статьи 3 настоящего закона, операторы личной информации, находящиеся за пределами территории Китайской Народной Республики, создают отдельное юридическое лицо или назначают своего представителя на территории Китайской Народной Республики, на которого возлагается ответственность за решение вопросов, касающихся обрабатываемой личной информации, и должны сообщить название соответствующего юридического лица или личное имя представителя, контактные данные и т. д. ведомствам, исполняющим функции и обязанности по защите личной информации.

Статья 54. Операторы личной информации должны регулярно проводить аудиты своей обработки личной информации и соблюдения законов и административных норм.
Статья 55. Операторы личной информации должны заранее выполнять оценку воздействия на защиту личной информации и регистрировать состояние дел с обработкой при наличии одного из следующих обстоятельств:

1. обработка конфиденциальной личной информации;
2. использование личной информации для автоматизированного принятия решений;
3. перепоручение обработки личной информации, предоставление личной информации другим операторам личной информации или ее раскрытие;
4. предоставление личной информации за границей;
5. другие виды деятельности по обработке личной информации, оказывающие серьезное влияние на физических лиц.

Статья 56. Оценка воздействия на защиту личной информации должна охватывать:

1. проверку законности и необходимости обработки личной информации, ее способа и т. д.;
2. влияние на права и интересы физических лиц, а также риски безопасности;
3. проверку мер защиты на предмет их законности, эффективности и соответствие степени риска.

Отчеты о результатах анализа воздействия на защиту личной информации и отчеты о состоянии дел с обработкой должны храниться не менее трех лет.
Статья 57. В случае утечки, искажения или потери личной информации операторы личной информации должны незамедлительно принять меры по исправлению ситуации и уведомить ведомства, исполняющие функции и обязанности по защите личной информации, а также физических лиц. Уведомление должно содержать следующие сведения:

1. категории информации, причины и возможный ущерб от утечки, искажения или потери информации, которые произошли или могут произойти;
2. меры по исправлению ситуации, принятые оператором личной информации, и меры, которые могут быть приняты физическими лицами для снижения ущерба;
3. контактные данные оператора личной информации.

Оператору личной информации разрешено не уведомлять физических лиц, если он принял меры, позволяющие эффективно предотвратить ущерб от утечки, искажения или потери информации; однако, если ведомства, исполняющие функции и обязанности по защите личной информации, считают, что ущерб может быть причинен, они имеют право потребовать, чтобы оператор личной информации направил уведомление физическим лицам.
Статья 58. Операторы личной информации, предоставляющие важные услуги интернет-платформ, у которых большое количество пользователей и сложные бизнес-модели, должны выполнять следующие обязательства:

1. создать и наладить системы и структуры контроля за защитой личной информации в соответствии с государственными нормами, а также сформировать независимый орган, состоящий преимущественно из сторонних лиц, для надзора за защитой личной информации;
2. соблюдать принципы открытости, справедливости и правомерности; сформулировать правила платформы; уточнить стандарты внутриплатформенной обработки личной информации поставщиками продуктов и услуг и их обязанности по защите личной информации;
3. прекратить предоставление услуг платформы поставщикам товаров или услуг, которые серьезно нарушают законы или административные нормы в отношении обработки личной информации;

4. регулярно публиковать отчеты о социальной ответственности в области защиты личной информации и признавать общественный контроль.

Статья 59. Доверенные лица, принимающие на себя обязанности по обработке личной информации, должны в соответствии с положениями настоящего закона и соответствующих законов и административных норм принимать необходимые меры для обеспечения безопасности личной информации, которую они обрабатывают, и способствовать выполнению предусмотренных в настоящем законе обязательств операторами личной информации.

8. Глава VI. Ведомства, исполняющие функции и обязанности по защите личной информации

Статья 60. Государственное ведомство по кибербезопасности и информатизации отвечает за комплексное планирование и координацию работы по защите личной информации и соответствующей надзорной и управленческой работы. Компетентные ведомства Государственного совета отвечают за работу по защите личной информации, надзору и управлению в рамках своих функций и обязанностей, в соответствии с положениями настоящего закона и соответствующих законов и административных норм. Функции и обязанности по защите личной информации, надзору и управлению компетентных ведомств народных правительств на уровне уездов и выше определяются соответствующими государственными нормами.

Все ведомства, указанные в предыдущих двух пунктах, именуются ведомствами, исполняющими функции и обязанности по защите личной информации.

Статья 61. Ведомства, исполняющие функции и обязанности по защите личной информации, исполняют следующие функции и обязанности по защите личной информации:

1. ведение пропаганды и обучения в области защиты личной информации, а также выполнение руководящей и надзорной роли в отношении работы операторов личной информации;
2. принятие и рассмотрение жалоб и сообщений, касающихся защиты личной информации;
3. проведение оценки состояния дел с защитой личной информации, в том числе используемых процедур, и публикация результатов оценки;
4. проведение расследований и решение вопросов, связанных с незаконной деятельность по обработке личной информации;
5. другие функции и обязанности, предусмотренные в законах или административных нормах.

Статья 62. Государственное ведомство по кибербезопасности и информатизации осуществляет общую координацию следующей работы компетентных ведомств по защите личной информации:

1. выработка конкретных правил и стандартов защиты личной информации;
2. выработка специализированных правил и стандартов защиты личной информации для мелких операторов личной информации, новых технологий и приложений для обработки конфиденциальной личной информации, распознавания лиц, искусственного интеллекта и т. д.;
3. поддержка исследования, разработки и широкого внедрения безопасных и удобных технологий электронной аутентификации личности, стимулирование создания общественных служб аутентификации онлайн-идентичности;
4. стимулирование создания систем обслуживания для организации коллективной работы по защите личной информации и поддержка введения компетентными организациями услуг по оценке и сертификации защиты личной информации;
5. совершенствование рабочих механизмов рассмотрения жалоб и сообщений, касающихся защиты личной информации.

Статья 63. При исполнении своих функций и обязанностей по защите личной информации ведомства, исполняющие функции и обязанности по защите личной информации, имеют право принимать следующие меры:

1. опрашивать заинтересованных сторон и расследовать обстоятельства, связанные с деятельностью по обработке личной информации;
2. ознакомляться и копировать соответствующие договоры, регистрационные записи и квитанции заинтересованной стороны, а также другие материалы, связанные с деятельностью по обработке личной информации;
3. проводить проверки на местах и расследования в связи с предполагаемой незаконной деятельностью по обработке личной информации;
4. осматривать оборудование и предметы, относящиеся к деятельности по обработке личной информации; при наличии доказательств того, что данное оборудование или предметы используются для незаконной деятельности по обработке личной информации, проинформировав в письменном виде основное ответственное лицо своего ведомства и получив одобрение с его стороны, опечатать или конфисковать их.

При исполнении законных функций и обязанностей по защите личной информации ведомствами, исполняющими функции и обязанности по защите личной информации, заинтересованные стороны должны оказывать им содействие и сотрудничать с ними, заинтересованные стороны не имеют права препятствовать их работе или затруднять ее.

Статья 64. При обнаружении ведомствами, исполняющими функции и обязанности по защите личной информации, относительно высоких рисков в деятельности по обработке личной информации или инцидентов безопасности личной информации, они имеют право провести переговоры с юридическим представителем или основным ответственным лицом оператора личной информации в соответствии с распорядительными полномочиями и процедурами или потребовать, чтобы оператор личной информации поручил специализированному учреждению провести аудит соответствия деятельности по обработке личной информации установленным требованиям. Операторы личной информации должны принять меры в соответствии с требованиями для исправления ситуации и устранения уязвимости.

Если при выполнении своих функций ведомства, исполняющие функции и обязанности по защите личной информации, обнаруживают случаи незаконной обработки личной информации и у них возникает подозрение, что это является преступлением, они должны незамедлительно передать дело органам общественной безопасности для рассмотрения в соответствии с законом.

Статья 65. Все организации и физические лица имеют право обращаться в ведомства, исполняющие функции и обязанности по защите личной информации, с жалобами или сообщениями о незаконной деятельности по обработке личной информации. Ведомства, получающие жалобы или сообщения, должны незамедлительно рассматривать их в соответствии с законом и уведомлять лицо, направившее жалобу или сообщение, о результатах.

Ведомства, исполняющие функции и обязанности по защите личной информации, должны публиковать контактные данные для принятия жалоб и сообщений.

Глава VII. Юридическая ответственность

Статья 66. При обработке личной информации в нарушение настоящего закона или невыполнении предусмотренных в настоящем законе обязанностей по защите личной информации во время ее обработки ведомства, исполняющие функции и обязанности по защите личной информации, направляют предписание об устранении нарушений, конфискуют незаконный доход и могут отдать распоряжение о приостановке или

прекращении оказания услуг и использования приложений, незаконно обрабатывающих личную информацию; в случае отказа исправить ситуацию дополнительно взимается штраф не более 1 млн юаней; с непосредственно ответственных лиц и другого непосредственно ответственного персонала взимается штраф от 10 000 до 100 000 юаней. Если обстоятельства совершения незаконных действий, упомянутых в предыдущем пункте, являются серьезными, провинциальные или вышестоящие ведомства, исполняющие функции и обязанности по защите личной информации, направляют предписание об устранении нарушений, конфискуют незаконный доход и взимают штраф не более 50 млн юаней или 5% годового дохода. Они также имеют право отдать распоряжение о приостановке соответствующих видов хозяйственной деятельности или о прекращении хозяйственной деятельности до устранения нарушений и проинформировать соответствующее компетентное ведомство для отзыва соответствующих распорядительных лицензий или аннулирования лицензий на ведение хозяйственной деятельности. С непосредственно ответственных лиц и другого непосредственно ответственного персонала взимается штраф от 100 000 до 1 млн юаней, а также может быть принято решение запретить им в течение определенного срока занимать должности директора, руководителя среднего или высшего звена или должность сотрудника по защите личной информации.

Статья 67. Случаи совершения противоправных действий, предусмотренных в настоящем законе, регистрируются в досье социального рейтинга согласно соответствующим законами и административными нормам и подлежат публикации.

Статья 68. В случае невыполнения государственными органами своих обязанностей по защите личной информации, предусмотренных в настоящем законе, вышестоящие органы или ведомства, исполняющие функции и обязанности по защите личной информации, должны направить предписание об устранении нарушений; на непосредственно ответственных руководителей лиц и других непосредственно ответственных лиц налагаются взыскания в соответствии с законом.

Если персонал ведомств, исполняющих функции по защите личной информации, пренебрегает своими обязанностями, злоупотребляет полномочиями, проявляет фаворитизм, но это не является преступлением, на него должны быть наложены взыскания в соответствии с законом.

Статья 69. Если обработка личной информации нарушает права и интересы в отношении личной информации и приводит к нанесению ущерба, а операторы персональной информации не могут доказать свою невиновность, то они выплачивают компенсацию и берут на себя иную ответственность за данное нарушение.

В вышеуказанном пункте размер компенсации за нарушение определяется, исходя из реально нанесенного физическому лицу ущерба или полученного оператором личной информации дохода. Если реально нанесенный физическому лицу ущерб или полученный оператором личной информации доход трудно оценить, размер компенсации определяется, исходя из практических условий.

Статья 70. Если при обработке личной информации в нарушение положений настоящего закона операторы личной информации ущемляют права и льготы многих физических лиц, народные прокуратуры, законодательно назначенные организации по защите потребителей и организации, назначенные государственными ведомством по кибербезопасности и информатизации, имеют право в соответствии с законом право подать иск в народный суд.

Статья 71. Если нарушение положений настоящего закона является нарушением общественной безопасности, то влечет за собой наказание за нарушение общественной безопасности в соответствии с законом; если оно является преступлением, то влечет за собой уголовную ответственности и проведение расследования в соответствии с законом.

Глава VIII. Дополнительные положения

Статья 72. Настоящий закон не распространяется на физических лиц, обрабатывающих личную информацию в рамках личных или семейных дел.

Если закон содержит положения об обработке личной информации народными правительствами всех уровней, их соответствующими ведомствами и организациями в рамках государственной статистической и архивной деятельности, применяются указанные положения.

Статья 73. В настоящем законе перечисленные ниже термины имеют следующие определения:

1. «Оператор личной информации» — организация или физическое лицо, которое при обработке личной информации самостоятельно определяет цели и способы обработки.
2. «Автоматизированное принятие решений» — использование компьютерных программ для автоматического анализа или оценки личного поведения, привычек, интересов, увлечений, состояния здоровья, финансового, кредитного и иного положения и принятия решений [на основе такого анализа].
3. «Деидентификация» — обработка личной информации, которая обеспечивает невозможность идентификации конкретного физического лица без использования дополнительной информации.
4. «Анонимизация» — обработка личной информации, которая обеспечивает невозможность выделения конкретного физического лица и восстановления исходной информации.

Статья 74. Настоящий закон вступает силу 1 ноября 2021 года.

Приложение 6
Нормы обеспечения безопасности критической информационной инфраструктуры[35] (выдержки)

Статья 2. Критической информационной инфраструктурой в настоящих нормах называется важная сетевая инфраструктура, информационные системы и т. д. важных отраслей и секторов, таких как связь общего пользования и информационные услуги, энергетика, транспорт, водное хозяйство, финансы, общественные услуги, электронное правительство, национальная оборона, наука, технологии, промышленность и т. д., а также информационная инфраструктура, которая в случае уничтожения, потери функциональности или утечки данных может поставить под серьезную угрозу национальную безопасность, национальную экономику и народное благосостояние или общественные интересы.
Статья 8. Компетентные ведомства и ведомства, исполняющие обязанности по надзору и управлению в важных отраслях и секторах, упомянутых в статье 2 настоящих норм, называются ведомствами, отвечающими за работу по обеспечению безопасности критической информационной инфраструктуры (далее сокращено «ведомствами по обеспечению безопасности»).
Статья 9. Ведомства по обеспечению безопасности должны сформулировать правила идентификации критической информационной инфраструктуры, исходя из реальной ситуации в своих отраслях и секторах, и представить их для регистрации в Министерство общественной безопасности Государственного совета.
При определении правил идентификации необходимо главным образом учитывать следующие факторы:

1. степень важности сетевой инфраструктуры, информационной системы и т. д. Для критических и основных видов деятельности в отрасли или секторе;
2. степень возможного ущерба в результате уничтожения, потери функциональности или утечки данных в сетевой инфраструктуре, информационной системе и т. д.;
3. сопутствующее влияние на другие отрасли и секторы.

Статья 18. При возникновении крупных инцидентов кибербезопасности или при обнаружении серьезных угроз кибербезопасности в критической информационной инфраструктуре операторы должны доложить о случившемся ведомству по обеспечению безопасности и органам общественной безопасности согласно соответствующим нормам.
При полном прекращении функционирования критической информационной инфраструктуры или при возникновении препятствий для выполнения ее основных функций, утечке основной национальной информации или других важных данных, относительно широкомасштабной утечке личной информации, нанесении относительно крупного экономического ущерба, распространения противозаконной информации в относительно крупных масштабах, а также при возникновении других аналогичных особенно серьезных инцидентов кибербезопасности или при обнаружении особенно серьезных угроз кибербезопасности ведомство по обеспечению безопасности после получения соответствующего сообщения должно незамедлительно доложить о случившемся национальному ведомству по кибербезопасности и информатизации и Министерству общественной безопасности Государственного совета.

[35] Постановление Государственного совета Китайской Народной Республики № 745, 30 июля 2021 года, http://www.gov.cn/zhengce/content/2021-08/17/content_5631671.htm?trs=1, в переводе DigiChina: https://digichina.stanford.edu/news/translation-critical-information-infrastructure-security-protection-regulations-effective-sept