Научная статья. Политические науки
УДК 327(5)
DOI: 10.31696/2072-8271-2024-2-2-63-195-207

E-GOVERNANCE В ПОДХОДАХ К ОБЕСПЕЧЕНИЮ КИБЕРБЕЗОПАСНОСТИ В АТР (НА ПРИМЕРЕ ТАЙВАНЯ И СИНГАПУРА)

Галина Юрьевна НИКИПОРЕЦ-ТАКИГАВА [1],
Олег Александрович ФИЛАТОВ [2]

[1,2] НИУ ВШЭ, Москва, Россия
[1] gnikiporets-takigawa@hse.ru, https://orcid.org/0000-0002-5611-8396
[2] oafilatov01@mail.ru, https://orcid.org/0009-0004-9777-544X

Аннотация: В статье рассматриваются подходы Тайваня и Сингапура к вопросам развития E-Governance как части национальной стратегии кибербезопасности. В исследовании выявляется текущее стремление к усилению влияния государственных институтов в цифровой среде. Для тайваньской администрации ключевым фактором для проведения данного курса служит внешняя напряженность в отношениях с материковым Китаем, в то время как правительство Сингапура во многом укрепляет внутреннюю стабильность конституционного строя.

Ключевые слова: *E-Governance, кибербезопасность, киберсуверенитет, Тайвань, Сингапур*

Для цитирования: *Никипорец-Такигава Г.Ю., Филатов О.А.* E-Governance в подходах к обеспечению кибербезопасности в АТР (на примере Тайваня и Сингапура) // Юго-Восточная Азия: актуальные проблемы развития, 2024, Том 2, № 2 (63). С. 195–207. DOI: 10.31696/2072-8271-2024-2-2-63-195-207

Original article. Political science

E-GOVERNANCE IN APPROACHES TO ENSURING THE CYBERSECURITY IN APR (CASES OF TAIWAN AND SINGAPORE)

Galina Yu. NIKIPORETS-TAKIGAWA [1], **Oleg A. FILATOV** [2]
[1,2] HSE Universuty, Moscow, Russia
[1] gnikiporets-takigawa@hse.ru, https://orcid.org/0000-0002-5611-8396
[2] oafilatov01@mail.ru, https://orcid.org/0009-0004-9777-544X

Abstract: The paper examines the approaches of Taiwan and Singapore towards e-governance development as a part of national cybersecurity strategy. The study highlights the current drive to strengthen the influence of governmental institutions in the digital area. For the Taiwanese administration, the key factor in this vector is external tension in rela-

tions with mainland China, while the Singaporean government is mainly strengthening the internal stability of the constitutional order.

Keywords: *E-Governance, cybersecurity, cyber sovereignty, Taiwan, Singapore*

For citation: Nikiporets-Takigawa G.Yu., Filatov O.A. E-Governance in Approaches to Ensuring the Cybersecurity in APR (Cases of Taiwan and Singapore). *Yugo-Vostochnaya Aziya: aktual'nyye problemy razvitiya*, 2024, T. 2, № 2 (63). Pp. 195–207. DOI: 10.31696/2072-8271-2024-2-2-63-195-207

Фрагментация киберпространства как часть процесса выстраивания нового мирового порядка

Независимый от государственного контроля и управления интернет в том мировом порядке, в котором глобализация, стирание государственных границ и другие элементы либеральной парадигмы считались жизнеспособными, претендовал на позицию глобального института.

Вопросы управления такого института планировалось передать на уровень ООН и работающих при ней органов, подобных Международному союзу электросвязи (МСЭ)[a], Всемирному Саммиту по управлению информационным обществом (ВВУИО)[b1], Рабочей группе по управлению интернетом[c]; Форуму по управлению интернетом[d].

ВВУИО на первом же саммите в 2003-2005 гг. выработал основополагающую Концепцию будущего управления Интернетом: Тунисские обязательства и Тунисскую программу[23], далее развитую в «Глобальной программе кибербезопасности» МСЭ 2007 г.[4]. Согласно Концепции, управлять интернетом предстояло совместно «органам государственного управления, а также частному сектору, гражданскому обществу, Организации Объединенных Наций и другим межправительственным международным организациям»[5], то есть при помощи всех «заинтересованных сторон, которые сообща и равноправно соби-

[a] *International Telecommunication Union (ITU)*, созданный в 1865 г. и с 1947 г. работающий при ООН.

[b] *World Summit on the Information Society (WSIS)*, поддержанный ООН и начавший работу с 2001 г., впервые проведенный по резолюции Генеральной Ассамблеи ООН в две фазы в 2003 г. в Женеве и в 2005 г. в Тунисе.

[c] *Working Group on Internet Governance (WGIG)*, члены которой были назначены Генеральным секретарем ООН на первом саммите ВВУИО.

[d] *Internet Governance Forum (IGF)*.

рались обеспечивать функционирование интернета как глобального, открытого и свободного института»[6].

Однако попытки организовать более или менее равноправную международную систему управления интернетом не имели успеха. Местонахождение Корпорации по управлению доменными именами и IP-адресами *ICANN*[e]; занимающегося техническими вопросами Инженерного совета интернета[f] и создавшего его в 1986 г. Совета по архитектуре интернета[g]; Общества интернета[h], которое занимается развитием интернета с 1979 г.; а также 70% глобальных платформ подобных *Google, Amazon, Facebook*(*запрещённая на территории Российской Федерации организация*), Apple* (о влиянии которых на мировое лидерство подробнее у И.В. Данилина [7]), приводит к зависимости функционирования интернета от американского государства.

Дж. Вайнберг называет эту ситуацию «провалом демократии»[8], иллюстрируя его историей корпорации *ICAAN*. Она создавалась в 1998 г. Джо Постелем по контракту с американским министерством обороны, но как независимая частная компания, не имеющая управленческой иерархии и развивающаяся коллективными усилиями, практикующая открытые выборы и решения и т.д. Уже с 1999 г. начались спорадические попытки государства вмешаться в работу *ICAAN*, а к 2006 г. оно «принимало активное участие в разработке концепции и окончательном утверждении устава *ICANN*»[9] и настояло на том, чтобы в правлении *ICAAN* были ключевые стейкхолдеры и проводились прямые выборы[10]. В текущей политической ситуации такое отсутствие автономности *ICANN* немедленно проявилось. Несмотря на то, что *ICANN* подчеркивает свой аполитичный статус, заявляя, что «интернет не должен страдать из-за геополитических конфликтов», и даже в 2022 г. отвергла предложение Украины отключить домен России от глобального интернета, Россия, как и целый ряд стран, которые не являются союзниками США и/или находятся под западными санкциями, подвержены риску «разделегирования» доменных зон из-за невозможности проведения платежей и подобных вполне технических причин[11].

[e] The Internet Corporation of Assigned Names and Numbers (Корпорация по управлению доменными именами и IP-адресами).
[f] Internet Engineering Task Force (IETF), созданное в 1986 г. в США открытое международное сообщество проектировщиков, учёных, сетевых операторов и провайдеров, занимающееся развитием протоколов и архитектуры интернета.
[g] Internet Architecture Board (IAB), созданная в 1979 г. в США группа технических советников Общества интернета (ISOC).
[h] Internet Society (ISOC).

Глобальное, безграничное, свободное *per se* киберпространство оказалось подчиненным правилам однополярного мира во главе с США, риторически упакованным в либеральную обертку «глобального института». Как данная риторика, так и практика развития интернета – как «глобального» института и как института под руководством США – в новых политических реалиях активно оспариваются[12].

Во многом примером отказа от делегирования управления цифровой средой на надстрановый уровень служит Китай, который выстроил архитектуру суверенного Интернета. В то же время США и другие страны либерально-демократического курса развития предпринимают шаги по концептуальному противопоставлению своих подходов к обеспечению кибербезопасности политике не только КНР, но и других государств, достигнувших прогресса в формировании независимых подходов по отношению к цифровой среде. Принятая в 2022 г. Декларация о будущем интернета (*Declaration for the Future of the Internet*) формально нацелена на противодействие фрагментации киберпространства, однако фактически разделяет национальных акторов на единомышленников США и оппонентов встроенной в понятие цифровой глобализации монополии государственных институтов США и аффиллированных с ними IT-корпораций на контроль над интернетом. К подписавшим документ государствам относятся США, Канада, Великобритания, страны-члены ЕС, кандидаты на вступление в ЕС, Аргентина, Колумбия, Перу, Австралия, Новая Зеландия, Япония, Тайвань (признается большинством стран частью Китая) и другие представители коллективного запада.

С учетом растущей напряженности в АТР, во многом связанной с курсом США на выстраивание блока сдерживания КНР, формирование коалиции в цифровом пространстве, включающей Тайвань, представляющий одну из ключевых точек эскалации, является заметной тенденцией, которая требует научного анализа. Тайбэй традиционно отмечается на лидирующих позициях в рейтингах конкурентоспособности национальных политик цифровизации *World Digital Competitiveness Ranking*[13]. Сложившееся на острове правительство, не признаваемое абсолютным большинством стран легитимным государственным институтом суверенного национального актора, призвано демонстрировать противоположные принятым в КНР идеи и подходы E-Governance и обеспечения национальной безопасности в цифровой среде.

E-Governance Тайваня: на фоне внешней напряженности

Тайвань выстраивает собственную политику в сфере кибербезопасности. Администрация Тайваня официально осуществляет цифровую трансформацию острова с 1996–1998 гг. Одним из результатов планомерной работы к настоящему моменту стало обеспечение доступа более 90% населения к интернету. С конца 1990-х гг. создание цифровых порталов для предоставления государственных услуг находилось в приоритете тайваньских властей: запускались различные платформы, последней из которых к настоящему времени стал портал «Мое электронное правительство»[14].

С 2017 г. (с принятием обновленной версии в 2020 г.) реализуется программа «Цифровая нация и инновационное экономическое развитие» (*DIGI+2025*)[15]. Цифровое развитие острова должно осуществляться по шести ключевым направлениям: создание инфраструктуры, необходимой для инноваций; подготовка соответствующих специалистов; поддержка межотраслевого внедрения цифровых инноваций; развитие открытого общества в условиях цифровой среды; цифровизация городской среды и укрепление позиций в мировой цифровой экономике[16]. К 2025 г. администрация Тайваня также намерена внедрить облачные вычисления и искусственный интеллект для оптимизации процесса принятия решений и выстраивания работы в соответствии с запросами отдельно взятого пользователя.

Качественному переходу на новую ступень цифрового развития острова способствовала активизация гражданской активности в ходе протестного «Движения подсолнухов» 2014 г., изначально направленного против укрепления торгово-экономических связей с материковым Китаем, а также курса Гоминьдана в целом. Молодые специалисты в сфере цифровых технологий были активно вовлечены в информационное освещение манифестаций. Одним из таких людей является Одри Тан, один из наиболее известных программных разработчиков Тайваня. Основным проектом, запущенным Тан, стала платформа для создания петиций и проведения онлайн-опросов *vTaiwan*, призванная предоставить жителям острова возможность прямого влияния на актуальные политические и социально-экономические вопросы. Можно констатировать, что таким образом продвигалась идея электронной демократии как отдельного направления в рамках развития электронного правительства Тайваня. В 2016 г., с приходом к власти Демократической прогрессивной партии (ДПП), Тан, один из активных участ-

ников и организаторов протестной кампании 2014 г., стал членом Исполнительного Юаня (правительства), где занялся встраиванием гражданской цифровой платформы в систему администрации Тайваня.

При этом платформа *vTaiwan* была впервые использована для проведения консультаций при принятии решений при руководстве партии Гоминьдан. С приходом администрации ДПП *vTaiwan* не получила большего влияния, имея краткосрочное и ограниченное применение в рамках системы тайваньской администрации. К вопросам, которые были санкционированы властями для общественного онлайн-обсуждения, относились проблемы легализации онлайн-продажи алкогольных напитков, а также умышленного распространения третьими лицами фотографий в сети интернет, нарушающих достоинство и честь гражданина[17]. В контексте вопроса кибербезопасности нельзя не отметить, что одним из основных инструментов, используемых платформой *vTaiwa*n для сбора общественного мнения жителей Тайваня, являлась запущенная в США гражданская инициатива – портал *Pol.is*[18].

При этом, с развитием цифровизации на острове, администрация которого выстраивает работу с позиций противодействия влиянию КНР, существенно возрастает роль системы кибербезопасности. С приходом к власти Демократической прогрессивной партии, выступающей за суверенитет Тайваня, в 2001 г. была создана Национальная группа по информационной и коммуникационной безопасности, в обязанности которой входит выстраивание политики в сфере кибербезопасности, отслеживание и противодействие возможных инцидентов. Следующим шагом в институционализации системы национальной безопасности в цифровой среде на острове стоит считать учреждение в 2015 г., при гоминьдановской администрации Ма Инцзю, департамента киберразведки при Национальном бюро безопасности[19]. С возвращением к власти ДПП в лице завершившей работу в мае 2024 г. администрации Цай Инвэнь и нарастанием уровня конфронтации между берегами Тайваньского пролива в течение последних влсьми лет, противодействие дезинформации в киберпространстве было официально закреплено в функционале администрации Тайваня. Для этого в 2022 г. под руководством Одри Тан было создано Министерство цифрового развития, в которое вошла упомянутая выше Национальная группа по информационной и коммуникационной кибербезопасности[20].

Фактическое завершение институционализации системы национальной безопасности в цифровой среде при администрации Цай Ин-

вэнь демонстрирует тенденцию к повышению роли властей в киберпространстве. Продвигаемые активистами-сторонниками ДПП механизмы электронной демократии на Тайване прошли через процесс огосударствления. Одной из наиболее показательных мер в этом контексте представляется запуск администрацией Тайваня собственной платформы *Join*, служащей аналогом разработанной гражданскими активистами *vTaiwan*. Основное заметное отличие правительского портала от гражданской инициативы в том, что петиции и опросы на платформе *Join* касаются бытовых вопросов в отдельных муниципалитетах (изменения расписания транспорта, строительства и ремонта объектов инфраструктуры и т.д.), а также социальной сферы (улучшения трудового законодательства, развития страховых фондов, увеличения площади зеленых насаждений на острове и т.д.)[21]; в то время как на vTaiwan – вопросов развития открытого парламента и вовлеченности жителей в процесс обсуждения и принятия законопроектов[22]. Таким образом, заметно изменение направленности фокуса цифровой демократии на Тайване: администрация Тайваня поддерживает участие общественности в решении текущих социальных вопросов, оставляя гражданские идеи в политической сфере, воспринимаемой как уязвимая для внешнего вмешательства, за рамками обязательного реагирования со стороны руководства острова.

Актуальные новости демонстрируют стремление администрации острова к дальнейшему усилению своей роли в киберпространстве и противодействию влиянию Пекина. Обсуждается принятие поправок к действующим Закону о предотвращении вмешательства и Закону об управлении в сфере кибербезопасности, которые должны расширить функционал Министерства цифрового развития в области отслеживания киберпространства[23]. Здесь очевидны параллели с предложенным в Сенате США Законом об устойчивости кибербезопасности Тайваня, предполагающим углубление сотрудничества США с островом по вопросам цифровой безопасности ввиду конфронтации с Пекином[24]. Также на фоне ведущейся в США кампании по борьбе с ТикТок Министерство цифрового развития Тайваня объявило приложение угрозой национальной безопасности[25]. С учетом сохранения нынешней политики в связи со вступлением в должность руководителя администрации Тайваня Лай Циндэ при одновременном наличии оппозиционного большинства в Законодательном Юане, а также продолжающегося нарастания конфронтации и угроз в отношениях острова и материкового Китая вопрос подхода Тайбэя к обеспечению ки-

бербезопасности в рамках цифровизации будет оставаться одним из ключевых аспектов в региональной безопасности АТР.

E-Governance Сингапура: обеспечение стабильности конституционного строя

На фоне выявленных стремлений Тайваня, который является участником Декларации о будущем интернета (формально призванной противостоять нарастанию фрагментации и контроля «авторитарных» государств в киберпространстве), к фактическому усилению влияния правительства на цифровую среду, выделяется подход Сингапура, который также относится к лидерам мировой цифровизации, согласно *World Digital Competitiveness Ranking*, и, как и Тайвань, частично может считаться территорией китайского цивилизационного влияния (около 75% населения Сингапура – этнические китайцы (хань)[26]). При этом Сингапур не присоединился к продвигаемой США Декларации о будущем интернета и разрабатывает сопоставимые по эффективности с КНР системы защиты киберсуверенитета.

Сингапур проводит цифровую трансформацию с 1980 г., когда была запущена Национальная программа компьютеризации (*National Computerization Programme*). Для осуществления соответствующей политики был создан Национальный компьютерный совет. Впоследствии, в 1999 г., данный орган был объединен с Управлением телекоммуникациями в единое учреждение, отвечавшее за цифровизацию страны – Управление развития инфокоммуникаций. С 2016 г. произошло его преобразование в Агентство технологий при правительстве (*Government Technology Agency – GovTech*)[27]. С 2019 г. в рамках структуры функционируют пять центров, координирующих вопросы кибербезопасности, развитие порталов электронного правительства, продвижение технологий искусственного интеллекта (ИИ), работы государственной инфраструктуры информационно-коммуникационных технологий (ИКТ). Согласно действующему Плану цифрового правительства (*Digital Government Blueprint*), E-Governance Сингапура направлено на облегчение и повышение технологичности бизнес-процессов, переоснащение технологической инфраструктуры, переход от фокуса на предоставлении услуг для граждан и бизнеса к инновационной работе внутри государственного аппарата[28].

Одной из ключевых точек в развитии E-Governance в Сингапуре стоит считать запущенную в 2014 г. платформу *Smart Nation*, которая представляет собой ключевой ресурс оказания многофункциональных государственных услуг[29]. В конструкцию цифрового проекта входит

ряд порталов и приложений: *GoBusiness* (государственная поддержка бизнес-инициатив), *CODEX* (платформа взаимодействия правительства и частных компаний для углубления цифровизации), *E-Payments* (внедрение единой системы оплаты), *National Digital Identity* (цифровая идентификация граждан и предприятий для совершения финансовых транзакций и получения дистанционных государственных услуг), *LifeSG* (получение полного перечня электронных государственных услуг) и т.д.[30].

В контексте рассмотренного выше вопроса развития электронной демократии Тайваня и растущей в связи с этим проблемы монополии правительства на контроль над гражданскими инициативами в цифровом пространстве с целью сохранения национальной безопасности, ситуация в Сингапуре иная. Правительство страны внедряет платформы ограниченного вовлечения граждан в процессы обсуждения и принятия решений по вопросам развития. Одним из основных официальных сервисов служит созданный в 2016 г. *Tech Kaki*[31]. Пользователи имеют право направить предложения или присоединиться к онлайн-дискуссиям, форумам, по вопросам развития цифровых услуг в Сингапуре. В то же время текущие социально-экономические проблемы находятся вне поля общественного обсуждения и могут быть рассмотрены властями по результатам индивидуальных обращений через цифровой сервис электронных государственных услуг *LifeSG*. Таким образом, в отличие от тайваньского правительственного портала *Join*, предусматривающего возможности регистрации петиций и обсуждения бытовых и социальных проблем и предложений, сингапурские государственные сервисы допускают граждан лишь к вопросам цифровизации страны.

Кроме того, при сравнении с Тайванем при анализе проводимой Сингапуром политики могут быть отмечены большая степень ограничения гражданской активности, потенциально способной создать риски для национальной кибербезопасности, и соответствующий более высокий уровень контроля государства за киберпространством. В 2015 г. (в один год с Тайванем) Сингапур создал орган, непосредственно отвечающий за противодействие преступлениям в цифровом пространстве – Агентство кибербезопасности Сингапура[32]. Учреждение отслеживает сообщения о противоправных действиях в интернете, информирует граждан о мерах по их предотвращению. При этом государство получает безграничный доступ к персональным данным пользователей и возможность тотального контроля за своими гражданами.

Этому способствует прямая аффилированность основноготелекоммуникационного оператора страны *SingTel* с государственными учреждениями Сингапура[33]. Компания владеет *Kai Square*, программой отслеживания пользователей через сканирование камеры, получения данных о местоположении и телефонных звонках, доступ к которым осуществляется через используемые гражданами платформы электронных государственных услуг[34].

Не менее существенным инструментом по выстраиванию суверенного контроля над киберпространтвом и обеспечению кибербезопасности является принятый в стране в 2019 г. Закон о защите от обмана и манипуляций в онлайн-среде (*Protection from Online Falsehoods and Manipulation Act – POFMA*). Для реализации мер нормативноправового акта в рамках структуры правительства был создан офис *POFMA*[35]. Под действия закона подпадают ложные утверждения, распространяемые с территории Сингапура в киберпространстве. Согласно анализу зарубежных исследователей, за первые три года действия закона было зафиксировано 67 случаев его применения. По результатам работы офиса *POFMA* в отношении лиц или организаций выносились рекомендации об исправлении или удалении постов. Более того, осуществлялась блокировка страниц в социальных медиа[36].

***

Как было отмечено ранее, шаги в направлении большего регулирования цифровой среды являются современной тенденцией в большинстве государств, стремящихся к обеспечению своего суверенитета и безопасности в киберпространстве. При этом интенсивность принятия мер в этом направлении во многом зависит от типа политического режима того или иного государства или самоуправляемого региона. В то время как Сингапур, где исполнительная и законодательная ветви власти устойчиво контролируются Партией народного действия, утвердил законодательные меры по контролю распространяемой в интернете информации в 2019 г., на Тайване, для которого характерна двухпартийная (с растущей ролью третьей силы) конкуренция за формирование органов власти, по состоянию на первую половину 2024 г. вопрос о принятии соответствующих норм в виде поправок к действующим законодательным актам проходит общественные обсуждения и имеет ограничения для принятия ввиду сложившейся по результатам выборов 2024 г. оппозиционной коалиции в парламенте (Законодательном Юане). Кроме того, заметной является привязка инициатив тайваньских властей к аналогичным мерам в сфе-

ре кибербезопасности, которые предпринимаются в США, что подчеркивает ограниченность независимой политики администрации острова и в сфере защиты национального цифрового пространства.

Таким образом, на основе полученных результатов делаются выводы о том, что: 1) национальные стратегии цифрового развития и кибербезопасности Тайваня и Сингапура обнаруживают пересечения в сходном понимании необходимости противодействия киберугрозам и последовательной институционализации системы кибербезопасности; 2) в связи с данным пониманием общим является и осознание акторами необходимости защиты национального кибепространства; 3) в зависимости от уровня политической самостоятельности и особенностей внутриполитического устройства Тайвань и Сингапур проявляют разные степени интенсивности внедрения мер, направленных на усиление роли правительства в киберпространстве. Несмотря на присоединение к продвигаемой США идее коалиции по формальному противодействию фрагментации цифровой среды, фактически являющейся элементом курса на стратегическое сдерживание Китая, остров Тайвань демонстрирует схожие с неподписавшим Декларацию о будущем интернета 2022 г. Сингапуром тенденции в политике в отношении контроля над киберпространством, являющиеся частью глобального процесса выделения национальных сегментов мировой сети. Данные выводы приводят к заключению о том, что по пути КНР, впервые разработавшей разветвленную стратегию и идеологию управления в сфере Интернета, готовы частично двигаться другие представители АТР, некоторые из которых исторически официально противопоставляют себя Пекину.

ИНФОРМАЦИЯ ОБ АВТОРАХ

НИКИПОРЕЦ-ТАКИГАВА Галина Юрьевна, доктор политических наук, профессор, Факультет мировой экономики и мировой политики, НИУ ВШЭ, Москва, Россия

ФИЛАТОВ Олег Александрович, ассистент, Факультет мировой экономики и мировой политики, НИУ ВШЭ, Москва, Россия

Вклад авторов: все авторы сделали эквивалентный вклад в подготовку публикации. Авторы заявляют об отсутствии конфликта интересов.

Статья поступила в редакцию 30.04.2024;
одобрена после рецензирования 16.05.2024;
принята к публикации 31.05.2024.

INFORMATION ABOUT THE AUTHORS

Galina Yu. NIKIPORETS-TAKIGAWA, DSc (Political Science), Professor, HSE University, Moscow, Russia

Oleg A. FILATOV, Assistant, Faculty of World Economy and International Relations, HSE University, Moscow, Russia

Contributions of the authors: the authors contributed equality to this article. The authors declare no conflicts of interests.

The article was submitted 30.04.2024;
approved 16.05.2024;
accepted to publication 31.05.2024.

[1] WSIS Outcome documents. ITU. 2005. URL: https://www.itu.int/net/wsis/outcome/booklet.pdf
[2] Tunis Agenda for the Information Society. ITU. 2005. URL: https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html
[3] Tunis Commitment. ITU. 2005. URL: https://www.itu.int/net/wsis/docs2/tunis/off/7.html
[4] Глобальная программа кибербезопасности (ГПК), Global Cybersecurity Agenda (GCA) // МСЭ. 2007. URL: https://www.ifap.ru/pr/2008/080908aa.pdf
[5] Tunis Commitment. ITU. 2005. URL: https://www.itu.int/net/wsis/docs2/tunis/off/7.html
[6] WSIS+10 Statement on the Implementation of WSIS Outcomes. ITU. 2014. URL:https://www.itu.int/net/wsis/review/inc/docs/final/wsis10.statement.pdf
[7] Данилин И.В. Влияние цифровых технологий на лидерство в глобальных процессах: от платформ к рынкам // Вестник МГИМО-Университета. 2020;13(1):100-116. https://doi.org/10.24833/2071-8160-2020-1-70-100-116
[8] Weinberg, Jonathan, Non-State Actors and Global Informal Governance - The Case of ICANN (June 7, 2010). International Handbook on Informal Governance, Thomas Christiansen, Christine Neuhold, eds., Forthcoming, Wayne State University Law School Research Paper No. 10-05, URL: https://ssrn.com/abstract=1621862. DOI:4337/9781848445611/00023
[9] Weinberg, Jonathan, Non-State Actors and Global Informal Governance... P. 17.
[10] Weinberg, Jonathan, Non-State Actors and Global Informal Governance... P. 2.
[11] Никипорец-Такигава Г.Ю. Интернет как политический институт в новых политических реалиях: зарубежный опыт. Политические институты в современном мире: коллапс или перезагрузка? / Сборник материалов по итогам Всероссийской научной конференции. Санкт-Петербург. 2023. С. 217-219.: 217.
[12] Никипорец-Такигава Г.Ю. Интернет как политический институт... С. 218-219.
[13] World Digital Competitiveness Ranking 2023. URL: https://www.imd.org/centers/wcc/world-competitiveness-center/rankings/world-digital-competitiveness-ranking/
[14] 我的E政府 Мое электронное правительство. Официальный сайт. URL: https://www.gov.tw/
[15] Digital Government Program 2.0 of Taiwan (2021-2025). National Development Council, 2020. P. 1-44.
[16] Digital Government Program 2.0 of Taiwan (2021-2025).
[17] 違反本人意願而散布本人的身體私密影像 [Распространение личных изображений тела против своей воли]. vTaiwan URL: https://vtaiwan.tw/topic/nonconsensual-pornography/
[18] Horton C. The Simple but Ingenious System Taiwan Uses to Crowdsource Its Laws // MIT Technology Review. URL: https://www.technologyreview.com/2018/08/21/240284/the-simple-but-ingenious-system-taiwan-uses-to-crowdsource-its-laws/
[19] Huang H. A Collaborative Battle in Cybersecurity? Threats and Opportunities for Taiwan // Asia Policy, 2020, 15(2). P. 101-106.
[20] 數位發展部 [Министерство цифрового развития. Официальный сайт]. URL: https://moda.gov.tw/aboutus/introduction/404
[21] Join [Официальный сайт]. URL: https://join.gov.tw/
[22] VTaiwan Working Group General Info. URL: https://g0v.hackmd.io/@tmonk/rJHYWR9S4/%2Ff9c4pS_TQjClh0g6wCJ8iw?type=book&fbclid=IwAR2bodPbII7xN-nMJtaYSaxAJY24Hy_fwH3i60hi257Ysnoxg4wHB7klyiM
[23] Taiwan's Digital Ministry Proposes Modest Amendment to Cyber Security Management Act // BGA Taiwan. URL: https://bowergroupasia.com/taiwans-digital-ministry-proposes-modest-amendment-to-cyber-security-management-act/
[24] Taiwan Cybersecurity Resiliency Act of 2023 // Congress.gov. URL: https://www.congress.gov/bill/118th-congress/senate-bill/1241
[25] TikTok Classified in Taiwan as National Security Threat: Minister (March 22, 2024) // Focus Taiwan. URL: https://focustaiwan.tw/politics/202403220009
[26] Астафьева Е. М. Новое в национальной классификации сингапурцев // Юго-Восточная Азия: актуальные проблемы развития, 2011, №. 17. С. 304-315
[27] Cybersecurity. GovTech Singapore. URL: https://www.tech.gov.sg/singapore-digital-government-journey/cybersecurity
[28] Cybersecurity. GovTech Singapore.
[29] Singapore's Smart Nation Initiative – A Policy and Organisational Perspective. Lee Kuan Yew School of Public Policy. URL: https://lkyspp.nus.edu.sg/docs/default-source/case-studies/singapores-smart-nation-initiative-final_112018.pdf?sfvrsn=354e720a_2

[30] GovTech Singapore [Официальный сайт]. URL: https://www.tech.gov.sg/
[31] Tech Kaki Community. GovTech Singapore. URL: https://www.tech.gov.sg/products-and-services/tech-kaki-community/
[32] Singapore Cyber Emergency Response Team [Официальный сайт]. URL: https://www.csa.gov.sg/Explore/who-we-are/our-identity/about-singcert
[33] History of Temasek // Temasek. URL: https://www.temasek.com.sg/en/about-us/history-of-temasek#portfolio
[34] Iaroshenko I. E-Government in Singapore: strengthening political control over society. Lund University, 2016. P. 77.
[35] Protection from Online Falsehoods and Manipulation Act. POFMA. URL: https://www.pofmaoffice.gov.sg/regulations/protection-from-online-falsehoods-and-manipulation-act/
[36] Tan N., & Preece C. Democratic Backsliding in Illiberal Singapore // Asian Journal of Comparative Politics, 2024, 9(1). P. 25-49. DOI: https://doi.org/10.1177/20578911221141090