

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ,
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 004

DOI: 10.17212/2782-2230-2024-2-25-54

ОТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
К НАЦИОНАЛЬНОЙ: ПРОТИВОБОРСТВО
ИТ-КОМПАНИЙ США И КНР*

Ю.Ю. ПЕТРУНИН¹, В.В. БУХАРИН²

¹ 119991, РФ, г. Москва, Ломоносовский проспект, 27, корпус 4, Московский государственный университет имени М.В. Ломоносова, доктор философских наук, профессор, заведующий кафедрой «Математические методы и информационные технологии в управлении». E-mail: petrunin@spa.msu.ru

² 119991, РФ, г. Москва, Ломоносовский проспект, 27, корпус 4, Московский государственный университет имени М.В. Ломоносова, кандидат исторических наук, доцент кафедры «Математические методы и информационные технологии в управлении». E-mail: bukharin@spa.msu.ru

В статье исследуются отдельные аспекты деятельности крупных ИТ-компаний, тесно связанные с проблемой информационной безопасности, обеспечения цифрового суверенитета как основы национальной безопасности. Особое внимание уделено борьбе транснациональных ИТ-корпораций США и КНР за альтернативные рынки сбыта, а также ряду ограничений, налагаемых на них законами иностранных государств. Основываясь на исследовании официальных документов американских и китайских государственных органов и ИТ-корпораций, а также материалов СМИ, авторы приходят к выводу, что геополитические интересы США и КНР соприкасаются с целями крупного бизнеса и вынуждают правительства прибегать к различного рода запретам и протекционистским мерам. ИТ-корпорации США и Китая, разработчики мессенджеров и социальных сетей уделяют недостаточно внимания вопросам информационной безопасности своих клиентов.

Ключевые слова: информационная безопасность, ИТ-корпорации, национальная безопасность, информационная война, цифровой суверенитет, Microsoft, Google, ByteDance, TikTok, WeChat, WhatsApp, Zoom, кибербезопасность

* Статья получена 16 мая 2024 г.

ВВЕДЕНИЕ

В современном мире влияние транснациональных компаний на национальные государства многократно возросло. Геополитические интересы США и КНР сталкиваются и переплетаются с целями крупного бизнеса. Наиболее ярко это проявляется в чрезвычайно быстро развивающейся ИТ-сфере. Деятельность крупных технологических компаний, обладающих огромными массивами данных своих клиентов и ресурсами для продвижения собственных интересов, выносит на повестку дня вопросы обеспечения информационной безопасности, влияния корпорации на национальную безопасность государства и их участия в информационных войнах. В рамках настоящей публикации предпринята попытка исследовать деятельность наиболее крупных корпораций ИТ-сферы США и Китая, разработчиков и владельцев мессенджеров, социальных сетей, что свидетельствует о новизне представленного исследования. В качестве методологической основы изучения этой проблемы были использованы принципы объективности и историзма, реализованные при анализе деятельности ИТ-компаний США и Китая. В соответствии с этими принципами был изучен широкий круг источников, среди которых наибольшее значение имели официальные документы американских и китайских корпораций, нормативно-правовые акты США и КНР, документы Министерства финансов США, Федеральной торговой комиссии США, Конгресса и Сената США, Министерства общественной безопасности КНР, Государственной канцелярии интернет-информации КНР, материалы американских и китайских СМИ, в том числе официального журнала Федерального правительства США Federal Register.

В отечественной и зарубежной историографии нет специальных работ, посвященных этой теме. Исследователи сосредоточили внимание на таких тематически близких проблемах, как информационный, цифровой и киберсуверенитет [1, 2], на различных аспектах национальной безопасности, геополитическом противостоянии США и КНР [3, 4], информационной войне [5], политике кибербезопасности [6–8], регулировании сети Интернет [9], а также отдельных вопросах кибербезопасности продуктов ИТ-корпораций [10].

ОСНОВНАЯ ЧАСТЬ

Информационная война – явление достаточно сложное и многогранное. Она может вестись как между блоками государств или отдельными странами, так и на уровне бизнеса, компаний. Цели информационных войн также могут очень сильно отличаться: от решения конкретных бизнес-задач до глобального доминирования в системе международных отношений, фор-

мирования однополярного мира. Исследование участия IT-корпораций в информационных войнах [5] представляет особый интерес, поскольку охватывает, по сути, все уровни, весь спектр проблем. В феврале 2019 года в разгар торговой войны между Соединенными Штатами Америки и Китайской Народной Республикой началась информационная война против социальной сети для обмена короткими видео в TikTok, принадлежащей пекинской компании ByteDance. США объявили TikTok угрозой национальной безопасности. Компания ByteDance была оштрафована Федеральной торговой комиссией (FTC) США. Одним из первых обвинений, выдвинутых в адрес TikTok со стороны американских политиков и бизнесменов, был сбор информации о пользователях – детях до 13 лет. На официальном сайте Федеральной торговой комиссии 27 февраля 2019 года было опубликовано заявление, что TikTok согласилась заплатить 5,7 млн долл. в целях урегулирования ситуации [11].

Юридическим продолжением конфликта между США и Китаем в информационной сфере стал опубликованный в августе 2020 года указ Президента США Дональда Трампа (2017–2021), предписывающий американским фирмам прекратить бизнес-сотрудничество с мобильной коммуникационной системой WeChat [12], разработанной компанией Tencent. Приложение WeChat используется во всём мире. Трамп обвинил WeChat в сборе «огромных массивов» личных данных пользователей, что, по его мнению, являлось угрозой безопасности американцев. Китайские пользователи WeChat расценили блокировку приложения, являющегося ярким примером технологических инноваций в Китае, как нападение на «свою культуру, свой народ» и государство. В ответ на решение Трампа Министерство иностранных дел Китая обвинило США в использовании проблемы национальной безопасности в качестве прикрытия для осуществления гегемонии. Действия президента США нанесли серьезный удар не только по крупной китайской IT-корпорации, но и повлияли на общественное мнение в Китае. Аудитория этого приложения насчитывает миллиард пользователей. WeChat – не только платформа социальных сетей, но и инструмент для решения множества повседневных задач, таких как покупки, игры, знакомства людей и др. Популярность приложения, по мнению ряда экспертов, связана с аналогичным запретом в Китае многих западных платформ, где с 2003 года в рамках проекта «Золотой щит» или «Великий китайский файрвол» [13] начали осуществлять фильтрацию содержимого интернета.

Одной из наиболее крупных западных корпораций, столкнувшихся с юридическими ограничениями, направленными на поддержку китайской информационной безопасности и информационного суверенитета [2], стала американская транснациональная корпорация Google, которая пыталась про-

никнуть на китайский IT-рынок. В 2006 году корпорация объявила, что она запустит китайские версии своих поисковых и новостных веб-сайтов, которые будут подвергать цензуре материалы в соответствии с законами КНР. «Google.cn будет соблюдать местные китайские законы и правила» [14], – говорилось в заявлении. «Решая, как лучше всего подойти к китайскому – или любому другому – рынку, мы должны сбалансировать наши обязательства по удовлетворению интересов пользователей, расширению доступа к информации и реагированию на местные условия» [14], – подчеркивал Google.

Подобным образом поступили и другие IT-корпорации. Например, Microsoft удалила блоги и заблокировала запросы пользователей со словами «независимость Тайваня», «Тибет», «Далай-лама», «Фалуньгун», «терроризм» и «резня» на платформе для создания онлайн-журналов и блогов MSN Spaces [15], сославшись на свою политику соблюдения «местных законов».

Поисковая система Bing, разработанная и принадлежавшая Microsoft, в 2009 году не только осуществляла цензурированные поисковые запросы в Китае, но и, как обнаружил блогер портала New York Times Николас Кристоф, цензурировала все поисковые запросы, в которых использовались упрощенные китайские иероглифы, чаще всего применяемые в материковом Китае, в Сингапуре и среди студентов, изучающих китайский язык в других странах. По его мнению, эта «самоцензура», превзошла аналогичные действия корпорации Google. Политика Google заключалась в том, чтобы отображать результаты поиска на Google.com без цензуры в любой точке мира вне зависимости от того, используется ли китайский язык, но цензурировать результаты поиска на сайте google.cn после выхода серии публикаций этого блогера компания Microsoft признала наличие проблемы, но отрицала преднамеренность [16] своих действий. В 2010 году googl.com в Китае был заблокирован и американская корпорация вынуждена была уйти с китайского рынка.

В данный период ограничения в Китае были введены в отношении социальной сети Facebook, принадлежавшей корпорации Facebook (признана в России экстремистской организацией и запрещена), которая после ребрендинга 2021 года стала называться Meta Platforms (признана в России экстремистской организацией и запрещена) [17]. Социальная сеть была заблокирована в КНР после июльских беспорядков 2009 года в Урумчи в связи с тем, что активисты движения за независимость Синьцзяна использовали Facebook как часть своей коммуникационной сети. Facebook отрицал предоставление информации активистам [18]. В 2014 году в Китае была заблокирована социальная сеть Instagram (признана в России экстремистской организацией и запрещена), также принадлежащая компании Meta. Ее блокировку связывают с демонстрациями в Гонконге против политики китайских властей, с так

называемой «революцией зонтиков». Местные жители выкладывали в социальную сеть видео- и фотоматериалы, на которых были запечатлены столкновения протестующих с полицией. В отдельных китайских СМИ была опубликована информация о прекращении работы Instagram в КНР, однако о реальных причинах блокировки и протестах не сообщалось [19]. Примечательно, что эта транснациональная корпорация была заинтересована в освоении китайского рынка IT. Согласно информации, опубликованной в The New York Times, Facebook в 2015 году заблокировал около 55 000 единиц контента примерно в 20 странах [20]. Непосредственно для Китая, сообщалось в газете, разрабатывалось дополнительное программное обеспечение, позволяющее осуществлять более глубокую фильтрацию контента, включая новостные ленты. Автор статьи предположил, что данное программное обеспечение будет доступно партнерской китайской компании, которая получит «полный контроль над тем, должны ли эти сообщения отображаться в лентах пользователей» [20]. Официального комментария относительно планов Facebook не последовало.

Важно отметить, что 27 декабря 2015 года был принят «Закон о противодействии терроризму Китайской Народной Республики», в рамках которого ужесточался контроль за иностранными средствами массовой информации [21]. Согласно данному закону поставщики интернет-услуг и операторы связи должны предоставить технические интерфейсы, дешифрование и другую поддержку правоохранительным органам для борьбы с террористической деятельностью в соответствии с законодательством КНР. В законе также предусматривались меры по контролю над содержанием китайского интернет-трафика. Еще одним шагом Китая, направленным на укрепление национальной безопасности [8] в целом и информационной в частности, стал опубликованный 7 ноября 2016 года «Закон о кибербезопасности Китайской Народной Республики» [22]. Важно отметить, что среди положений этого закона были зафиксированы новые правила хранения данных операторами критической информационной инфраструктуры. Согласно статье 37 личная информация или важные данные должны храниться на территории материкового Китая. Несмотря на то что закон предполагал возможность передачи данных за рубеж («в связи с требованиями бизнеса»), этот алгоритм в законе не был детализирован. В документе отсутствовало также четкое определение «критически важной информационной инфраструктуры». В законе отмечалось, что в некоторых случаях сбор данных может осуществляться только с разрешения правительства Китая. Закон неоднократно подвергался критике со стороны западной прессы. По мнению некоторых американских аналитиков, «Закон о кибербезопасности Китайской Народной Республики» может быть «уязвим» для злоупотребления со стороны китайского правительства. Кроме того, ино-

странные фирмы оказались в неравном положении с китайскими и обязаны нести дополнительные финансовые издержки.

The Wall Street Journal в начале 2017 года отмечала, что Facebook предпринял множество попыток для возвращения в Китай. Однако, по мнению авторов статьи, некоторое время казалось, что шансы вернуться на китайский рынок IT изменились к лучшему, когда власти Пекина предоставили Facebook лицензию, позволяющую открыть представительство в двух офисных башнях в столице [23]. Вместе с тем можно сделать вывод, что подобные «успехи» были мнимыми, поскольку разрешение было выдано на очень короткий срок (3 месяца) и корпорация Facebook им не воспользовалась.

Важно отметить, что Китай попытался также заблокировать возможные пути обхода введенных ограничений. Считается, что наиболее распространенным способом преодоления блокировки для доступа к западным мессенджерам и соцсетям является использование технологии VPN (от англ. virtual private network – «виртуальная частная сеть») [24]. Согласно информации, опубликованной в американских и гонконгских СМИ, в марте 2016 года во время заседания высшего законодательного органа КНР «Всекитайского собрания народных представителей» в Пекине VPN-сервисы в Китае были заблокированы.

«Многие компании жаловались, что их платные VPN-сервисы не функционировали почти неделю» [25]. Министерство информации и технологий Китая объявило, что VPN-сервисы должны получить лицензию от регуляторов [26]. Подобные меры автоматически ограничили использование западных VPN-сервисов в Китае, сделав многие из них нелегальными. Необходимо отметить, что ограничения касались не самой технологии VPN, которая часто используется в корпоративном секторе, а VPN-анонимайзеров, применяемых во многих странах для обхода различных блокировок. Дальнейшая борьба с VPN продолжилась и в 2018 году, когда крупнейшие провайдеры страны China Mobile, China Unicom и China Telecom заблокировали доступ к VPN [25]. А 31 марта в Китае был введен полный запрет на использования VPN. Несмотря на то что ряд экспертов отмечали важность принятого закона, поставившего, по их мнению, окончательную точку в борьбе с использованием VPN для обхода ограничений, на момент его принятия многие сервисы уже были заблокированы [27].

Ограничения коснулись не только социальной сети Facebook, принадлежащей одноименной корпорации, но и приобретенного ею в 2014 году мессенджера WhatsApp. Он был заблокирован в 2017 году. По мнению газеты New York Times, это было связано с «усилением слежки в преддверии большого собрания Коммунистической партии» [28]. Отключение мессенджера для материкового Китая стало серьезным ударом для IT-гиганта. Незадолго до

этих событий исполнительный директор Facebook Марк Цукерберг настаивал на возвращении мессенджера на китайский рынок и интенсивно изучал китайский язык [29].

New York Times делала акцент на защищенность WhatsApp от контроля китайских цензоров. Действительно, в приложении присутствует функция так называемого сквозного шифрования. Однако утверждение, что владельцы Facebook не могут получить доступ к текстовым, голосовым и видеосообщениям, проходящим через их серверы, выглядит не вполне обоснованным, поскольку в том же году стало широко известно о наличии «бекдора»¹ в этом приложении, который позволяет компании подменить ключи шифрования и потребовать от приложения-отправителя повторно зашифровать все сообщения и отправить, используя новые ключи [30]. Когда подобная информация стала широко известна, то возник вопрос, насколько действия со стороны США правомочны. В ответ на запрос от сенатора Дж. Рона Уайдена [31] правительство США заявило, что не нуждается в судебном решении для осуществления слежки и может попросить технологическую компанию создать бэкдор в шифровании [10]. Правительство до настоящего времени руководствовалось разделом 702 «Закона о надзоре за внешней разведкой» [32] для осуществления основной части своих операций по сбору разведанных и наблюдению. Применение полномочий, предоставляемых этим законом, давало право правительству требовать от технологических компаний специально обходить шифрование в своих продуктах.

Подобный способ обхода шифрования был некогда встроен и в принадлежащий Microsoft мессенджер Skype, а также не стоит забывать о программе PRISM [33], к которой присоединилась Microsoft еще в 2011 году [34]. Следует отметить, что сама компания до сих пор отрицает наличие свободного доступа со стороны спецслужб к информации своих серверов благодаря данной программе. По утверждению компании Microsoft, PRISM [1, с. 86] – «это не добровольная программа, а внутренняя правительственная компьютерная система для обработки целевых данных, собранных в соответствии с действующими законами» [35]. Microsoft также приводит заявление директора национальной разведки, который, поясняя ситуацию с PRISM, ссылаясь на уже упомянутый раздел 702 «Закона о надзоре за внешней разведкой» [36].

В актуальном лицензионном соглашении WhatsApp (дата вступления в силу: 4 января 2021 г.) сказано, что, «являясь одной из компаний Meta, WhatsApp получает информацию от других компаний Meta и предоставляет информацию другим компаниям Meta» [37]. На практике это означает, что Facebook получит

¹ От англ. back door – «черный ход» или «тайный ход», позволяющий получить несанкционированный доступ к данным.

доступ к номерам телефонов, сведениям о транзакциях и IP-адресам пользователей. Следовательно, полученные данные могут быть использованы не только в коммерческих интересах компании и переданы третьим лицам, но и в информационной войне, создавая угрозу национальной безопасности.

Социальная сеть Facebook уже давно стала площадкой информационной войны. По словам В.Б. Вехова, эксперта в области информационной безопасности, профессора кафедры юриспруденции интеллектуальной собственности и судебной экспертизы МГТУ им. Баумана, «Facebook изначально являлся не только коммерческим проектом, но и проектом, направленным на ведение информвойны, поскольку финансировался за счет денежных средств фонда Сороса. Соответственно, в условиях, когда необходимо применять один из элементов информационного оружия, он и был применен» [38]. М.Г. Делягин – доктор экономических наук, депутат ГД РФ, член научного совета при Совете Безопасности РФ – отметил, что «поднимал вопрос о необходимости блокировки Facebook, откровенно русофобского политического инструмента» [39]. Проблема заключается не только в том, что США используют Facebook в информационной войне против государств (таких как РФ или КНР) и организуют с его помощью цветные революции, но и подвергают опасности персональные данные каждого пользователя, конкретного человека. При этом США позиционируют себя как главного в мире защитника интересов и свободы личности.

Несмотря на тот факт, что наиболее известной иллюстрацией подобной угрозы является скандал, связанный с компанией Cambridge Analytica, которая использовала данные более 50 млн пользователей Facebook, чтобы влиять на избирателей перед голосованием по Brexit, следует прежде всего обратить внимание на события, произошедшие в 2021 году, являющиеся примером использования исключительно технических уязвимостей. Так, 3 апреля 2021 года, согласно информации, опубликованной на страницах Insider, 533 млн телефонных номеров и личных данных пользователей Facebook «утекли» в Интернет [40]. Подобные угрозы невозможно ликвидировать запретом зарубежных компаний, однако дополнительный контроль и аудит безопасности может уменьшить вероятность их возникновения. Несмотря на масштаб проблемы, противодействие подобным угрозам представляется достаточно сложной задачей, особенно если учитывать, что коммерческий интерес в деятельности социальных сетей превалирует над интересами национальной безопасности. Случаи, аналогичные описанному на страницах Insider, представляют для владельцев соцсетей исключительно репутационные риски, но не оказывают достаточно серьезного влияния на финансовое состояние владеющих ими корпораций. Среди стран, пострадавших от утечки, только в Ирландии была предпринята попытка применить экономические инстру-

менты. Так, в середине апреля 2021 года ирландская юридическая фирма Digital Rights Ireland (DRI) объявила о подаче иска против Facebook за утечки данных миллионов пользователей социальной сети. Ирландская фирма предложила всем пострадавшим присоединиться к иску против цифрового гиганта [41]. С этой целью была создана интернет-страница, позволяющая зарегистрироваться и принять участие в иске [42].

Еще один интересный случай противостояния в сети Интернет связан с компанией Zoom Video Communications. Zoom (приложение для видеоконференц-связи, значительно увеличило свою аудиторию в 2020 году во время введения карантина (пандемии COVID-19)) использовали и продолжают использовать миллионы людей для работы и проведения общественных мероприятий. Например, в марте 2020 года премьер-министр Великобритании Борис Джонсон опубликовал на своей странице в соцсети Twitter фотографию, на которой он председательствовал на заседании Кабинета министров через приложение [43].

Компания Zoom Video Communications основана выходцем из Китая Эриком Юань и базируется в США. Есть основание предполагать, что приложение Zoom было разработано тремя компаниями в Китае, каждая из которых имела название Ruanshi Software, две из них принадлежали непосредственно компании Zoom, третья – компании American Cloud Video Software Technology Co., Ltd. [44]. Косвенно приведенные факты легко подтвердить, если обратить внимание на данные регистрационной формы S-1², согласно которой на конец января 2019 года в Китае штат программистов Zoom составлял 500 человек [45]. Согласно документам американской Комиссии по ценным бумагам, в 2020 году Zoom нанимал через свои филиалы в Китае не менее 700 сотрудников, которые занимались «исследованиями и разработками» [46]. Zoom неоднократно блокировал пользователей по запросу китайского правительства, а согласно официальному заявлению, опубликованному в июле 2020 года, Zoom разрабатывал технологию, которая позволила бы компании удалять или блокировать пользователя на основе их географического расположения по запросу местных властей, когда публикации пользователей являлись незаконными в их юрисдикции [47].

В сети в настоящее время распространилась непроверенная информация, что «Zoom подтвердил, что Zoom.us теперь доступен в Китае в дополнение к Zoom.com. Данные местных пользователей Китая будут храниться в центрах обработки данных Zoom, расположенных в Китае, и этим пользователям также потребуется ввести действительный номер мобильного телефона для

² Форма S-1 SEC – первоначальная регистрационная форма для новых ценных бумаг, требуемая Комиссией по ценным бумагам и биржам США.

использования Zoom» [48]. По сообщениям, опубликованным в «Сообществе Zoom» [49], можно сделать вывод, что международная версия сайта на момент публикации настоящей статьи была заблокирована. Официальная служба поддержки приложения на сообщения пользователей о проблемах с использованием Zoom в КНР не отвечала. Проанализировав информацию, опубликованную в «Сообществе Zoom», и публикации в СМИ, можно сделать вывод, что пользователи имели возможность присоединяться к конференции, но им была недоступна функция «создать конференцию». Возможность создавать конференции существовала только у владельцев «премиальной» подписки, которую было возможно приобрести у местного дилера. Все китайские пользователи могли присоединиться к любой конференции Zoom в Гонконге и за рубежом, а также в материковом Китае, используя URL-адрес приглашения или идентификатор конференции. (Пользователям из материкового Китая необходимо предоставить номер телефона, чтобы подтвердить свою личность и присоединиться к собранию.)

Введение жестких ограничений на использование зарубежных мессенджеров полностью согласуется с информационной политикой КНР, направленной на защиту информационной безопасности. Важно отметить, что даже китайские WeChat, Weibo, Baidu Tieba не избежали проверки на соблюдение «закона о контенте» [50]. Информация о проведении расследования в отношении упомянутых компаний была опубликована на официальном сайте Администрации киберпространства Китая (CAC) – государственного органа, контролирующего содержание китайского сегмента интернета [51]. Представляется важным упомянуть «Положение о надзоре и проверке интернет-безопасности органами общественной безопасности», которое было принято Министерством общественной безопасности КНР 5 сентября 2018 года (обнародовано и вступило в силу 1 ноября 2018 г.). Этот документ наделил правоохранительные органы полномочиями на доступ (в том числе удаленный) и копирование данных, имеющих отношение к кибербезопасности [52].

На момент выхода приложение Zoom имело серьезные недостатки в системе безопасности, включая уязвимость, которая позволяла злоумышленнику удалять участников собраний, подделывать сообщения от пользователей и использовать общие экраны. Это вызвало вопрос: насколько безопасно его использовать для правительственных заседаний. В настоящей статье мы не ставим своей задачей проанализировать уязвимости приложения, а рекомендуем читателю обратиться к тематическим публикациям. Например, к статье в журнале *Forbes*, опубликованной в 2020 году под названием «Все “дыры” Zoom: чем рискуют пользователи самого популярного сервиса видеоконференций эпохи карантина» [53]. Популярность Zoom сделала его лакомым объектом как для хакеров, так и для государственных структур США. Как и мно-

гие западные ресурсы, Zoom небезопасен и может быть использован не только хакерами, но и спецслужбами в глобальном информационном противостоянии. Даже если не вдаваться в конспирологические теории, забыть на какой-то момент про информационные войны, а просто внимательно изучить «заявление о конфиденциальности» [54], то можно заметить, что Zoom продолжает передавать информацию рекламным партнерам (например, Google Ads и Google Analytics), а реальная защита информации обеспечивается исключительно для госучреждений США, поскольку их данные размещены на территории США в отдельном облаке, сертифицированном в рамках Федеральной программы управления рисками и авторизацией (FedRAMP).

В документации Zoom также присутствует ряд неясных заявлений о шифровании. В некоторых документах и приложении Zoom говорится о том, что платформа в настоящее время использует сквозное (E2E) шифрование [55], однако согласно официальному пояснению, опубликованному в блоге компании Zoom, корпорация дает собственную трактовку данного термина, далекую от общепринятой [44]. Важно отметить, что использование «сквозного шифрования», согласно инструкции [56], требует дополнительных манипуляций от самого пользователя. Таким образом, можно сделать вывод, что сквозное шифрование может оказаться не более чем маркетинговым ходом.

Действия Китая по отношению к американским корпорациям не являются уникальными, как это часто изображается в западных СМИ. В той или иной степени к подобным мерам прибегали и другие страны. Так, Facebook кроме Китая заблокировали Северная Корея, Мьянма, Иран, Куба, Россия, Туркменистан [9].

В 2020 году правительство США объявило, что рассматривает возможность запрета китайской социальной сети TikTok, принадлежащей ByteDance. Министерство обороны и Пентагон запретили использовать данную социальную сеть военным [57]. Примечательно, что ранее военные США размещали в соцсети рекламный контент для привлечения в свои ряды новых рекрутов [58]. В августе Трамп подписал указы [59], запрещавшие американским компаниям заключать какие-либо сделки с китайской компанией ByteDance, вынуждая компанию продать TikTok. В ответ на действия Трампа 24 августа 2020 года в окружной суд Центрального округа Калифорнии был подан иск, в котором утверждалось, что указ был мотивирован стремлением президента укрепить свою поддержку на выборах благодаря протекционистским мерам, направленным против Китая [60]. В иске также подчеркивалось, что TikTok и ByteDance были лишены права на справедливое процессуальное обеспечение в соответствии с пятой поправкой, которая распространяется на иностранные и местные компании;

что президентский указ не предоставил доказательств реальной угрозы, исходящей от TikTok, для безопасности страны, а также достаточного обоснования для данного запрета. TikTok протестовал против применения устаревшей декларации о чрезвычайной ситуации от мая 2019 года относительно «обеспечения цепочки поставок информационных и коммуникационных технологий и услуг». В иске утверждалось, что предполагаемая угроза для национальной безопасности, выявленная Комитетом по иностранным инвестициям США (CFIUS), была основана на устаревших данных и не учитывала предоставленные TikTok документы [61].

В 2020–2021 годах несколько крупных американских компаний рассматривали возможность приобретения как самого TikTok, так и технологий, используемых компанией ByteDance [62]. Корпорация Microsoft выразила намерение о приобретении алгоритма работы TikTok, а также некоторых других технологий, связанных с искусственным интеллектом. Согласно информации, опубликованной телеканалом CNBC, сумма обсуждаемой сделки могла составить от 20 до 30 млн долл. [63]. Несмотря на давление [3, с. 20] со стороны правительства США, ByteDance сохранила независимость, отказав американской компании [64].

Администрация президента Дж. Байдена 9 июня 2021 года издала указ «Защита конфиденциальных данных американцев от иностранных противников» («ЕО 14034») [65]. Документ отменил три указа, изданных администрацией Трампа, которые фактически запрещали использование некоторых китайских приложений в США, включая TikTok и WeChat. Несмотря на отмену этих законов, в документе было подчеркнуто, что в соответствии с «Указом 13873» [66] «Китайская Народная Республика, среди прочего, продолжает угрожать национальной безопасности, внешней политике и экономике Соединенных Штатов». Документ призвал федеральные агентства продолжить широкую проверку приложений, «принадлежащих или контролируемых иностранным противником» [66].

Законодатели США 13 декабря 2022 года представили в Конгресс проект закона, который запрещал использование TikTok и позволял вводить санкции против медиакомпаний, подконтрольных определенным странам. По мнению авторов, этот закон должен был защитить американцев от угрозы со стороны социальных сетей Китая, России и ряда других иностранных государств (или находящихся под их влиянием) [67]. Разработчиками закона являлись сенатор Марко Рубио (республиканец от штата Флорида), а также члены Палаты представителей Конгресса США Майк Галлахер (республиканец от штата Висконсин) и Раджа Кришнамурти (демократ от штата Иллинойс). Законодатели в качестве угрозы национальной безопасности отмечали, что по китайскому законодательству компания обязана предоставить эти приложения

Коммунистической партии Китая (КПК). В опубликованном пресс-релизе отмечалось, что «от директора ФБР до комиссаров FCC и экспертов по кибербезопасности все ясно дали понять о риске использования TikTok для слежки за гражданами США» [67]. Президент Джо Байден 30 декабря 2022 года подписал закон о запрете TikTok на «государственных устройствах». Закон запретил установку и использование TikTok на всех (с некоторыми исключениями) устройствах федерального правительства и государственных корпораций и предписывал удалить TikTok там, где он уже установлен [68]. Согласно информации, опубликованной телеканалом NBC, «администрация Байдена пригрозила потенциальным запретом популярного приложения для социальных сетей в США, если его китайские владельцы откажутся продавать свои доли в нем» [69]. Авторы репортажа также недвусмысленно намекнули, что именно позиция администрации Байдена стала причиной начатого 17 марта 2023 года ФБР и Министерством юстиции США официального расследования фактов шпионажа за американскими журналистами.

В начале марта 2023 года в Сенат США был представлен «Закон об ограничении» [70]. Законопроект требовал от федерального правительства принять меры по обнаружению и устранению угроз, исходящих из-за границы, в отношении продуктов и услуг в сфере информационно-коммуникационных технологий, таких как приложения для социальных сетей. В законопроекте было подчеркнуто, что «Министерство торговли должно выявлять, сдерживать, срывать, предотвращать, запрещать, расследовать и смягчать последствия транзакций, связанных с продуктами и услугами ИКТ, в которых любой иностранный противник (такой как Китай) имеет какой-либо интерес и которые представляют неоправданный или неприемлемый риск для национальной безопасности США или безопасности граждан США» [70]. Через год в США был принят «Закон о защите американцев от приложений, контролируемых иностранными противниками» (HR 7521) [71]. Из закона следовало, что если TikTok в течение полугода не сменит владельца и останется частью китайской компании ByteDance, то его заблокируют в США. Согласно информации, опубликованной в The Wall Street Journal, правительство Китая «сигнализировало» компании ByteDance, что предпочтет запрет в США продаже социальной сети [72].

ЗАКЛЮЧЕНИЕ

В современном мире происходит борьба транснациональных IT-компаний за альтернативные рынки сбыта, а также новых клиентов. Стратегия различных транснациональных компаний в IT-сфере имеет достаточно много общих

черт вне зависимости от страны происхождения бизнеса. Корпорации, стремясь максимизировать свою прибыль, пытаются всеми возможными способами потеснить конкурентов, достичь технологического преимущества [4]. Ради достижения этой цели они готовы мириться с некоторыми ограничениями, налагаемыми на них законами иностранных государств.

Как показывает проведенный анализ, корпорации уделяют недостаточно внимания вопросам информационной безопасности своих клиентов. Данные пользователей постоянно находятся в зоне риска. Важно отметить, что инциденты, связанные с утечкой персональных данных, происходят достаточно часто, однако материальный и репутационный ущерб для крупных компаний не является фатальным. Заявления ряда компаний о высокой степени защиты данных (например, об использовании сквозного шифрования) не в полной мере соответствуют действительности, часто являются маркетинговым ходом.

Правительства США и Китая прибегают к различного рода ограничениям и протекционистским мерам, оказывая поддержку собственному крупному бизнесу. Для США это коррелируется с защитой национальной безопасности, поскольку лидерство США, обеспечиваемое в IT-сфере крупными корпорациями, трактуется данной страной как основной способ обеспечения ее национальной безопасности. В погоне за глобальным доминированием США стремятся взять под свой контроль информационное пространство других государств.

США и Китай уделяют достаточно много внимания своей информационной безопасности, обеспечению цифрового суверенитета как основы национальной безопасности. В их подходе к решению этой задачи есть как общие черты, так и принципиальные различия. Оба государства активно внедряют информационно-коммуникационные технологии в социально-экономическую жизнь страны, но при этом стремятся ограничить доступ к данным своих граждан со стороны иностранных держав.

Принципиальные различия в подходе к обеспечению информационной безопасности между Соединенными Штатами Америки и Китаем касаются трех ключевых аспектов: свободы интернета, места и роли государства в области информационной безопасности, сотрудничества и обмена информацией [6] с другими странами и международными организациями в области кибербезопасности. США декларируют защиту прав граждан на свободный доступ к информации и свободу выражения мнения в сети. Такой подход объясняется доминированием американских IT-корпораций, контролируемых американским правительством и спецслужбами, в то время как в Китае интернет цензурируется и контролируется государством, что в значительной степени является ответом на внешние угрозы. Например, торго-

вая война с США стимулировала усиление информационного контроля в Китае. Обеспечение информационной безопасности в США в значительной степени возлагается на частный бизнес, коммерческие компании. В Китае государство играет центральную роль в контроле и регулировании информационной безопасности, а также принимает более строгие меры для мониторинга и контроля интернета. США активно сотрудничают с другими странами и международными организациями в области кибербезопасности. Китай также осуществляет сотрудничество, например, в рамках ООН или БРИКС [7], однако в менее широком формате в связи с особенностями политики контроля над информацией.

СПИСОК ЛИТЕРАТУРЫ

1. Бухарин В.В. Компоненты цифрового суверенитета Российской Федерации как техническая основа информационной безопасности // Вестник МГИМО-Университета. – 2016. – № 6 (51). – С. 76–91. – DOI: 10.24833/2071-8160-2016-6-51-76-91.
2. Moore G.J. Huawei, cyber-sovereignty and liberal norms: China's challenge to the west/democracies // Journal of Chinese Political Science. – 2023. – Vol. 28 (1). – P. 151–167. – DOI: 10.1007/s11366-022-09814-2.
3. Цветкова Н., Сытник А. Цифровое противостояние США и КНР: экономическое и политическое измерения // Мировая экономика и международные отношения. – 2023. – Т. 67, № 11. – С. 15–23. – DOI: 10.20542/0131-2227-2023-67-11-15-23.
4. Гамза Л.А. Технологическое противостояние США и Китая в Европе // Мировая экономика и международные отношения. – 2021. – Т. 65, № 7. – С. 98–105.
5. Каткова Е.Ю., Юнюшкина А.С. Китайские концепции и возможности в информационной войне: соперничество КНР и США в киберпространстве // Вестник РУДН. Серия: Всеобщая история. – 2022. – Т. 14, № 2. – С. 197–210. – DOI: 10.22363/2312-8127-2022-14-2-197-210.
6. Julian N. United States' and China's cybersecurity policies: collaboration or confrontation? // The Sigma Iota Rho (SIR) Journal of International Relations. – 2021. – January 24. – URL: <https://www.sirjournal.org/research/2021/1/24/united-states-and-chinas-cybersecurity-policies-collaboration-or-confrontation> (accessed: 29.05.2024).
7. Бухарин В.В. Кибербезопасность БРИКС // Государственное управление Российской Федерации: повестка дня власти и общества. Материалы

XVI Международной конференции (31 мая – 02 июня 2018 г.). – М., 2019. – С. 552–559.

8. *Cheung T.M.* The rise of China as a cybersecurity industrial power: balancing national security, geopolitical, and development priorities // *Journal of Cyber Policy*. – 2018. – Vol. 3 (3). – P. 306–326. – DOI: 10.1080/23738871.2018.1556720.

9. *Курьлев К.П., Пархитько Н.П., Смолик Н.Г.* Национальные режимы регулирования сети интернет в странах СНГ // *Постсоветские исследования*. – 2021. – Т. 4, № 8. – С. 705–718. – DOI: 10.24412/2618-7426-2021-8-705-718.

10. *Endeley R.E.* End-to-end encryption in messaging services and national security – case of Whatsapp messenger // *Journal of Information Security*. – 2018. – Vol. 9 (1). – P. 95–99. – DOI: 10.4236/jis.2018.91008.

11. Video social networking app Musical.ly agrees to settle FTC allegations that it violated children's privacy law // *Federal Trade Commission*. – 2019. – February 27. – URL: <https://www.ftc.gov/news-events/press-releases/2019/02/video-social-networking-app-musically-agrees-settle-ftc> (accessed: 29.05.2024).

12. *Zhaoyin F., Cheetham J.* Trump WeChat ban 'an unwelcome signal' for Chinese community // *BBC*. – 2020. – August 10. – URL: <https://www.bbc.com/news/world-asia-china-53686507> (accessed: 09.01.2024).

13. *Shen X.* The story of China's Great Firewall, the world's most sophisticated censorship system // *South China Morning Post*. – 2019. – November 7. – URL: <https://www.scmp.com/abacus/who-what/what/article/3089836/story-chinas-great-firewall-worlds-most-sophisticated> (accessed: 29.05.2024).

14. *Mills E.* Google to censor China Web searches // *CNET*. – 2006. – January 25. – URL: <https://www.cnet.com/news/google-to-censor-china-web-searches/> (accessed: 29.05.2024).

15. *Watts J.* Microsoft helps China to censor bloggers // *The Guardian*. – 2005. – June 15. – URL: <https://www.theguardian.com/technology/2005/jun/15/newmedia.microsoft> (accessed: 29.05.2024).

16. *Kristof N.* Microsoft and Chinese Censorship // *The New York Times*. – 2009. – June 24. – URL: <https://archive.nytimes.com/kristof.blogs.nytimes.com/2009/06/24/microsoft-and-chinese-censorship/?searchResultPosition=6> (accessed: 29.05.2024).

17. Информация по делу № 02-2473/2022 // Официальный портал судов общей юрисдикции г. Москвы. – URL: <https://mos-gorsud.ru/rs/tverskoj/services/cases/civil/details/de7ea6a0-a3ab-11ec-8a7e-51b31fb55b35?participants=meta> (дата обращения: 29.05.2024).

18. 80 pct of netizens agree China should punish Facebook // People's Daily Online. – 2009. – July 10. – URL: <https://en.people.cn/90001/90776/90882/6697993.html> (accessed: 01.08.2020).

19. Коцар Ю., Бевза Д. Протесты лишили Китай Instagram // Газета.Ru – 2014. – 29 сентября. – URL: https://www.gazeta.ru/tech/2014/09/29_a_6240045.shtml (дата обращения: 29.05.2024).

20. Isaac M. Facebook said to create censorship tool to get back into China // The New York Times. – 2016. – November 22. – URL: <https://www.nytimes.com/2016/11/22/technology/facebook-censorship-tool-china.html> (accessed: 29.05.2024).

21. Counter-Terrorism Law (as amended in 2018) // China Law Translate. – URL: <https://www.chinalawtranslate.com/en/counter-terrorism-law-2015/> (accessed: 29.05.2024).

22. Creemers R., Webster G., Triolo P. Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017) / Stanford Cyber Policy Center. – URL: <https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/> (accessed: 29.05.2024).

23. Abkowitz A., Seetharaman D., Dou E. Facebook is trying everything to Re-Enter China – and it's not working // The Wall Street Journal. – 2017. – January 30. – URL: <https://www.wsj.com/articles/mark-zuckerbergs-beijing-blues-1485791106> (accessed: 29.05.2024).

24. Economy E.C. The great firewall of China: Xi Jinping's internet shutdown // The Guardian. – 2018. – June 29. – URL: <https://www.theguardian.com/news/2018/jun/29/the-great-firewall-of-china-xi-jinpings-internet-shutdown> (accessed: 29.05.2024).

25. Ye J. China tightens Great Firewall by declaring unauthorised VPN services illegal // South China Morning Post. – 2017. – January 23. – URL: <https://www.scmp.com/news/china/policies-politics/article/2064587/chinas-move-clean-vpns-and-strengthen-great-firewall> (accessed: 29.05.2024).

26. How Web-connected is China? / ChinaPower. – URL: <https://chinapower.csis.org/web-connectedness> (accessed: 29.05.2024).

27. China's internet underground fights for its life // Bloomberg. – URL: <https://www.bloomberg.com/news/articles/2018-03-01/china-s-internet-underground-fights-for-its-life> (accessed: 29.05.2024).

28. Bradsher K. China blocks WhatsApp, broadening online censorship // The New York Times. – 2017. – September 25. – URL: <https://www.nytimes.com/2017/09/25/business/china-whatsapp-blocked.html> (accessed: 29.05.2024).

29. *Mozur P.* China disrupts WhatsApp service in online clampdown // The New York Times. – 2017. – July 18. – URL: <https://www.nytimes.com/2017/07/18/technology/whatsapp-facebook-china-internet.html> (accessed: 29.05.2024).

30. WhatsApp design feature means some encrypted messages could be read by third party // The Guardian. – 2017. – January 13. – URL: <https://www.theguardian.com/technology/2017/jan/13/whatsapp-design-feature-encrypted-messages> (accessed: 29.05.2024).

31. *Whittaker Z.* US says it doesn't need secret court's approval to ask for encryption backdoors // ZDNet. – 2017. – December 7. – URL: <https://www.zdnet.com/article/us-says-it-does-not-need-courts-to-approve-encryption-backdoors/> (accessed: 29.05.2024).

32. FISA questions (July 2017). Wyden's encryption backdoor question // Web archive. – URL: <https://web.archive.org/web/20230106172742/https://www.documentcloud.org/documents/4320971-FISA-questions-July-2017.html> (accessed: 29.05.2024).

33. *Gellman B., Lindeman T.* Inner workings of a top-secret spy program // Washington Post. – 2013. – June 29. – URL: <https://web.archive.org/web/20170830105407/https://apps.washingtonpost.com/g/page/national/inner-workings-of-a-top-secret-spy-program/282/> (accessed: 29.05.2024).

34. Microsoft handed the NSA access to encrypted messages / G. Greenwald, E. MacAskill, L. Poitras, S. Ackerman, D. Rushe // The Guardian. – 2013. – July 12. – URL: <https://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data> (accessed: 29.05.2024).

35. Microsoft. About our practices and your data – URL: <https://blogs.microsoft.com/datalaw/our-practices/#did-participate-in-prism-program> (accessed: 29.05.2024).

36. Facts on the collection of intelligence pursuant to Ection 702 of the Foreign Intelligence Surveillance Act // Office of the Director of National Intelligence. – URL: <https://www.dni.gov/files/documents/Facts%20on%20the%20Collection%20of%20Intelligence%20Pursuant%20to%20Section%20702.pdf> (accessed: 30.05.2024).

37. Политика конфиденциальности WhatsApp // WhatsApp. – URL: <https://www.whatsapp.com/legal/updates/privacy-policy?eea=0#privacy-policy-updates-how-we-work-with-other-facebook-companies> (дата обращения: 30.05.2024).

38. Вехов: Facebook – инструмент информационной войны // Sputnik Молдова. – 2019. – 18 февраля. – URL: <https://md.sputniknews.ru/20190218/vekhov->

facebook-instrument-informatsionnoy-voyny-24775421.html (дата обращения: 30.05.2024).

39. Мы можем закрыть Facebook уже завтра. Как России не проиграть в информационной войне? / Михаил Делягин. – URL: <https://delyagin.ru/articles/192-deljagina-tsitirujut/90483-my-mozhem-zakryt-fa-ebook-uzhe-zavtra-kak-rossii-ne-proigrat-v-informatsionnoy-voyne> (дата обращения: 14.03.2024).

40. *Holmes A.* 533 million Facebook users' phone numbers and personal data have been leaked online // Business Insider. – 2021. – April 3. – URL: https://www.businessinsider.com/stolen-data-of-533-million-facebook-users-leaked-online-2021-4?utm_source=notification&utm_medium=referral (accessed: 30.05.2024).

41. Press release: Thousands expected to sue Facebook in mass action against privacy breach // Digital Rights Ireland. – 2021. – April 16. – URL: <https://www.digitalrights.ie/facebook-breach/> (accessed: 30.05.2024).

42. DRI Facebook action // Digital Rights Ireland. – URL: <https://www.digitalrights.ie/facebook/> (accessed: 30.05.2024).

43. *Wakefield J.* Coronavirus: Zoom is in everyone's living room – how safe is it? // BBC. – 2020. – 27 March. – URL: <https://www.bbc.com/news/technology-52033217> (accessed: 14.03.2024).

44. *Marczak B., Scott-Railton J.* Move fast and roll your own crypto. A quick look at the confidentiality of zoom meetings // Citizen Lab. – 2020. – April 3. – URL: <https://citizenlab.ca/2020/04/move-fast-roll-your-own-crypto-a-quick-look-at-the-confidentiality-of-zoom-meetings/> (accessed: 30.05.2024).

45. FORM S-1. Zoom Video Communications, Inc. March 22, 2019 // The United States Securities and Exchange Commission. – URL: <https://www.sec.gov/Archives/edgar/data/1585521/000119312519083351/d642624dsl.htm> (accessed: 30.05.2024).

46. Zoom Video Communications US SEC Form 10-K (2020, 31 January) // Internet Archive. – URL: <https://web.archive.org/web/20200511122414/https://investors.zoom.us/static-files/09a01665-5f33-4007-8e90-de02219886aa> (accessed: 30.05.2024).

47. Zoom. Improving our policies as we continue to enable global collaboration. – URL: <https://www.zoom.com/en/blog/improving-our-policies-as-we-continue-to-enable-global-collaboration/> (accessed: 30.05.2024).

48. Zoom access from China // University of California, Santa Barbara. – URL: <https://help.lsit.ucsb.edu/hc/en-us/articles/360042172231-Zoom-Access-from-China> (accessed: 14.03.2024).

49. "China support, my China colleagues cannot enter zoom meeting, why?" // Zoom Community. – URL: <https://community.zoom.com/t5/Meetings/China-support-my-china-colleagues-cannot-enter-zoom-meeting-why/m-p/139630> (accessed: 30.05.2024).

50. Chinese regulator launches probe into Tencent, Weibo and Baidu // Bloomberg. – 2017. – 11 August. – URL: <https://www.bloomberg.com/news/articles/2017-08-11/chinese-regulator-starts-probe-into-tencent-weibo-and-baidu> (accessed: 30.05.2024).

51. 腾讯微信、新浪微博、百度贴吧涉嫌违反《网络安全法》被立案调查 // 中央网络安全和信息化委员会办公室 中华. – URL: http://www.cac.gov.cn/2017-08/11/c_1121467425.htm (accessed: 30.05.2024).

52. 公安机关互联网安全监督检查规定 (公安部令第151号) // 中华人民共和国公安部 版权所有. – URL: <https://www.mps.gov.cn/n6557558/c6263180/content.html> (проверено 14.03.2024 г.).

53. Жукова К. Все «дыры» Zoom: чем рискуют пользователи самого популярного сервиса видеоконференций эпохи карантина // Forbes. – 2020. – 23 апреля. – URL: <https://www.forbes.ru/tehnologii/398629-vse-dyry-zoom-chem-riskuyut-polzovateli-samogo-populyarnogo-servisa> (дата обращения: 30.05.2024).

54. Zoom. Заявление о конфиденциальности // Zoom Video Communications. – URL: <https://explore.zoom.us/ru/privacy/> (дата обращения: 30.05.2024).

55. Kaspersky Team. Сквозное шифрование: что это и зачем оно нужно вам // Блог Касперского. – URL: <https://www.kaspersky.ru/blog/what-is-end-to-end-encryption/29075/> (проверено 14.03.2024 г.).

56. Сквозное шифрование (E2EE) конференций // Zoom Поддержка. – URL: https://support.zoom.com/hc/en/article?id=zm_kb&sysparm_article=KB0065408 (дата обращения: 30.05.2024).

57. Rosenblatt K. Army bans TikTok following guidance from the Pentagon // NBC News. – 2019. – December 31. – URL: <https://www.nbcnews.com/tech/tech-news/u-s-army-bans-tiktok-following-guidance-pentagon-n1109001> (accessed: 30.05.2024).

58. Makena K. The Army is in hot water over TikTok recruiting activity // The Verge. – 2021. – December 15. – URL: <https://www.theverge.com/2021/12/14/22834405/tiktok-army-marco-rubio-ban-report-government-personal-devices> (accessed: 30.05.2024).

59. Regarding the acquisition of Musical.ly by ByteDance Ltd. A Presidential Document by the Executive Office of the President on 08/14/2020 //

U.S. Department of the Treasury. – URL: <https://home.treasury.gov/system/files/136/EO-on-TikTok-8-14-20.pdf> (accessed: 30.05.2024).

60. *Pettersson E., Glovin D., Brody B.* TikTok sues Trump to challenge U.S. Government restrictions // Bloomberg. – 2020. – 24 August. – URL: <https://www.bloomberg.com/news/articles/2020-08-24/tiktok-says-it-s-suing-u-s-over-ban-claims-no-security-threat> (accessed: 30.05.2024).

61. Why we are suing the Administration // TikTok. – 2020. – 24 August. – URL: <https://newsroom.tiktok.com/en-us/tiktok-files-lawsuit> (accessed: 30.05.2024).

62. *Wells G., Tilley A.* Oracle wins bid for TikTok in U.S., beating Microsoft // The Wall Street Journal. – 2020. – September 14. – URL: <https://www.wsj.com/articles/microsoft-drops-out-of-bidding-for-tiktoks-u-s-operations-11600039821> (accessed: 30.05.2024).

63. *Sherman A., Repko M.* TikTok likely to announce sale of U.S. operations in the coming days in \$20 billion to \$30 billion range // CNBC. – 2020. – 27 August. – URL: <https://www.cnbc.com/2020/08/27/tiktok-likely-to-announce-sale-us-operations-in-the-coming-days.html> (accessed: 30.05.2024).

64. Microsoft statement on TikTok // Official Microsoft Blog. – URL: <https://blogs.microsoft.com/blog/2020/09/13/microsoft-statement-on-tiktok/> (accessed: 30.05.2024).

65. Executive Order 14034 of June 9, 2021. Protecting Americans' Sensitive Data from Foreign Adversaries // Federal Register. – URL: <https://www.federalregister.gov/d/2021-12506> (accessed: 30.05.2024).

66. Executive Order 13873 of May 15, 2019. Securing the Information and Communications Technology and Services Supply Chain // Federal Register. – URL: <https://www.federalregister.gov/d/2019-10538> (accessed: 30.05.2024).

67. Rubio, Gallagher introduce bipartisan legislation to ban TikTok // Senator Rubio. – URL: <https://www.rubio.senate.gov/rubio-gallagher-introduce-bipartisan-legislation-to-ban-tiktok/> (accessed: 14.03.2024).

68. S.1143 – No TikTok on government devices Act // United States Congress. – URL: <https://www.congress.gov/bill/117th-congress/senate-bill/1143> (accessed: 30.05.2024).

69. *Dilanian K., Shabad R.* The DOJ and FBI are investigating TikTok over allegations that employees spied on journalists // NBC. – 2023. – March 18. – URL: <https://www.nbcnews.com/politics/justice-department/doj-fbi-are-investigating-tiktok-allegations-employees-spied-journalis-rcna75497> (accessed: 30.05.2024).

70. S.686 – Restrict Act // United States Congress. – URL: <https://www.congress.gov/bill/118th-congress/senate-bill/686> (accessed: 30.05.2024).

71. H.R.7521 – Protecting Americans from Foreign Adversary Controlled Applications Act // United States Congress. – URL: <https://www.congress.gov/bill/118th-congress/house-bill/7521> (accessed: 30.05.2024).

72. Huang R. China signals opposition to forced sale of TikTok in the U.S. // The Wall Street Journal. – 2024. – March 15. – URL: <https://www.wsj.com/tech/tiktok-ban-chinese-owners-bytedance-1a857a06> (accessed: 30.05.2024).

Петрунин Юрий Юрьевич, доктор философских наук, профессор, заведующий кафедрой «Математические методы и информационные технологии в управлении» факультета государственного управления Московского государственного университета имени М.В. Ломоносова, руководитель секции «Управление знаниями» Научного совета РАН по методологии искусственного интеллекта, руководитель Центра анализа больших данных в общественных науках. Область научных интересов: искусственный интеллект, нейрокompьютинг, анализ данных, наукометрия. Имеет более 150 публикаций. E-mail: petrunin@spa.msu.ru

Бухарин Владислав Викторович, кандидат исторических наук, доцент кафедры «Математические методы и информационные технологии в управлении» факультета государственного управления Московского государственного университета имени М.В. Ломоносова. Область научных интересов: информационная безопасность, национальная безопасность, международные отношения, геополитика, история Великобритании. E-mail: bukharin@spa.msu.ru

DOI: 10.17212/2782-2230-2024-2-25-54

From information security to national security: the confrontation between us and chinese IT-companies*

Yu.Yu. Petrunin¹, V.V. Bukharin²

¹ Lomonosov Moscow State University, 27/4 Lomonosov Prospekt, Moscow, 119991, Russian Federation, DSc (Philosophical Sciences), professor, head of the mathematical methods and information technology in management department. E-mail: petrunin@spa.msu.ru

² Lomonosov Moscow State University, 27/4 Lomonosov Prospekt, Moscow, 119991, Russian Federation, Ph.D. (Historical Sciences), associate professor of the mathematical methods and information technology in management department. E-mail: bukharin@spa.msu.ru

The article examines certain aspects of the activities of large IT-companies that are closely related to the problem of information security, ensuring digital sovereignty as the basis of national security. Special attention is paid to the struggle of transnational IT-corporations of the USA and China for alternative markets, as well as a number of restrictions imposed on them by the laws of foreign countries. Based on a study of official documents of American and Chinese government agencies and IT-corporations, as well as media materials, the authors conclude that the geopolitical interests of the United States and China are in contact with the goals of big business and force governments to resort to various kinds of prohibitions and protectionist measures. IT-corporations in the USA and China, developers of messengers and social networks do not pay enough attention to the information security of their users.

Keywords: information security, IT-corporations, national security, information warfare, digital sovereignty, Microsoft, Google, ByteDance, TikTok, WeChat, WhatsApp, Zoom, cybersecurity

REFERENCES

1. Bukharin V.V. Komponenty tsifrovogo suvereniteta Rossiiskoi Federatsii kak tekhnicheskaya osnova informatsionnoi bezopasnosti [The Russian's digital sovereignty as a technical basis of information security]. *Vestnik MGIMO-Universiteta = MGIMO Review of International Relations*, 2016, no. 6 (51), pp. 76–91. DOI: 10.24833/2071-8160-2016-6-51-76-91.
2. Moore G.J. Huawei, cyber-sovereignty and liberal norms: China's challenge to the west/democracies. *Journal of Chinese Political Science*, 2023, vol. 28 (1), pp. 151–167. DOI: 10.1007/s11366-022-09814-2.
3. Tsvetkova N., Sytnik A. Tsifrovoe protivostoyanie SShA i KNR: ekonomicheskoe i politicheskoe izmereniya [Digital confrontation between USA and China:

* Received 16 May 2024.

economic and political dimensions]. *Mirovaya ekonomika i mezhdunarodnye otnosheniya* = *World Economy and International Relations*, 2023, vol. 67, no. 11, pp. 15–23. DOI: 10.20542/0131-2227-2023-67-11-15-23.

4. Gamza L.A. Tekhnologicheskoe protivostoyanie SShA i Kitaya v Evrope [Technological confrontation between USA and China in Europe]. *Mirovaya ekonomika i mezhdunarodnye otnosheniya* = *World Economy and International Relations*, 2023, vol. 65, no. 7, pp. 98–105. DOI: 10.20542/0131-2227-2021-65-7-98-105.

5. Katkova E.Yu., Yunyushkina A.S. Kitaiskie kontseptsii i vozmozhnosti v informatsionnoi voine: sopernichestvo KNR i SShA v kiberprostranstve [Chinese strategies and opportunities in information warfare: China–US rivalry in cyberspace]. *Vestnik RUDN. Seriya: Vseobshchaya istoriya* = *RUDN Journal of World History*, 2022, vol. 14 (2), pp. 197–210. DOI: 10.22363/2312-8127-2022-14-2-197-210.

6. Julian N. United States' and China's cybersecurity policies: collaboration or confrontation? *The Sigma Iota Rho (SIR) Journal of International Relations*, 2021, January 24. Available at: <https://www.sirjournal.org/research/2021/1/24/united-states-and-chinas-cybersecurity-policies-collaboration-or-confrontation> (accessed 29.05.2024).

7. Bukharin V.V. [BRICS cybersecurity]. *Gosudarstvennoe upravlenie Rossiiskoi Federatsii: povestka dnya vlasti i obshchestva* [Public administration of the Russian Federation: the agenda of government and society]. Proceedings of the XVI International Conference (May 31 – June 02, 2018). Moscow, 2019, pp. 552–559. (In Russian).

8. Cheung T.M. The rise of China as a cybersecurity industrial power: balancing national security, geopolitical, and development priorities. *Journal of Cyber Policy*, 2018, vol. 3 (3), pp. 306–326. DOI: 10.1080/23738871.2018.1556720.

9. Kurylev K.P., Parkhitko N.P., Smolik N.G. Natsional'nye rezhimy regulirovaniya seti internet v stranakh SNG [National internet regulatory regimes in the CIS countries]. *Postsovetskie issledovaniya* = *Journal Post-Soviet Studies*, 2021, vol. 4 (8), pp. 705–718. DOI: 10.24412/2618-7426-2021-8-705-718.

10. Endeley R.E. End-to-end encryption in messaging services and national security – case of Whatsapp messenger. *Journal of Information Security*, 2018, vol. 9 (1), pp. 95–99. DOI: 10.4236/jis.2018.91008.

11. Video social networking app Musical.ly agrees to settle FTC allegations that it violated children's privacy law. *Federal Trade Commission*, 2019, February 27. Available at: <https://www.ftc.gov/news-events/press-releases/2019/02/video-social-networking-app-musically-agrees-settle-ftc> (accessed 29.05.2024).

12. Zhaoyin F., Cheetham J. Trump WeChat ban 'an unwelcome signal' for Chinese community. *BBC*, 2020, August 10. Available at: <https://www.bbc.com/news/world-asia-china-53686507> (accessed 09.01.2024).

13. Shen X. The story of China's Great Firewall, the world's most sophisticated censorship system. *South China Morning Post*, 2019, November 7. Available at: <https://www.scmp.com/abacus/who-what/what/article/3089836/story-chinas-great-firewall-worlds-most-sophisticated> (accessed 29.05.2024).

14. Mills E. Google to censor China Web searches. *CNET*, 2006, January 25. Available at: <https://www.cnet.com/news/google-to-censor-china-web-searches/> (accessed 29.05.2024).

15. Watts J. Microsoft helps China to censor bloggers. *The Guardian*, 2005, June 15. Available at: <https://www.theguardian.com/technology/2005/jun/15/newmedia.microsoft> (accessed 29.05.2024).

16. Kristof N. Microsoft and Chinese Censorship. *The New York Times*, 2009, June 24. Available at: <https://archive.nytimes.com/kristof.blogs.nytimes.com/2009/06/24/microsoft-and-chinese-censorship/?searchResultPosition=6> (accessed 29.05.2024).

17. Informatsiya po delu № 02-2473/2022 [Information on case No. 02-2473/2022]. *Ofitsial'nyi portal sudov obshchei yurisdiktsii g. Moskvy* [The official website of the Courts of general jurisdiction of Moscow]. Available at: <https://mos-gorsud.ru/rs/tverskoj/services/cases/civil/details/de7ea6a0-a3ab-11ec-8a7e-51b31fb55b35?participants=meta> (accessed 29.05.2024).

18. 80 pct of netizens agree China should punish Facebook. *People's Daily Online*, 2009, July 10. Available at: <https://en.people.cn/90001/90776/90882/6697993.html> (accessed 01.08.2020).

19. Kotsar Yu., Bevza D. Protesty lishili Kitai Instagram [Protests deprived China of Instagram]. *Gazeta.Ru*, 2014, 29 September. (In Russian). Available at: https://www.gazeta.ru/tech/2014/09/29_a_6240045.shtml (accessed 29.05.2024).

20. Isaac M. Facebook said to create censorship tool to get back into China. *The New York Times*, 2016, November 22. Available at: <https://www.nytimes.com/2016/11/22/technology/facebook-censorship-tool-china.html> (accessed 29.05.2024).

21. Counter-Terrorism Law (as amended in 2018). *China Law Translate*. Available at: <https://www.chinalawtranslate.com/en/counter-terrorism-law-2015/> (accessed 29.05.2024).

22. Creemers R., Webster G., Triolo P. *Translation: Cybersecurity Law of the People's Republic of China* (Effective June 1, 2017). Stanford Cyber Policy Center. Available at: <https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/> (accessed 29.05.2024).

23. Abkowitz A., Seetharaman D., Dou E. Facebook is trying everything to re-enter China – and it's not working. *The Wall Street Journal*, 2017, January 30.

Available at: <https://www.wsj.com/articles/mark-zuckerbergs-beijing-blues-1485791106> (accessed 29.05.2024).

24. Economy E.C. The great firewall of China: Xi Jinping's internet shutdown. *The Guardian*, 2018, June 29. Available at: <https://www.theguardian.com/news/2018/jun/29/the-great-firewall-of-china-xi-jinpings-internet-shutdown> (accessed 29.05.2024).

25. Ye J. China tightens Great Firewall by declaring unauthorised VPN services illegal. *South China Morning Post*, 2017, January 23. Available at: <https://www.scmp.com/news/china/policies-politics/article/2064587/chinas-move-clean-vpns-and-strengthen-great-firewall> (accessed 29.05.2024).

26. ChinaPower. *How Web-connected is China?* Available at: <https://chinapower.csis.org/web-connectedness/> (accessed 29.05.2024).

27. China's internet underground fights for its life. *Bloomberg*. Available at: <https://www.bloomberg.com/news/articles/2018-03-01/china-s-internet-underground-fights-for-its-life> (accessed 29.05.2024).

28. Bradsher K. China blocks WhatsApp, broadening online censorship. *The New York Times*, 2017, September 25. Available at: <https://www.nytimes.com/2017/09/25/business/china-whatsapp-blocked.html> (accessed 29.05.2024).

29. Mozur P. China disrupts WhatsApp service in online clampdown. *The New York Times*, 2017, July 18. Available at: <https://www.nytimes.com/2017/07/18/technology/whatsapp-facebook-china-internet.html> (accessed 29.05.2024).

30. WhatsApp design feature means some encrypted messages could be read by third party. *The Guardian*, 2017, January 13. Available at: <https://www.theguardian.com/technology/2017/jan/13/whatsapp-design-feature-encrypted-messages> (accessed 29.05.2024).

31. Whittaker Z. US says it doesn't need secret court's approval to ask for encryption backdoors. *ZDNet*, 2017, December 7. Available at: <https://www.zdnet.com/article/us-says-it-does-not-need-courts-to-approve-encryption-backdoors/> (accessed 29.05.2024).

32. FISA questions (July 2017). Wyden's encryption backdoor question. *Web archive*. Available at: <https://web.archive.org/web/20230106172742/https://www.documentcloud.org/documents/4320971-FISA-questions-July-2017.html> (accessed 29.05.2024).

33. Gellman B., Lindeman T. Inner workings of a top-secret spy program. *Washington Post*, 2013, June 29. Available at: <https://web.archive.org/web/20170830105407/https://apps.washingtonpost.com/g/page/national/inner-workings-of-a-top-secret-spy-program/282/> (accessed 29.05.2024).

34. Greenwald G., MacAskill E., Poitras L., Ackerman S., Rushe D. Microsoft handed the NSA access to encrypted messages. *The Guardian*, 2013, July 12.

Available at: <https://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data> (accessed 29.05.2024).

35. Microsoft. *About our practices and your data*. Available at: <https://blogs.microsoft.com/datalaw/our-practices/#did-participate-in-prism-program> (accessed 29.05.2024).

36. Facts on the collection of intelligence pursuant to Section 702 of the Foreign Intelligence Surveillance Act. *Office of the Director of National Intelligence*. Available at: <https://www.dni.gov/files/documents/Facts%20on%20the%20Collection%20of%20Intelligence%20Pursuant%20to%20Section%20702.pdf> (accessed 30.05.2024).

37. WhatsApp Privacy Policy. *WhatsApp*. Available at: <https://www.whatsapp.com/legal/updates/privacy-policy?eea=0#privacy-policy-updates-how-we-work-with-other-facebook-companies> (accessed 30.05.2024).

38. Vekhov: Facebook – instrument informatsionnoi voyiny [Vekhov: Facebook is an information warfare tool]. *Sputnik Moldova*, 2019, 18 February. (In Russian). Available at: <https://md.sputniknews.ru/20190218/vekhov-facebook-instrument-informatsionnoy-voyny-24775421.html> (accessed 30.05.2024).

39. Delyagin Mikhail. *My mozhem zakryt' Facebook uzhe zavtra. Kak Rossii ne proigrat' v informatsionnoi voine?* [We can close Facebook tomorrow. How can Russia not lose in the information war?]. (In Russian). Available at: <https://delyagin.ru/articles/192-deljagina-tsitirujut/90483-my-mozhem-zakryt-facebook-uzhe-zavtra-kak-rossii-ne-proigrat-v-informatsionnoy-voyne> (accessed 14.03.2024).

40. Holmes A. 533 million Facebook users' phone numbers and personal data have been leaked online. *Business Insider*, 2021, April 3. Available at: https://www.businessinsider.com/stolen-data-of-533-million-facebook-users-leaked-online-2021-4?utm_source=notification&utm_medium=referral (accessed 30.05.2024).

41. Press release: Thousands expected to sue Facebook in mass action against privacy breach. *Digital Rights Ireland*, 2021, April 16. Available at: <https://www.digitalrights.ie/facebook-breach/> (accessed 30.05.2024).

42. DRI Facebook action. *Digital Rights Ireland*. Available at: <https://www.digitalrights.ie/facebook/> (accessed 30.05.2024).

43. Wakefield J. Coronavirus: Zoom is in everyone's living room – how safe is it? *BBC*, 2020, 27 March. Available at: <https://www.bbc.com/news/technology-52033217> (accessed 14.03.2024).

44. Marczak B., Scott-Railton J. Move fast and roll your own crypto. A quick look at the confidentiality of zoom meetings. *Citizen Lab*, 2020, April 3. Available at: <https://citizenlab.ca/2020/04/move-fast-roll-your-own-crypto-a-quick-look-at-the-confidentiality-of-zoom-meetings/> (accessed 30.05.2024).

45. FORM S-1. Zoom Video Communications, Inc. March 22, 2019. *The United States Securities and Exchange Commission*. Available at: <https://www.sec.gov/Archives/edgar/data/1585521/000119312519083351/d642624ds1.htm> (accessed 30.05.2024).

46. Zoom Video Communications US SEC Form 10-K (2020, 31 January). *Internet Archive*. Available at: <https://web.archive.org/web/20200511122414/https://investors.zoom.us/static-files/09a01665-5f33-4007-8e90-de02219886aa> (accessed 30.05.2024).

47. Zoom. *Improving our policies as we continue to enable global collaboration*. Available at: <https://www.zoom.com/en/blog/improving-our-policies-as-we-continue-to-enable-global-collaboration/> (accessed 30.05.2024).

48. Zoom access from China. *University of California, Santa Barbara*. Available at: <https://help.lsit.ucsb.edu/hc/en-us/articles/360042172231-Zoom-Access-from-China> (accessed 14.03.2024).

49. "China support, my China colleagues cannot enter zoom meeting, why?". *Zoom Community*. Available at: <https://community.zoom.com/t5/Meetings/China-support-my-china-colleagues-cannot-enter-zoom-meeting-why/m-p/139630> (accessed 30.05.2024).

50. Chinese regulator launches probe into Tencent, Weibo and Baidu. *Bloomberg*, 2017, 11 August. Available at: <https://www.bloomberg.com/news/articles/2017-08-11/chinese-regulator-starts-probe-into-tencent-weibo-and-baidu> (accessed 30.05.2024).

51. Tencent WeChat, Sina Weibo and Baidu Post Bars were investigated for suspected violations of the "Network Security Act." *Office of the Central Commission for Network Security and Information Technology of China*. (In Chinese). Available at: http://www.cac.gov.cn/2017-08/11/c_1121467425.htm (accessed 30.05.2024).

52. Regulation on the Supervision and Verification of Internet Security by Public Security Authorities (Order No. 151 of the Ministry of Public Security). *Ministry of Public Security of the People's Republic of China*. (In Chinese). Available at: <https://www.mps.gov.cn/n6557558/c6263180/content.html> (accessed 30.05.2024).

53. Zhukova K. Vse «dyry» Zoom: chem riskuyut pol'zovateli samogo populyarnogo servisa videokonferentsii epokhi karantina [All vulnerability of Zoom: what are the risks of users of the most popular video conferencing service of the quarantine era]. *Forbes*, 2020, 23 April. (In Russian). Available at: <https://www.forbes.ru/tehnologii/398629-vse-dyry-zoom-chem-riskuyut-polzovateli-samogo-populyarnogo-servisa> (accessed 30.05.2024).

54. Zoom. Zayavlenie o konfidentsial'nosti [Zoom Privacy Statement]. *Zoom Video Communications*. Available at: <https://explore.zoom.us/ru/privacy/> (accessed 30.05.2024).

55. Kaspersky Team. Skvoznoe shifrovanie: chto eto i zachem ono nuzhno vam [Kaspersky Team. End-to-end encryption: what is it and why do you need it]. *Blog Kasperskogo* [Kaspersky's blog]. Available at: <https://www.kaspersky.ru/blog/what-is-end-to-end-encryption/29075/> (accessed 30.05.2024).

56. Skvoznoe shifrovanie (E2EE) konferentsii [End-to-end encryption (E2EE) of conferences]. *Zoom Podderzhka* [Zoom Support]. Available at: https://support.zoom.com/hc/en/article?id=zm_kb&sysparm_article=KB0065408 (accessed 30.05.2024).

57. Rosenblatt K. Army bans TikTok following guidance from the Pentagon. *NBC News*, 2019, December 31. Available at: <https://www.nbcnews.com/tech/tech-news/u-s-army-bans-tiktok-following-guidance-pentagon-n1109001> (accessed 30.05.2024).

58. Makena K. The Army is in hot water over TikTok recruiting activity. *The Verge*, 2021, December 15. Available at: <https://www.theverge.com/2021/12/14/22834405/tiktok-army-marco-rubio-ban-report-government-personal-devices> (accessed 30.05.2024).

59. Regarding the Acquisition of Musical.ly by ByteDance Ltd. A Presidential Document by the Executive Office of the President on 08/14/2020. *U.S. Department of the Treasury*. Available at: <https://home.treasury.gov/system/files/136/EO-on-TikTok-8-14-20.pdf> (accessed 30.05.2024).

60. Pettersson E., Glovin D., Brody B. TikTok Sues Trump to Challenge U.S. Government Restrictions. *Bloomberg*, 2020, 24 August. Available at: <https://www.bloomberg.com/news/articles/2020-08-24/tiktok-says-it-s-suing-u-s-over-ban-claims-no-security-threat> (accessed 30.05.2024).

61. Why we are suing the Administration. *TikTok*, 2020, 24 August. Available at: <https://newsroom.tiktok.com/en-us/tiktok-files-lawsuit> (accessed 30.05.2024).

62. Wells G., Tilley A. Oracle wins bid for TikTok in U.S., beating Microsoft. *The Wall Street Journal*, 2020, September 14. Available at: <https://www.wsj.com/articles/microsoft-drops-out-of-bidding-for-tiktoks-u-s-operations-11600039821> (accessed 30.05.2024).

63. Sherman A., Repko M. TikTok likely to announce sale of U.S. operations in the coming days in \$20 billion to \$30 billion range. *CNBC*, 2020, 27 August. Available at: <https://www.cnbc.com/2020/08/27/tiktok-likely-to-announce-sale-us-operations-in-the-coming-days.html> (accessed 30.05.2024).

64. Microsoft statement on TikTok. *Official Microsoft Blog*. Available at: <https://blogs.microsoft.com/blog/2020/09/13/microsoft-statement-on-tiktok/> (accessed 30.05.2024).

65. Executive Order 14034 of June 9, 2021. Protecting Americans' Sensitive Data from Foreign Adversaries. *Federal Register*. Available at: <https://www.federalregister.gov/d/2021-12506> (accessed 30.05.2024).

66. Executive Order 13873 of May 15, 2019. Securing the Information and Communications Technology and Services Supply Chain. *Federal Register*. Available at: <https://www.federalregister.gov/d/2019-10538> (accessed 30.05.2024).

67. Rubio, Gallagher introduce bipartisan legislation to ban TikTok. *Senator Rubio*. Available at: <https://www.rubio.senate.gov/rubio-gallagher-introduce-bipartisan-legislation-to-ban-tiktok/> (accessed 14.03.2024).

68. S.1143 – No TikTok on government devices Act. *United States Congress*. Available at: <https://www.congress.gov/bill/117th-congress/senate-bill/1143> (accessed 30.05.2024).

69. Dilanian K., Shabad R. The DOJ and FBI are investigating TikTok over allegations that employees spied on journalists. *NBC*, 2023, March 18. Available at: <https://www.nbcnews.com/politics/justice-department/doj-fbi-are-investigating-tiktok-allegations-employees-spied-journalis-rcna75497> (accessed 30.05.2024).

70. S.686 – Restrict Act. *United States Congress*. Available at: <https://www.congress.gov/bill/118th-congress/senate-bill/686> (accessed 30.05.2024).

71. H.R.7521 – Protecting Americans from Foreign Adversary Controlled Applications Act. *United States Congress*. Available at: <https://www.congress.gov/bill/118th-congress/house-bill/7521> (accessed 30.05.2024).

72. Huang R. China signals opposition to forced sale of TikTok in the U.S. *The Wall Street Journal*, 2024, March 15. Available at: <https://www.wsj.com/tech/tiktok-ban-chinese-owners-bytedance-1a857a06> (accessed 30.05.2024).

Для цитирования:

Петрунин Ю.Ю., Бухарин В.В. От информационной безопасности к национальной: противостояние IT-компаний США и КНР // Безопасность цифровых технологий. – 2024. – № 2 (113). – С. 25–54. – DOI: 10.17212/2782-2230-2024-2-25-54.

For citation:

Petrinin Yu.Yu., Bukharin V.V. Ot informatsionnoi bezopasnosti k natsional'noi: protivoborstvo IT kompanii SShA i KNR [From information security to national security: the confrontation between US and Chinese IT-companies]. *Bezopasnost' tsifrovyykh tekhnologii = Digital Technology Security*, 2024, no. 2 (113), pp. 25–54. DOI: 10.17212/2782-2230-2024-2-25-54.