

1. Владзимирский А.В. История научного обоснования концепции «телемедицины»: вклад исследовательской группы профессора К.Т.Берда//История и современное мировоззрение. 2002. Т.4. №2. С.95-103. DOI: 10.33693/2658-4654-2022-4-2-95-103.
2. Пятьдесят восьмая сессия Всемирной ассамблеи здравоохранения: резолюции и решения: приложение: Всемирная организация здравоохранения, WHA58/2005/REC/1/Женева, 16-25 мая 2005 г. С. 119-121.
3. Концепция развития электронного здравоохранения Республики Беларусь на период до 2022 года: Приказ Министерства здравоохранения Респ. Беларусь, 20.03.2018г., № 244// Режим доступа: <https://belcmt.by/ru/sanitation>. – Дата доступа: 03.10.2022.
4. Особенности и достижения национальной системы здравоохранения, [Электронный ресурс] –Режим доступа: <https://president.gov.by/ru/belarus/social/healthcare/nacionalnaya-sistema><https://president.gov.by/ru/belarus/social/healthcare/nacionalnaya-sistema>. – Дата доступа: 03.10.2022.
5. О здравоохранении: Закон Респ. Беларусь, 18 июня 1993 г., № 2435-XII: в ред. Закона Респ. Беларусь от 11 дек. 2020 г., № 94-З// Право.by. Национальный правовой портал Республики Беларусь. – Минск, 2022.
6. О порядке функционирования и использования централизованной информационной системы здравоохранения: постановление Совета Министров Респ. Беларусь, 3 мая 2021 г., № 267// Право.by. Национальный правовой портал Республики Беларусь. – Минск, 2022.

Ребицкая Екатерина Витальевна

**ВМЕШАТЕЛЬСТВО ТНК В ИНФОРМАЦИОННЫЙ СУВЕРЕНИТЕТ
ГОСУДАРСТВ: МЕЖДУНАРОДНО-ПРАВОВОЙ АСПЕКТ**

Аспирант 2 года обучения кафедры государственного управления,
юридический факультет, Белорусский государственный университет,

rebitskayaev@yandex.by

Аннотация. В современном мире информационная сфера приобретает ключевое значение в развитии любого государства. Вместе с тем трансформация социума в информационное общество порождает новые угрозы не только со стороны государств, но и юридических лиц, и напрямую затрагивает вопросы защиты информационного суверенитета государств. В статье аргументируется потенциальная угроза ТНК в отношении государственного информационного суверенитета и предлагается способ по предупреждению данной угрозы на международном уровне.

Ключевые слова: информационный суверенитет; информационная безопасность; ТНК; международная безопасность; кибербезопасность.

Динамичное развитие средств коммуникации, совершенствование технологий информационного воздействия в рамках интернет-платформ, контролируемых ТНК, поставили в повестку дня многих государств настоятельную потребность защиты информационного суверенитета. Актуальность темы исследования вызвана значительным усилением роли ТНК

на международной арене в области формирования глобального информационного пространства.

Привлекают внимание в аспекте проблематики нашего исследования работы, рассматривающие вопросы функционирования ТНК и их воздействие на ход и характер построения информационного общества (П.А. Цыганков, И.Я. Киселева, М.М. Лебедев, Л.А. Лунц, Р. Кеохейа, Б. Коэн, Ф. Миллард), а также научные труды, посвященные проблематике защиты информационного суверенитета (И. С.Ашманов, М.С.Азаров, М. М. Кучерявый, Н.О.Мороз, Ю.А. Караулова).

Цель работы – определить способы обеспечения защиты государственного информационного суверенитета от вмешательств со стороны ТНК.

Содержание понятия «суверенитет» было впервые сформулировано в решении Постоянной палаты третейского суда по делу об острове Пальмас. Так, Постоянная палата третейского суда указала, что «суверенитет в отношениях между государствами означает независимость. Независимость в отношении части земного шара представляет собой право осуществлять там, исключая любое другое государство, функции государства [1, с.838].

Взаимосвязь между понятиями «суверенитет» и «внутренние дела» была разъяснена Международным Судом ООН в решении по делу о военных и полувоенных действиях в Никарагуа и против нее (Никарагуа против США). В частности, Международный Суд ООН указал, что «данный принцип запрещает всем государствам или группам государств прямо или косвенно вмешиваться во внутренние или внешние дела других государств. Соответственно, запрещенное вмешательство должно иметь отношение к вопросам, в которых каждому государству разрешено свободно принимать решения на основании принципа государственного суверенитета. Один из них – это выбор политической, экономической, социальной и культурной системы, а также формулирование внешней политики» [2, с.14]. Такая позиция была также поддержана в Декларации Генеральной Ассамблеи ООН о принципах международного права, касающихся дружественных отношений и сотрудничества между государствами в соответствии с Уставом Организации Объединенных Наций 1970 г., где закреплено, что «каждое государство пользуется правами, присущими полному суверенитету».

Повсеместная цифровизация общества привела к размыванию категории «государственный суверенитет», расширяя границы ее классического понимания. Так появился новый вид суверенитета –информационный суверенитет. Один из ключевых российских разработчиков концепции информационного суверенитета И. С. Ашманов рассматривал его, в первую очередь, как возможность обеспечить уверенную работу всех государственных структур в условиях искусственно создаваемой информационной турбулентности. Ученый и практик М. М. Кучерявый уточняет и детализирует это определение: «Информационный суверенитет – это верховенство и независимость государственной власти при формировании и реализации

информационной политики в национальном сегменте и глобальном информационном пространстве» [3, с.12]. Аналогичную точку зрения высказывает китайский ученый профессор Пекинского университета Вэньсян Гонг. Он подчеркивает, что внутренний информационный суверенитет подразумевает верховную власть государства при принятии решений и поддержании информационного порядка в стране [4, с.129].

На международной арене вопросы информационного суверенитета регулируются нормами мягкого права (Конвенцией об обеспечении международной информационной безопасности (концепция) 2011 года; Таллиннским руководством 2.0), а также нормами международной морали. Наиболее значимыми источниками норм международной морали в части определения правил ответственного поведения государств в киберпространстве являются отчеты Группы правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникаций. Вместе с тем на международном уровне отсутствует единый нормативный акт, регламентирующий вопросы обеспечения защиты государствами своего информационного суверенитета, что вынуждает государства совершать попытки урегулирования данной проблемы в рамках национальных законодательств.

Определение информационного суверенитета присутствует в нормативных документах и Республики Беларусь, и в ряде стран ближнего и дальнего зарубежья. В соответствии с п.8 Главы 3 Постановления Совета Безопасности Республики Беларусь от 18 марта 2019 г. № 1 «О Концепции информационной безопасности Республики Беларусь» информационный суверенитет Республики Беларусь представляет собой неотъемлемое и исключительное верховенство права государства самостоятельно определять правила владения, пользования и распоряжения национальными информационными ресурсами, осуществлять независимую внешнюю и внутреннюю государственную информационную политику, формировать национальную информационную инфраструктуру, обеспечивать информационную безопасность.

Необходимо отметить, что белорусский термин «информационный суверенитет» в меньшей степени направлен на определение границ суверенной власти Республики Беларусь в киберпространстве. В первую очередь, термин сформулирован в русле традиционного понимания суверенитета в международном праве [5, с.201].

В Законе Украины «О национальной программе информатизации» информационный суверенитет государства определяется как «способность государства контролировать и регулировать потоки информации из-за пределов государства в целях соблюдения законов Украины, прав и свобод граждан, гарантирования национальной безопасности государства».

Любопытной является китайская практика обеспечения защиты информационного суверенитета. Еще с 2003 года в КНР была создана система фильтрации и блокировки доступа китайским гражданам к информационным ресурсам и контенту, запрещенным правительством страны – система «Золотой

щит», более известная в западных СМИ как «Великий китайский файервол» (The Great Firewall of China). С 2010 года в государстве активно развивается так называемая концепция «интернет суверенитета», которая нашла отражение в «белой книге» под названием «Интернет в Китае». Данная концепция неоднократно подвергалась критике со стороны американских и европейских политиков и журналистов. Джеймс Ареди на страницах журнала «The Wall Street Journal» отмечал, что «председатель КНР Си Цзиньпин с помощью консерваторов в правительстве, учёных, военных и использования высоких технологий стремится к тому, чтобы оказывать влияние на весь цифровой мир Китая, от полупроводников до социальных медиа». А редакция газеты «The Washington Post» опубликовал статью «Страшный урок Китая для мира: Цензура интернета работает», в которой осуждала политику китайского правительства, как нарушающую права человека [6, с.78]. На наш взгляд, данный подход действительно довольно радикален, однако его введение нельзя назвать бесосновательным.

В настоящее время цифровые ТНК-монополисты (такие как Google, Meta, Microsoft) полностью контролируют не только глобальное интернет-пространство, создавая информационное поле, но и могут осуществлять контроль за локальными точками доступа, внедрив свои операционные системы в ПК практически любого человека. Последние несколько десятилетий на микропроцессорном рынке господствуют две американские компании: Intel и AMD. Подавляющее большинство серверных и настольных компьютеров основано именно на их процессорах. Данное обстоятельство не только ставит другие страны в зависимость от продукции американских корпораций, но и в перспективе может стать средством вмешательства в информационный суверенитет государств. Ещё в 2005 году Научный совет министерства обороны США опубликовал отчёт, в котором была отмечена опасность производства процессоров за пределами США. В документе подчёркивалось, что существует возможность намеренного изменения процессора в ходе проектирования или производства, что может поставить под угрозу национальную безопасность. Данная угроза некоторое время считалась гипотетической, но в 2013 г. её реальность, опытным путем доказали: Георг Беккер, Франческо Регаццони, Кристоф Паар и Уэйн Берлесон. Эта интернациональная команда учёных, возглавляемая профессором из университета штата Массачусетс Г. Беккером, смогла создать две версии «тройня аппаратного уровня» [6, с.84]. Следовательно, внедренный в процессор «тройнянский конь» или «аппаратная закладка» могут оставаться незамеченными, угрожая не только государственному информационному суверенитету, но и национальной безопасности страны в целом.

Кроме того, практика последних лет подтверждает, что акты по тайному сбору информации в киберпространстве, которые совершаются либо при непосредственном участии ТНК, либо с использованием ТНК как инструмента преступления, становятся не исключением, а нормой на международной арене. В подтверждение этого можно привести историю с китайской шпионской

киберсетью GhostNet, в результате деятельности которой были взломаны не менее 1295 информационных систем в 103 государствах мира. В частности, 30 % таких информационных систем находились в правительственных структурах различных государств: по 11 – в Министерстве иностранных дел Бутана и в посольстве Мальты в Бельгии и семь – в посольстве Индии в США. Были взломаны также восемь информационных систем в офисе крупнейшего оператора связи Венесуэлы; три – в офисах Азиатского банка развития и более 150 компьютеров – в штаб-квартирах торговых союзов Вьетнама и Тайваня. По одной взломанной информационной системе было обнаружено в посольствах Португалии, Румынии, Кипра, Индии, Таиланда, Германии, расположенных в разных странах мира, и в штабе Верховного главнокомандующего Объединенными вооруженными силами НАТО в Европе. Также десятки информационных систем были взломаны в организациях, борющихся за независимость Тибета, в том числе в штаб-квартирах различных протибетских организаций в Нью-Йорке, Лондоне, Брюсселе и Женеве [7, с.73]. Подобные нарушения совершаются и в отношении отдельных физических лиц. Например, в начале октября 2022 года некоммерческая система здравоохранения США Advocate Aurora Health уведомила более 3 млн. своих пациентов о нарушении их конфиденциальности из-за использования Meta* Pixel. Ранее медицинские компании США уведомляли своих пациентов о том, что сайты больниц, использующие Pixel, непреднамеренно передавали данные пациентов Facebook. Собранные данные включали: диагнозы пациентов; медицинские назначения; имена поставщиков; контактные данные пациентов; IP-адреса; информацию о приемах пациентов врачами [8]. Ранее кампания Meta неоднократно была уличена в незаконном сборе конфиденциальной информации, в особенности пользователей Facebook.

Из вышеотмеченного становится очевидным то, что ТНК могут вмешиваться в информационный суверенитет государств (как непосредственно, так и опосредовано), затрагивая следующие его аспекты: идеологический и технический. Идеологический аспект подразумевает проведение государством собственной политики по наполнению и развитию информационного пространства, повышению уровня массовой культуры, контролем за системой пропаганды, а также усовершенствованного законодательства в области информации и информатизации. К техническому аспекту относятся: наличие национального программного обеспечения, электронной платежной системы, собственные социальные сети и т.п.

Следует отметить, что неурегулированный правовой статус ТНК на международной арене не позволяет рассматривать их в качестве субъекта преступлений и привлекать к международно-правовой ответственности. Привлечение же к ответственности в рамках национальных законодательств усложняется трансграничным статусом компаний и отсутствием в большинстве стран уголовной ответственности для юридических лиц.

Таким образом, в настоящее время деятельность ТНК может выступать средством вмешательства в информационный суверенитет государств путем

формирования информационной повестки в глобальном информационном пространстве, сборе данных пользователей интернет-площадок, кибершпионаже и т.д. Отсюда возникает острая необходимость выявления способов регулирования деятельности ТНК в области обеспечения защиты информационного суверенитета государств на международном уровне. Решение данной проблемы возможно путем внесения в Таллинское руководство 2.0 нормы, акцентирующей внимание на потенциальной угрозе государственному информационному суверенитету со стороны ТНК, а также разработки международного договора по вопросам защиты информационного суверенитета государств.

Список использованных источников

1. Island of Palmas case (Netherlands, USA) // Reports of international arbitral awards, 4 April 1928. – Vol. II. – P. 829-871 (P. 838)
2. Military and Paramilitary Activities in und against Nicaragua (Nicaragua v. United States of America). Merits, Judgment. I.C.J. Reports 1986, p. 14, para 205.
3. Кучерявый М. М. Государственная политика информационного суверенитета России в условиях современного глобального мира / М.М.Кучерявый // Управленческое консультирование. – 2014. – № 9 (69). – С. 8-15.
4. Gong Wenxiang. Information Sovereignty Reviewed // Peking University. Intercultural Communication Studies. 2005. Vol. XIV. Issue 1. P. 119–135.
5. Мороз, Н.О. Информационный суверенитет как основа обеспечения информационной безопасности Республики Беларусь / Мороз Н.О. // Конституционное право как фактор динамичного развития белорусского государства: история и современность : материалы респ. науч.-практ. конф., Минск, 15 окт. 2021 г. / Белорус. гос. ун-т ; редкол.: Г. А. Василевич (гл. ред.), А. В. Шавцова; В. Е. Петухова. – Минск : БГУ, 2021. – С.199-203.
6. Бухарин, В.В. Компоненты цифрового суверенитета Российской Федерации как техническая основа информационной безопасности / В.В.Бухарин // Вестник МГИМО. – 2016. – № 6(51) – С.76-91.
7. Гаркуша-Божко, С.Ю. Проблема кибершпионажа в международном гуманитарном праве / С.Ю. Гаркуша-Божко // Московский журнал международного права. – 2021. – №1. – С.70-80.
8. Securitylab.ru [Электронный ресурс]. – Режим доступа: https://www.securitylab.ru/blog/personal/Business_without_danger/29565.php. – Дата доступа: 25.10.2022.

Рожок Елена Петровна

ЗАЩИТА СЕМЬИ И ТРАДИЦИОННЫХ СЕМЕЙНЫХ ЦЕННОСТЕЙ В СТРУКТУРЕ ЦЕЛЕЙ УСТОЙЧИВОГО РАЗВИТИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Соискатель кафедры политологии юридического факультета, Белорусский государственный университет, г.Минск, Беларусь,
alenaarazhok@bsu.by

Аннотация. В статье отражены основные принципы государственной семейной политики Республики Беларуси, анализируются направления государственной политики, приоритеты и индикаторы устойчивого развития. Отражены важнейшие задачи семейной