УДК 341.2 /16.8

ОСНОВНЫЕ НАПРАВЛЕНИЯ ПРОТИВОДЕЙСТВИЯ УГРОЗАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, ВОЗНИКАЮЩИМ СО СТОРОНЫ ЮРИДИЧЕСКИХ ЛИЦ

Е.В. Ребицкая
ВГУ имени П.М. Машерова, Республика Беларусь

Аннотация. В статье рассмотрены юридические лица, продуктом деятельности которых являются информационно-коммуникационных технологий, в качестве потенциальной угрозы международной информационной безопасности. Автор подробно анализирует действия цифровых ТНК в глобальном информационном пространстве, препятствующих поддержанию международного мира и безопасности. Приводятся конкретные примеры использования цифровых ТНК в террористической деятельности, а также деятельности, направленной на дестабилизацию общества. Для противодействие угрозам, связанных с осуществлением юридическими лицами в глобальном информационном пространстве действий, препятствующих поддержанию международного мира и безопасности, необходимо урегулировать деятельность цифровых ТНК в данной области на законодательном уровне. Так, в Республике Беларусь следует включить в Концепцию информационной безопасности Республики Беларусь нормы, акцентирующей внимание на потенциальной угрозе информационной безопасности со стороны ТНК.

Ключевые слова: международная информационная безопасность, юридические лица, информационная безопасность, цифровые ТНК.

Серьезной угрозой международной информационной безопасности стало использование информационно-коммуникационных технологий в преступных целях, в том числе для совершения преступлений в сфере компьютерной информации, а также для совершения различных видов мошенничества. Эта угроза особенно отчетливо проявилась в период пандемии, когда юридические лица, продуктом деятельности которых являются информационно-коммуникационных технологий (далее – цифровые ТНК), закрепили свое монопольное положение в сети Интернет. События последних лет свидетельствуют о прогрессирующей угрозе использования информационно-коммуникационных технологий для проведения компьютерных атак на информационные ресурсы государств, в том числе на критическую информационную инфраструктуру.

Цель данной научной работы – разработать предложения, направленные на противодействие угрозам, связанных с осуществлением юридическими лицами в глобальном информационном пространстве действий, препятствующих поддержанию международного мира и безопасности.

Материалы и методы. При написании статьи были ряд международных актов и актов национального белорусского законодательства, регламентирующих вопросы обеспечения международной и национальной информационной безопасности. Также были изучены научные труды, посвященные анализу деятельности цифровых ТНК как потенциальной угрозы безопасности в информационной сфере. Для анализа собранного материала были использованы метод анализа, синтеза и сравнительно-правовой метод.

Результаты и обсуждения. Динамичность и многоаспектность международной информационной безопасности определяет необходимость постоянной актуализации термина «международная информационная безопасность». В терминах, данных в документах ООН, под международной информационной безопасностью понимается защищенность глобальной информационной системы от «триады угроз» – террористической, преступной и военно-политической. Последний вид подразумевает информационное противоборство и информационные войны [1, с. 82]. В Республике Беларусь в международную информационную безопасность включаются как технические аспекты (безопасность и защищенность информационных сетей и систем), так и политико-идеологические, политико-психологические аспекты (например, манипулирование информацией, пропаганда посредством глобальных информационных сетей, различные формы информационного воздействия), что нашло свое отражение в терминах «информационная безопасность» и «международная информационная безопасность», закрепленных в п.8 Постановления Совета Безопасности Республики Беларусь от 18 марта 2019 г. № 1 «О Концепции информационной безопасности Республики Беларусь». Белорусское правительство уделяет большую роль противодействиям преступлений, совершаемых в информационной сфере, а Министерство иностранных дел Республики Беларусь постоянно поднимает на международной арене проблему использования информационно-коммуникационных технологий для вмешательства во внутренние дела государств, подрыва их суверенитета и нарушения территориальной целостности, что представляет угрозу международному миру и безопасности.

Согласно докладу Рабочей группы открытого состава по вопросам безопасности использования ИКТ и самих ИКТ от 2021 года, наибольшую опасность представляет военно-политическое измерение угроз международной информационной безопасности. К такого рода угрозам относится и использование информационно-коммуникационных технологий для разжигания межэтнической, межрасовой и межконфессиональной розни. Соответствующие угрозы могут быть направлены на подрыв суверенитета государств, нарушение территориальной целостности, подготовку и реализацию планов по проведению информационных операций и войн, а также непосредственное вмешательство во внутренние дела государства. Примером подобного вмешательства является операция Stuxnet 2010 года, когда компьютерный червь Stuxnet значительно замедлил ядерную программу Ирана. На современном этапе наметилась милитаризация глобального информационного пространства. Согласно данным ЮНИДИР, большинство современных государств проводят масштабные работы по созданию как оборонительного, так и наступательного информационного потенциала. Все чаще отмечаются случаи шпионажа, распространения вредоносных программ, ориентированных на воздействие на критические инфраструктуры. Соответственно, и военные действия переносятся в цифровое пространство [2, с. 7].

Практика последних лет подтверждает, что акты по тайному сбору информации в киберпространстве, которые совершаются либо при непосред-

ственном участии цифровых ТНК, либо с использованием продуктов их деятельности как инструмента преступления, становятся не исключением, а нормой на международной арене. В качестве примера можно привести историю с китайской шпионской кибersетью 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 [3, с.73]. По мере появления и распространения глобальных сетей и повсеместной информатизации правительственные органы государств осознали свою уязвимость в вопросах контроля над деятельностью цифровых ТНК. Государства стремятся ограничить хранение, перемещение и обработку ТНК, создающими цифровую продукцию, и обычно оправдывают свои действия по ограничению тех или иных цифровых платформ в качестве необходимой меры по защите своего цифрового суверенитета, а также прав своих граждан. Например, в 2021 году Россия оштрафовала Facebook на миллионы рублей за неудаление запрещенного контента. Штрафы компания не платила, а поскольку у нее не было официально созданных представительств и филиалов в России, исполнение решений российских судов было совершенно невозможно [4]. В 2022 году же компания Meta и вовсе была признана в качестве экстремисткой на территории Российской Федерации. Ведь цифровые ТНК становятся одной из потенциальных угроз национальной и международной информационной безопасности.

Последние годы также остро стоит вопрос международной ответственности юридических лиц за совершение коррупционных деяний, направленных на финансирование терроризма. В качестве яркого примера служит деятельность ФАТФ (Рекомендации ФАТФ «Отмывание денег и конфискация», «Финансирование терроризма и распространения ему», «Прозрачность и бенефициарная собственность юридических лиц и образований»). Кроме того, последние 15 лет существует практика наложения на юридических лиц односторонних санкций Советом безопасности ООН (например, при оказании юридическим лицом финансовой или любой иной помощи КНДР и Ирану по разработке ядерного оружия), а также целевых санкций со стороны отдельных государств (такая политика наиболее популярна в США, а последнее годы все чаще применяется и Европейским Союзом) [5, с.544]. По состоянию на начало 2023 года в Совете Без-

опасности ООН действует 14 режимов санкций, которые направлены на поддержку политического урегулирования конфликтов, ядерного нераспространения и борьбы с терроризмом. Но ни один из них не затрагивает деятельность цифровых ТНК.

Вместе с тем на международной арене систематически поднимаются обсуждения, связанные с деятельности цифровых ТНК как угрозой международной информационной безопасности (A/RES/73/27; A/RES/77/36, A/RES/74/274, A/КБ8/73/264 и др.) В рамках ООН создан Специальный комитет по разработке Конвенции о противодействии использованию информационных и коммуникационных технологий (ИКТ) в преступных целях, а также функционирует Рабочая группа открытого состава по вопросам безопасности использования ИКТ и самих ИКТ 2021-2025 (РГОС). Следует отметить, что в проекте Конвенции содержится норма, регулирующая ответственность юридических лиц в связи с преступлениями и иными противоправными деяниями в информационном пространстве (ст.30 Конвенции).

На региональном уровне вопрос обеспечения национальной информационной безопасности обычно являлся частью направления «международной безопасности» с акцентом на трансформацию различных секторов экономики, развитие отечественных компаний. Так, в рамках СНГ государства-участники реализуют свою политику в данной сфере в соответствии со Стратегией обеспечения информационной безопасности государств-участников СНГ, утвержденного Решением Совета глав правительств СНГ 25 октября 2019 года. В рамках ОДКБ функционирует Протокол о взаимодействии государств-членов ОДКБ по противодействию преступной деятельности в информационной сфере от 23 декабря 2014 г., который содержит ряд норм, регулирующих вопросы сотрудничества в борьбе с деяниями, которые совершаются при помощи информационных технологий и посягают как на безопасности государств-участников, так и на международный мир и безопасность в целом (ст. 3).

В рамках Союзного государства 22 февраля 2023 года была утверждена Концепция информационной безопасности Союзного государства (Постановление Высшего Государственного Совета Союзного государства от 22 февраля 2023 г. № 1 «О Концепции информационной безопасности Союзного государства»). Данная Концепция представляет собой революционный документ в области обеспечения информационной безопасности, принятый на региональном уровне постсоветского пространства. Защита информационной безопасности Союзного государства согласована с решением задач социально-экономического развития Союзного государства, а также с соблюдением национальных интересов государств-участников в различных сферах. В Концепции акцентируется внимание на возрастающей злоупотреблении возможностями трансграничного оборота информации с целью нанесения ущерба международной безопасности, а также увеличение количества кибератак, носящих транснациональный характер. Вместе с тем документ не акцентирует внимание на потенциальной угрозе информационной безопасности со стороны цифровых ТНК и не предлагает способы решения данной проблемы.

Необходимо отдельно остановиться и на Указе Президента Республики Беларусь от 14 февраля 2023 г. № 40 «О кибербезопасности» (акт еще не вступил в силу). Данный документ должен стать правовым фундаментом национальной системы обеспечения кибербезопасности, т.к. регулирует основные принципы создания и функционирования национальной системы обеспечения кибербезопасности. В большей степени Указ направлен на обнаружение, предотвращение и минимизацию негативных последствий кибератак на критически важные национальные объекты с целью повышения устойчивости и надежности информационных систем.

Полагаем, что в целях противодействие угрозам, связанных с осуществлением юридическими лицами в глобальном информационном пространстве действий, препятствующих поддержанию международного мира и безопасности необходимо урегулировать деятельность цифровых ТНК в данной области на законодательном уровне. Так, в п.16 Постановления Совета Безопасности Республики Беларусь от 18 марта 2019 г. № 1 «О Концепции информационной безопасности Республики Беларусь» целесообразно включить следующую формулировку «государство осуществляет контроль за деятельностью ТНК путем воспрепятствования в законном порядке распространению недостоверной массовой информации, запрещенной информации и информации, которая потенциально может нанести ущерб международному миру и безопасности в установленном законодательством порядке к распространению».

Заключение. Таким образом, глобальное возрастание роли информации в системе общественных отношений способствует актуализации темы защиты международной информационной безопасности и информационной безопасности государств. В тоже время на международной арене увеличивается роль цифровых ТНК, оказывающих существенное влияние на формирование глобального цифрового пространства. Спорный статус ТНК на международной арене не позволяет считать их субъектами международного права и, как следствие, распространять на них действие норм международных актов в сфере международно-правовой ответственности. Отсюда возникает острая необходимость выявления способов регулирования деятельности цифровых ТНК в контексте обеспечения информационной безопасности государств на национальном уровне. На наш взгляд, таким способом может выступать урегулирование деятельности ТНК в рамках национальных законодательств. Изучив Концепцию информационной безопасности Республики Беларусь, мы считаем целесообразным включения в нее нормы, акцентирующей внимание на потенциальной угрозе информационной безопасности со стороны ТНК.

Список использованных источников

1. Прохорова, Д.А. Международная информационная безопасность как современная проблема / Д.А. Прохорова // Журнал «Информационное общество», Института развития информационного общества. – М., 2022. – Вып. № 5. – С.81-90.

2. Международная информационная безопасность: теория и практика / А.В. Крутских [и др.]; под общ. ред. А.В. Крутских. – 2-е изд., доп. – М.: Аспект Пресс, 2021. – 384 с.

3. Гаркуша-Божко, С.Ю. Проблема кибершпионажа в международном гуманитарном праве / С.Ю. Гаркуша-Божко // Московский журнал международного права. – 2021. – № 1. – С.70-80.

4. Schultz, D., Moroz, N., Cyberspace and the Future of International Law and Politics [Electronic resource] // Mode of access: https://intpolicydigest.org/cyberspace-and-the-future-of-international-law-and-politics. – Date of access: 17.05.2023.

5. Ребицкая, Е.В. Специальная международная правосубъектность физических и юридических лиц: сравнительно-правовой анализ / Е. В. Ребицкая // Материалы региональной научно-практической конференции «Наука – образованию, производству, экономике», Витебск, 3 марта 2023 г. / Витеб. гос. ун-т; редкол.: Е.Я. Аршанский (гл. ред.) [и др.]. – Витебск: ВГУ имени П.М. Машерова. – С.542-545.

УДК 340

К ВОПРОСУ ОБ УРОВНЕ СФОРМИРОВАННОСТИ ПРАВОВОЙ КУЛЬТУРЫ СТУДЕНТОВ НА НЕЮРИДИЧЕСКИХ СПЕЦИАЛЬНОСТЯХ

О.В. Реут

ВГУ имени П.М. Машерова, Республика Беларусь

Аннотация. В статье рассматриваются результаты исследования сформированности уровня правовой культуры студентов неюридических специальностей, на основе когнитивного, мотивационного и поведенческого компонентов формирования правовой культуры.

Ключевые слова: молодежь, правовая культура, высшее образование, право, личность.

Формирование правовой культуры личности является одним из основных составляющих воспитания. В процессе подготовки специалистов с высшим образованием актуальной задачей является усвоение обучающимися неюридических специальностей систематизированных знаний о праве, законодательстве Республики Беларусь, формирования у них законопослушного поведения, понимания ответственности за противоправные действия. Цель исследования – изучить уровень сформированности правовой культуры студентов 1–2 курсов неюридических специальностей.

Материал и методы. Были использованы междисциплинарные исследования, в том числе работы философов, социологов, психологов, юристов и др. Методами исследования явились формально-логический и сравнительно-правовой методы, а также анкетирование.

Результаты и их обсуждение. Правовая культура является междисциплинарным институтом, который рассматривается учеными различных научных отраслей, что и определяет ее уникальность как объекта познания, но вместе с тем и порождает сложности в этом познании. В последние десятилетия появилось много работ, где правовая культура рассматривается либо в рамках идей правового государства и прав человека (Е.В. Аграновская, В.Н. Керимов, и др.), либо в связи с психологическими аспектами применения права (В.В. Лазарев, Ю.Н. Новик и др.), либо в социологических исследованиях правовых