КИБЕРВОЙНЫ И КИБЕРТЕРРОРИЗМ КАК УГРОЗА МЕЖДУНАРОДНОЙ БЕЗОПАСНОСТИ

Д. А. Акуленок,
студент факультета экономики и права
Витебский филиал Учреждения образования Федерации профсоюзов Беларуси «Международный университет «МИТСО», г. Витебск
Научный руководитель:
О. П. Рубо,
старший преподаватель кафедры правоведения и социально-гуманитарных дисциплин
Витебский филиал Учреждения образования Федерации профсоюзов Беларуси «Международный университет «МИТСО», г. Витебск

Обеспечение международной безопасности – одна из ключевых задач, стоящих перед мировым сообществом. Стремительное развитие информационных технологий и информатизации общества привело к появлению таких угроз, как кибервойна и кибертерроризм. Система международного сотрудничества в борьбе с новыми угрозами требует выработки соответствующих норм международного и внутригосударственного права. Сотрудничество субъектов международного права в противодействии киберугрозам на глобальном, региональном, двустороннем уровнях должно стать дополняющим друг друга, а не взаимоисключающим.

В настоящее время целью многих стран мира является обеспечение информационной безопасности. К главным угрозам в сфере международной информационной безопасности можно отнести использование информационных и коммуникационных технологий:

1) в качестве информационного оружия в военно-политических целях, противоречащих международному праву;
2) в террористических целях;
3) с целью вмешательства во внутренние дела суверенных государств;
4) для совершения преступлений, связанных с неправомерным доступом к компьютерной информации, с созданием и использованием вредоносных компьютерных программ [1, с. 100].

Регулирование информационной безопасности складывается как из юридически обязательных норм международных договоров, так и из «мягкого права» – деклараций, рекомендаций и докладов органов международных организаций [2, с. 293].

Развитие международно-правового института международной информационной безопасности осуществляется как на уровне ООН, так и в рамках двухсторонних соглашений и документов международных организаций [2, с. 293].

Несмотря на то, что термин «кибертерроризм» широко применяется в настоящее время, его согласованное и общепризнанное определение до сих пор отсутствует. Например, специальный агент ФБР М. Поллит определил кибертерроризм как любую «умышленную, политически мотивированную атаку на информацию, компьютерные системы, программы и данные, которые приводят к насилию в отношении невоенных целей, субнациональных групп или тайных агентов» [3, с. 30].

Первые шаги на укрепление безопасности глобальных информационных и телекоммуникационных систем были сделаны в декабре 1998 года, когда на 53-й сессии ГА ООН Россией был представлен проект Резолюции A/RES/53/70 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». Резолюция рекомендовала государствам – членам ООН высказаться о целесообразности разработки международных принципов, нацеленных на укрепление безопасности

глобальных информационных и телекоммуникационных систем и которые способствовали бы борьбе с международным терроризмом и криминалом [4].

Особого внимания заслуживает проект Конвенции ООН «Об обеспечении международной информационной безопасности», представленный Российской Федерацией в 2011 году. В ст. 2 Конвенция впервые в международной практике раскрывает термин «информационная война», определяя ее как «противоборство между двумя или более государствами в информационном пространстве с целью нанесения ущерба информационным системам… подрыва политической, экономической и социальной систем, массированной психологической обработки населения для дестабилизации общества и государства, а также принуждения государства к принятию решений в интересах противоборствующей стороны». Однако конвенция так и не была утверждена [1, с. 100].

К региональным источникам права международной информационной безопасности относится Конвенция о компьютерных преступлениях, подписанная членами Совета Европы в Будапеште 23 ноября 2001 г. В документе установлен порядок взаимодействия стран в борьбе с преступлениями против конфиденциальности, целостности и доступности компьютерных данных и систем, а также всеми видами правонарушений, связанных с использованием компьютерных технологий. Меры, предусмотренные Конвенцией, имеют особое значение в пресечении террористических преступлений.

В Декларации Совета коллективной безопасности Организации Договора о коллективной безопасности от 8 ноября 2018 г. утверждается, что одной из приоритетных задач ОДКБ является наращивание совместных усилий в целях борьбы со всеми видами современных вызовов и угроз, включая терроризм и связанный с ним экстремизм. Государства-участники призывают к формированию самой широкой антитеррористической коалиции под эгидой ООН на основе соблюдения общепризнанных норм и принципов международного права [5].

В качестве информационного оружия при широком подходе к феномену информационной войны могут выступать «средства уничтожения, искажения или хищения информационных массивов, добывания из них необходимой информации после преодоления систем защиты, ограничения или воспрещения доступа к ним законных пользователей, вывода из строя телекоммуникационных сетей, всех средств высокотехнического обеспечения жизни общества и функционирования государства» [6, с. 178].

Термин «информационная война» был введен в научный оборот ученым физиком Т. Роном, который в 1976 году определил информацию как самое слабое звено вооруженных сил и национальной обороны. Информационная война, по представлению ряда специалистов, это узкоспециальный институт международного права вооруженных конфликтов [6, с. 179].

Зачастую осуществляется разграничение военных и иных информационных конфликтов. При этом под «информационной войной» понимается одна из форм информационной борьбы сторон посредством использования информационного оружия в интересах уничтожения телекоммуникационных систем или взятия их под свой контроль, нанесения психологического удара по населению и личному составу вооруженных сил с возможным последующим ведением боевых действий на суше, морском и воздушном пространствах для достижения политических, экономических или иных целей и защиты собственных интересов, а под более широким понятием «информационная борьба» понимаются формы противоборства сторон, которые представляют собой специальные методы, способы и средства воздействия на информационную среду противостоящей стороны и защиты собственной в интересах достижения поставленных целей [6, с 180, 181].

В условиях информационной борьбы субъектов международного публичного права до сих пор не сформирована признанная правовая норма о возникновении права государства на самооборону против недружественной информационной политики других государств и их объединений. Информационные правоотношения, которые возникают

в ходе проведения государственными администрациями информационных операций, нацеленных против интересов других стран – членов международного сообщества, представляют собой пробел в международном публичном праве [6, с. 181].

Соответственно, важным представляется разработка и внедрение международного соглашения в сфере предотвращения и расследования киберагрессии, а также создание международного органа с региональными представительствами [7, с. 34].

Вместе с тем группа экспертов Центра передового опыта НАТО по совместной защите от киберугроз разработала Таллиннское руководство по международному праву, применимое при ведении кибервойны. Это руководство, опубликованное в 2013 году, предусматривает, что государства имеют право применять различные контрмеры против незаконных кибероперациий. Государство, ставшее жертвой «вооруженного нападения» в киберпространстве, повлекшего за собой человеческие жертвы или иной серьезный ущерб, имеет право ответить с помощью силы в киберпространстве или физическом мире [7, с. 33].

Сотрудничество в сфере международной информационной безопасности начинается с разработки правовых механизмов регулирования виртуального пространства на национальном уровне.

18 марта 2019 г. Совет Безопасности Республики Беларусь утвердил Концепцию информационной безопасности Республики Беларусь. Данная Концепция «основывается на соглашениях о сотрудничестве в области обеспечения информационной безопасности государств – участников Содружества Независимых Государств, стран – членов Организации Договора о коллективной безопасности, двусторонних соглашениях и иных обязательствах Республики Беларусь в области международной информационной безопасности, учитывает основные положения актов международных организаций, в том числе резолюций Генеральной Ассамблеи Организации Объединенных Наций, рекомендаций Организации по безопасности и сотрудничеству в Европе» (п. 7, разд. I). В соответствии с п. 13 разд. II «Беларусь последовательно участвует в процессах информатизации на трансграничном контуре, в том числе в рамках Союзного государства Беларуси и России, Евразийского экономического союза, Содружества Независимых Государств, Европейского союза и иных мировых систем политического и экономического взаимодействия и партнерства». Цель обеспечения информационной безопасности определяется как «достижение и поддержание такого уровня защищенности информационной сферы, который обеспечивает реализацию национальных интересов Республики Беларусь и ее прогрессивное развитие» (п. 15, разд. III). В п. 59 разд. V «рассматривается возможность реагирования на кибератаки как на вооруженную агрессию, что в условиях практической невозможности точной идентификации их источников (инициаторов) может привести к бездоказательной и произвольной трактовке обоснованности встречных военных действий». В п. 62 разд. V обозначено, что «перед Республикой Беларусь стоит стратегическая цель развития системы обеспечения кибербезопасности, базирующейся на передовых международных подходах управления рисками и предназначенной для реализации долгосрочных мер по их сокращению до приемлемого уровня» [8].

Таким образом, можно сделать вывод, что информационная сфера является динамично развивающейся системой организованных социальных институтов, которая не может быть подчинена исключительно позитивному праву одного государства. Обеспечение международной информационной безопасности невозможно без создания единых правил, которые были бы выражены в качестве международного акта и признаны большей частью цивилизованных государств [1, с. 102].

Список использованных источников

1. Алиева, М. Н. Проблемы международно-правового сотрудничества в сфере информационной безопасности / М. Н. Алиева // Юридический вест. ДГУ. – 2017. – № 4. – С. 99–103.

2. Ефремов, А. А. Тенденции развития института международной безопасности / А. А. Ефремов // Вест. Воронежского гос. ун-та. Сер. Право. – 2016. – № 4 (27). – С. 293–303.

3. Капитонова, Е. А. Особенности кибертерроризма как новой разновидности террористического акта / Е. А. Капитонова // Известия вузов. Поволжский регион. Общественные науки. – 2015. – № 2 (34). – С. 29–41.

4. Официальный сайт ООН [Электронный ресурс] – Режим доступа: https://undocs.org/ru/A/53/576. – Дата доступа: 18.03.2019.

5. Декларация Совета коллективной безопасности Организации Договора о коллективной безопасности [Электронный ресурс] // Официальный сайт Президента России. – Режим доступа: http://www.kremlin.ru/supplement/5356/prin. – Дата доступа: 18.03.2019.

6. Кириленко, В. П. Международное право и информационная безопасность государства : монография / В. П. Кириленко, Г. В. Алексеев. – СПб. : СПбГИКиТ, 2016. – 396 с.

7. Булай, Ю. Г. Профилактика и противодействие киберпреступности, а также международным киберугрозам / Ю. Г. Булай, Р. И. Булай // Академическая мысль. – 2017. – № 1. – С. 31–35.

8. О Концепции информационной безопасности Республики Беларусь [Электронный ресурс] : постановление Совета Безопасности Респ. Беларусь, 18 марта 2019 г., № I // Официальный интернет-портал Президента Республики Беларусь. – Режим доступа: http://president.gov.by/uploads/documents/2019/1post.pdf. – Дата доступа: 18.03.2019.