процессами, который учитывает системный поход и является его надстройкой. Благодаря наличию оргсистемного подхода, в анализ включается развитие интеграционных объединений и роль ключевых факторов, что в свою очередь позволяет более детально анализировать внутренние процессы, а также моделировать сценарии дальнейшего функционирования интеграционных объединений.

Список использованных источников

1. *Анисимов, А. М.* Общественные резервы – потенциал евразийской интеграции / А. М. Анисимов, С. Ю. Градов // Социальное и гуманитарное сотрудничество в ЕАЭС: реалии и перспективы: сб. науч. ст. XI Евразийского научного форума / под общ. науч. ред. М. Ю. Спириной. – СПб.: Университет при МПА ЕврАзЭС, 2019. – Ч. I. – С. 38–48.

2. *Анисимов, А. М.* К вопросу о планировании и управлении реализацией сверхструктурных проектов в экономике на примере актуальной задачи нефтегазового комплекса / А. М. Анисимов, Е. А. Руденко // Проблемы современной экономики. – 2016. – № 2. – С. 167–172.

3. *Глазьев, С. Ю.* Последняя мировая война / С. Ю. Глазьев. – М.: Книжный мир, 2016. – 512 с.

4. *Глазьев, С. Ю.* Экономика будущего. Есть ли у России шанс? / С. Ю. Глазьев // «Коллекция Изборского клуба». – М.: Книжный мир, 2017. – 640 с.

5. Евразийская интеграция: развитие представлений объективного обществоведения: доклад / А. М. Анисимов [и др.]. – СПб.: СИНЭЛ, 2019. – 174, [1] с.

6. Экономика общественных резервов; общая теория [хозяйственного уклада в форме] общественных резервов: доклад / А. М. Анисимов, С. Ю. Градов, Е. А. Руденко. – СПб.: СИНЭЛ, 2020. – С. 240.

(Дата подачи: 26.02.2021 г.)

Д. В. Драгун
Белорусский государственный университет, Минск

D. V. Dragun
Belarusian State University, Minsk

УДК 323.22

ПОЛИТИЧЕСКАЯ ПРОТЕСТНАЯ КИБЕРАКТИВНОСТЬ: ПОНЯТИЕ, ФОРМЫ И МЕХАНИЗМЫ ПРОТИВОДЕЙСТВИЯ

POLITICAL PROTEST CYBERACTION: CONCEPT, FORMS AND MECHANISMS OF COUNTERACTION

Статья посвящена анализу современных проявлений политической протестной киберактивности, состояния и механизмов противодействия ее противоправным формам. Впервые сформулировано авторское определение термина «политическая протестная киберактивность», предложены авторская классификация форм политической протестной киберактивности и некоторые рекомендации по противодействию противоправным формам политической протестной киберактивности.

Ключевые слова: политическая протестная киберактивность; неконвенциональная форма политической протестной киберактивности; хактивизм; киберэкстремизм; кибертерроризм.

The article is devoted to the analysis of modern manifestations of political protest cyber activity, the state and mechanisms of countering its illegal forms. For the first time, the author's definition of the term "political protest cyber activity" is formulated, the author's classification of forms of political protest cyber activity and some recommendations for countering illegal forms of political protest cyber activity are proposed.

Keywords: political protest cyber activity; an unconventional form of political protest cyber activity; hacktivism; cyber extremism; cyber terrorism.

Жизнь современного общества отмечена стремительным развитием компьютерных технологий, масштабным ростом числа пользователей сети Интернет в общемировом [1] и национальном сегментах [2, с. 23], всеобщей киберинтеграцией [3, с. 16–17]. Изменения, продуцируемые диджитализацией общественной жизни, охватывают различные ее стороны: будь то политика, государственное управление, микро- и макроэкономика, образование, наука или культура.

Такие многочисленные преимущества киберпространства, как: неограниченный и постоянно расширяющийся круг пользователей; возможность низкобюджетного и оперативного распространения информации в рамках целевой аудитории посредством мультимедийных технологий; право анонимного доступа пользователей; недостижимость всеохватывающего анализа размещенной информации; невозможность полномасштабного ограничения доступа к ней [4, с. 159; 5, с. 6–7; 6, с. 125], трансформируют его, с одной стороны, в благоприятную среду осуществления политической протестной активности и, с другой стороны, в эффективный инструмент ее организации.

Отечественная и зарубежная наука в последние годы уделяет пристальное внимание различным аспектам политической протестной киберактивности. Существенный вклад в разработку данной темы внесли западные ученые: Ф. Бардо, С. Вилсон, Д. Деннинг, М. Кастельс, Б. Коллин, П. Олсон, Ф. Паже, М. Поллит, Д. Рейнсель, А. Сэмюэль и другие. Ряд аспектов данной проблематики получил отражение в трудах таких белорусских, украинских, российских ученых и аналитиков, как: Л. А. Бураева, В. Б. Вехов, Д. Н. Карпова, Д. А. Ковлагина, В. А. Копылов, Е. А. Кошечкина, Е. Н. Молодчая, Н. О. Мороз, С. Г. Туронок, Н. А. Швед и др.

Новизна темы данной статьи обусловлена появлением новых форм политической протестной деятельности, их активной популяризацией политическими акторами, и, несмотря на значительный объем публикаций по теме работы, остается широкий спектр вопросов, требующих дополнительных исследовательских усилий именно с политологических позиций.

Цель статьи – раскрыть понятие, формы и механизмы противодействия политической протестной киберактивности.

Появление киберпространства, как уникальной скоростной, гибкой и общедоступной среды, существенно облегчающей создание, хранение, распространение и обсуждение социально-политической информации, повлекло возникновение новых, «виртуальных» форм политических протестов, для обозначения которых предлагаем использовать термин *«политическая протестная киберактивность»*. Под *политической протестной киберактивностью* понимается совокупность конвенциональных или неконвенциональных индивидуальных или коллективных практик выражения недовольства по отношению к политической

системе общества или отдельным ее элементам посредством глобальной компьютерной сети Интернет.

Политическая протестная киберактивность имеет универсальный характер воздействия на социум, так как охватывает практически все сферы жизни общества. В силу практически стопроцентного внедрения в общества развитых стран цифровых технологий «киберпротестующие» получают колоссальный простор возможностей.

Во-первых, это связано с тем, что политическая протестная киберактивность характеризуется большей рентабельностью по сравнению с традиционными методами ведения борьбы. Для участия в виртуальной протестной деятельности требуется компьютер и стабильное и быстрое Интернет-соединение, что, как правило, обходится намного дешевле и легче при осуществлении, чем организация традиционных массовых мероприятий, если речь идет о конвенциональной форме политического протеста, или приобретение традиционных видов вооружений, если речь идет о кибертерроризме. Кроме того, в последнем случае такой метод борьбы не предполагает гибели нападавшего, как это имеет место с террористами-смертниками [7, с. 211].

Во-вторых, имеется возможность анонимного участия в политической протестной киберактивности, что провоцирует неспособность правоохранительных органов полноценно осуществлять меры противодействия неконвенциональным ее проявлениям.

В-третьих, политическая протестная киберактивность осуществляется удаленно, без непосредственного физического контакта с материальным миром. Это может привести к транснациональному характеру рассматриваемой деятельности.

В-четвертых, целевой аудиторией киберпротестного воздействия будет являться большее число людей, чем при использовании традиционных методов политического протеста, что связано со всепроникающим характером киберпространства. Отметим, что наиболее подверженной такому воздействию группой населения является молодежь.

В данном контексте необходимо указать на некоторые тенденции развития политической протестной киберактивности, характерные для современного этапа эволюции социума. Это, в первую очередь, беспрерывный рост общемирового уровня популярности виртуальных форм протеста на фоне все большей цифровизации традиционных его форм. Так, социальные сети и мессенджеры обрели широкое применение для информационной поддержки протестующих. Более того, в рамках сети Интернет формируется выразительная организационная структура деятельности протестных акторов, обмена информацией, согласования проводимых акций, что способствует вовлечению в политическую протестную киберактивность новых участников из различных слоев населения. И, наконец, под воздействием обострения идеологических, конфессиональных и политических конфликтов политическая протестная киберактивность становится долговременным фактором политического процесса.

Однако, несмотря на вышеуказанные аспекты политической протестной киберактивности, свидетельствующие об актуальности исследований в данной сфере, в современной политической науке не выработана четкая классификация виртуальных форм политического протеста. Так, российский политолог Р. И. Шарапов к таковым относит, с одной стороны, протестную деятельность

в социальных сетях и блогосфере и, с другой стороны, политически мотивированные кибератаки [8, с. 99], не указывая, однако, четких критериев классификации.

В данном контексте представляется необходимым предложить *авторскую классификацию форм политической протестной киберактивности*. В ее основу следует положить критерий соответствия виртуального протеста действующим нормативным правовым актам. Формы политической протестной киберактивности в таком случае подразделяются на *конвенциональные и неконвенциональные*.

Конвенциональная форма политической протестной киберактивности представляет собой совершение значимых действий, осуществляемых посредством инструментов сети Интернет и не выходящих за рамки действующего законодательства, которые демонстрируют критическое отношение актора к сложившейся политической системе общества или отдельным ее элементам. Это может выражаться, например, в ведении протестных каналов/групп в социальных сетях и мессенджерах и выражении негативной оценки в комментариях к официальным публикациям государственных органов и должностных лиц. В данном ракурсе нельзя не отметить и появившийся недавно феномен так называемых «онлайн-митингов» на платформах Zoom, YouTube, «Яндекс.Карты» и «Яндекс.Навигатор» [9, с. 17].

В свою очередь, *неконвенциональная форма политической протестной киберактивности* отличается противоправным характером совершаемых актором действий. В зависимости от общественной опасности в неконвенциональной политической протестной киберактивности можно выделить:

I. Хактивизм как незаконное использование компьютерных технологий для достижения политических целей. Особенностями хактивизма являются его ненасильственный характер и отсутствие серьезного ущерба, наносимого критически важной инфраструктуре, жизни и здоровью населения.

II. Киберэкстремизм как деятельность по созданию, хранению и распространению посредством сети Интернет информации экстремистского характера с целью оказания деструктивного воздействия на психику людей для достижения политических целей. Для отнесения информации к разряду экстремистской, она должна соответствовать следующим признакам:

1. Содержать отрицательную эмоциональную оценку объекта повествования (нации, расы, религии).

2. Формировать негативную установку по отношению к данному объекту.

3. Подстрекать к действиям, направленным против объекта повествования [10, с. 20].

III. Кибертерроризм как атаки на информационные системы, несущие угрозу здоровью и жизни людей, а также способные спровоцировать серьезные нарушения функционирования критически важных объектов в целях оказания воздействия на принятие решений органами власти и управления, воспрепятствования политической или иной общественной деятельности, устрашения населения и дестабилизации общественного порядка [11]. К особенностям данной неконвенциональной формы политической протестной киберактивности следует отнести следующие:

1. Кибертерроризм порождает реальную опасность для неопределенного круга лиц, которая возникает в результате угрозы совершения или претворения в жизнь общественно опасных действий.

2. Акт кибертерроризма представляет собой форму публичного насилия, рассчитанную на массовую ретрансляцию в средствах массовой информации.

3. Целью кибертерроризма является формирование социально-психологической обстановки напряженности, апатии и страха, провоцирующей те или иные деяния в интересах кибертеррористов со стороны государственных органов и гражданского общества.

4. При кибертеррористическом акте общеопасное насилие применяется для психологического воздействия и склонения к определенному поведению других лиц.

На современном этапе наиболее характерным проявлением неконвенциональной формы политической протестной киберактивности является хактивистская деятельность децентрализованного киберактивистского движения «Anonymous», киберактивистских группировок «Анонимный интернационал», «Киберберкут» и «Киберпартизаны».

Отдельного упоминания заслуживает инструментарий неконвенциональной формы политической протестной киберактивности. При совершении кибератак в информационном пространстве чаще всего используются получение незаконного доступа к личной, коммерческой, банковской информации, к государственным и военным секретам; нанесение ущерба физическим элементам информационного пространства; уничтожение информации, программного обеспечения, технических ресурсов путем внедрения вирусов, программных закладок, преодоления систем защиты; техническое внедрение в каналы трансляции средств массовой информации с целью распространения слухов, дезинформации, объявления требований террористической организации; уничтожение или подавление работы линий связи, перегрузка узлов коммуникации, изменение адресации запросов в сети Интернет [12, с. 34].

В настоящий момент международно-правовое сотрудничество в борьбе с неконвенциональными формами политической протестной киберактивности находится на начальном этапе развития. Основы такого сотрудничества на международном уровне заложены Резолюцией Генеральной ассамблеи Организации Объединенных Наций № 56/261 от 31 января 2002 года «Планы действий по осуществлению Венской декларации о преступности и правосудии: ответы на вызовы XXI века». На региональном уровне приняты Будапештская Конвенция Совета Европы «О преступности в сфере компьютерной информации» от 23 ноября 2001 года, Соглашение между правительствами государств-членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения информационной безопасности, Конвенция Лиги арабских государств о борьбе с преступлениями в области информационных технологий от 21 декабря 2010 года.

Противодействие противоправным формам политической протестной киберактивности в Республике Беларусь осуществляется как в рамках общей системы противодействия преступлениям в сфере информационных технологий, экстремизму и терроризму, так и в рамках системы обеспечения информационной безопасности.

Субъектами, непосредственно осуществляющими борьбу с противоправными формами политической протестной киберактивности в пределах своей компетенции, являются органы государственной безопасности Республики Беларусь, органы внутренних дел Республики Беларусь, Служба безопасности

Президента Республики Беларусь, Вооруженные Силы Республики Беларусь, органы пограничной службы Республики Беларусь. Общее руководство осуществляют Президент Республики Беларусь и Совет Министров Республики Беларусь [13; 14]. Координация деятельности вышеназванных субъектов осуществляется посредством Комиссии по противодействию экстремизму и борьбе с терроризмом [15].

Основными направлениями противодействия неконвенциональным формам политической протестной киберактивности являются предупреждение, выявление и пресечение противоправной киберактивистской деятельности в киберпространстве и минимизация последствий актов противоправного политического протестного киберактивизма [16]. Приоритетным направлением является предупреждение, которое состоит в устранении причин и условий популярности противоправных цифровых методов борьбы; оказании профилактического воспитательного воздействия на склонных к радикальной и насильственной деятельности лиц; прогнозировании угроз безопасности критически важным информационным системам, подлежащим первоочередной защите; создании эффективной системы защиты информационных систем от воздействия извне; повышении уровня правовой грамотности и цифрового этикета.

Выявление и пресечение противоправной протестной политической деятельности в киберпространстве осуществляются путем своевременного получения и анализа информации о подготовке и совершении в отношении Республики Беларусь или ее резидентов кибератак, призванных дестабилизировать общественный порядок, создать в социуме атмосферу страха, оказать воздействие на принятие решений государственными органами, воспрепятствования политической или иной общественной деятельности; предотвращения данных кибератак и установления и розыска лиц, причастных к их совершению.

Минимизация последствий неконвенциональных форм политической протестной киберактивности выражается в сведении к наименьшему количеству числа пострадавших от негативных последствий, причиненных кибератаками; ликвидации чрезвычайных ситуаций техногенного характера; форсированном восстановлении разрушенной инфраструктуры; минимизации размеров ущерба и материальных потерь и их возмещении физическим и юридическим лицам. Особого внимания требует нейтрализация морально-психологического воздействия и социальная реабилитация лиц, пострадавших в результате совершения противоправных актов политической протестной киберактивности.

Эффективность противодействия неконвенциональным формам политической протестной киберактивности обусловлена качеством обеспечения информационной безопасности, которое зависит от эффективности государственного реагирования на риски, вызовы и угрозы в информационной сфере и лежит в плоскости построения информационной инфраструктуры и информационных ресурсов, устойчивых к противоправным воздействиям. Немаловажным направлением обеспечения информационной безопасности является защита информации, неправомерные действия в отношении которой могут причинить вред ее обладателю, пользователю или иному лицу.

Таким образом, на основании проведенного в данном исследовании анализа противоправных форм политической протестной киберактивности можно сделать выводы о необходимости:

I. На международном уровне:

• выработать международные нормативные правовые акты в сфере совместной профилактики, выявления и предотвращения противоправных актов политической протестной киберактивности;

• создать международный орган, основной задачей которого будет объединение усилий национальных правоохранительных органов стран-участниц в области борьбы с киберпреступностью и противоправными формами политической протестной киберактивности.

II. На национальном уровне:

• закрепить кибертерроризм в качестве отдельного состава уголовно наказуемого деяния. При этом объектами данного деяния будут являться критически важные объекты информатизации, обеспечивающие жизнедеятельность населения и функционирование основных отраслей экономики, связь и системы коммуникации, а также те объекты, нарушение или прекращение функционирования которых может причинить ущерб окружающей среде;

• сформировать и укомплектовать двухуровневую систему органов кибербезопасности, включающую в себя:

1) научно-аналитический уровень, в рамках которого будут анализироваться угрозы кибербезопасности государства и разрабатываться методы по их устранению и минимизации;

2) исполнительный уровень, в рамках которого будут реализовываться меры по противодействию киберугрозам:

• повсеместно внедрить в учебные программы подготовки специалистов профессионально-технического, средне-специального и высшего образования специализированные дисциплины, формирующие у обучающихся «цифровые» навыки.

Список использованных источников

1. Новые данные МСЭ свидетельствуют как о растущем распространении интернета, так и о расширяющемся цифровом гендерном разрыве [Электронный ресурс] // Международный союз электросвязи. – 2019. – Режим доступа: https://www.itu.int/ru/mediacentre/Pages/2019-PR19.aspx. – Дата доступа: 12.01.2021.

2. Информационное общество в Республике Беларусь / Национальный Статистический Комитет Республики Беларусь; под общ. ред. И. В. Медведевой. – Минск, 2019. – 101 с.

3. *Ковалев, М. М.* Цифровая экономика – шанс для Беларуси: моногр. / М. М. Ковалев, Г. Г. Головенчик. – Минск: Изд. центр БГУ, 2018. – 327 с.

4. *Петрянин, А. В.* Уголовно-правовые, оперативно-розыскные и криминалистические механизмы противодействия экстремизму в телекоммуникационных сетях и сети «Интернет»: на примере статьи 280 УК РФ / А. В. Петрянин // Юридическая наука и практика: Вестник Нижегородской академии МВД России. – 2016. – № 1. – С. 158–161.

5. *Булах, Е. В.* Преимущества интернета как среды политической коммуникации в современном обществе / Е. В. Булах // Общество. Среда. Развитие. – 2015. – № 3. – С. 4–7.

6. *Валеев, А. Х.* Борьба с проявлением экстремизма в сети Интернет / А. Х. Валеев // Проблемы экономики и юридической практики. – 2011. – № 6. – С. 125–127.

7. *Драгун, Д. В.* Кибертерроризм – новая и наиболее опасная форма терроризма в условиях цифровизации белорусского государства / Д. В. Драгун // У истоков и в авангарде белорусской политологии: материалы науч. конф., посвящ. 30-летию кафедры политологии

Белорус. гос. ун-та, Минск, 27 нояб. 2020 г. / Белорус. гос. ун-т; редкол.: Н. А. Антанович (гл. ред.) [и др.]. – Минск: БГУ, 2020. – С. 209–214.

8. *Шарапов, Р. И.* Особенности виртуальных форм современного политического протеста / Р. И. Шарапов // Известия Саратовского университета. Новая серия. Серия Социология. Политология. – 2016. – № 1. – С. 97–101.

9. *Ильина, Е. М.* Цифровая трансформация политического участия / Е. М. Ильина // Современные инновационные технологии и проблемы устойчивого развития в условиях цифровой экономики: сб. ст. XIV междунар. науч.-практ. конф., Минск, 15 мая 2020 г. / Минский филиал РЭУ им. Г. В. Плеханова; редкол.: А. Б. Елисеев, И. А. Маньковский (гл. ред.) [и др.]. – Минск: СтройМедиаПроект, 2020 – С. 17.

10. Экстремистский текст и деструктивная личность / Ю. А. Антонова [и др.]; Уральский гос. пед. ун-т; под общ. ред. Ю. А. Антоновой. – Екатеринбург, 2014. – 276 с.

11. Об утверждении Концепции информационной безопасности Республики Беларусь: Постановление Совета Безопасности Респ. Беларусь, 18 марта 2019 г., № 1: в ред. Постановления Совета Безопасности Респ. Беларусь от 18.03.2019 г. // Нац. правовой Интернет-портал Респ. Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2019. – Режим доступа: http://www.pravo.by/document/?guid=12551&p0=P219s0001&p1=1. – Дата доступа: 12.01.2021.

12. *Прокопьева, В. А.* Политика противодействия кибертерроризму в современной России / В. А. Прокопьева // Вестник социально-гуманитарного образования и науки. – 2016. – № 4. – С. 31–38.

13. О противодействии экстремизму: Закон Респ. Беларусь, 4 янв. 2007 г., № 203-З: в ред. Закона Респ. Беларусь от 18.07.2019 г. // Нац. правовой Интернет-портал Респ. Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2019. – Режим доступа: http://www.pravo.by/document/?guid=3871&p0=H10700203. – Дата доступа: 12.01.2021.

14. О борьбе с терроризмом: Закон Респ. Беларусь, 3 января 2002 г., № 77-З: в ред. Закона Респ. Беларусь от 09.01.2018 г. // Комитет государственной безопасности Республики Беларусь [Электронный ресурс]. – 2018. – Режим доступа: http://kgb.by/ru/zakon77-3. – Дата доступа: 12.01.2020.

15. О комиссии по противодействию экстремизму и борьбе с терроризмом: Указ Президента Респ. Беларусь, 17 авг. 2015 г., № 356 // Нац. правовой Интернет-портал Респ. Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2015. – Режим доступа: http://www.pravo.by/document/?guid=12551&p0=P31500356&p1=1. – Дата доступа: 12.01.2021.

16. Об утверждении Концепции борьбы с терроризмом в Республике Беларусь: Постановление Совета Министров Респ. Беларусь, 25 июля 2013 г., № 658: в ред. Постановления Совета Министров Респ. Беларусь от 27.07.2015 г. // Нац. правовой Интернет-портал Респ. Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2015. – Режим доступа: http://www.pravo.by/document/?guid=3871&p0=C21300658. – Дата доступа: 12.01.2021.

(Дата подачи: 22.02.2021 г.)