риски. Кроме того, государствам-союзникам следует не только совершенствовать национальные Концепции информационной безопасности, но и согласовывать общецивилизационные меры противодействия угрозам и рискам масштабных кибератак, прилагать совместные усилия по разработке новых норм законодательства.

Список источников:

1. Котляров, И. В. Современная цивилизация: парадигма для XXI века. / И. В. Котляров //Иппокрена. – 2020. – №2. – С. 136–154.
2. Садовая, Е. С. Формирование новой социальной реальности: технологические вызовы / Е .С. Садовая, В. А. Сауткина, А. Р. Зенков. – М. : ИМЭМО РАН, 2019. – 190 с.
3. Гухман, В. Б. Информационная цивилизация/ В. Б. Гухман // Вестник ТвГУ. – 2019. – № 1(47). – С. 37–48.
4. Тоффлер, Э. Третья волна / Э. Тоффлер. – М. : Издательство «АСТ», 2009. – 800 с.
5. Шеховцев, Н. П. Информационное оружие: теория и практика применения в информационном противоборстве [Электронный ресурс] / Н. П. Шеховцев, Ю. Е. Кулешов. – Режим доступа: http://pentagonus.ru. – Дата доступа: 14.08.2021.

***Л.В. Николаева**, доцент*
Mikalayeva@bsuir.by
БГУИР (Минск)

ИНФОРМАЦИОННЫЙ ЭКСТРЕМИЗМ В КОНТЕКСТЕ ЦИФРОВОЙ ТРАНСФОРМАЦИИ ОБЩЕСТВА

Глобальное проникновение информационно-коммуникационных технологий (далее – ИКТ) и виртуализация ключевых сфер общественно-политической сферы вызвали к жизни складывание постинформационной среды, а также непосредственно отразились на работе органов государства [4, с. 12]. Глобализация содействовала формированию мирового информационного сообщества. Характеризуя ключевые тенденции современного мира, исследователи отмечают, что с развитием ИКТ, Интернета информационные потоки приобрели транснациональный характер. В таких условиях информационная сфера стала оказывать всеобъемлющее влияние на социально-экономические (включая использование криптовалют и иных цифровых финансовых активов) и общественно-политические процессы, происходящие в различных странах [1, с. 57; 2, с. 54]. С помощью ИКТ оказывается всеобъемлющее воздействие на общественные настроения, в первую очередь – молодежь. Кибербезопасность приобрела исключительное значение на уровне обеспечения национальной безопасности. Оперативное внедрение передовых разработок по совершенствованию средств вооруженной борьбы отражается на

способах и формах применения вооруженных сил, в т.ч. за счет их дальнейшей гибридизации [2, с. 54].

Помимо новых перспектив, которые открылись перед государствами в складывающихся условиях, также все более очевидным становится появление угроз и вызовов нового типа. В их числе – опасность манипуляции сознанием человека, информационный экстремизм и терроризм [3; 4, с. 15–16; 5, с. 62]. Прогнозы на будущее отмечают, что по-прежнему сохраняется опасность международного терроризма, который уже вооружен передовыми технологиями. Террористические организации активно используют ИКТ в целях пропаганды и финансирования терроризма, переброски сил и средств, массового распространения информации о прошедших терактах для нагнетания страха, а также увеличения численности своих сторонников [1, с. 57; 2, с. 54].

Негативные информационно-коммуникационные эффекты в наше время проявляются более зримо, чем положительные. Одним из них является трансформация облика «классического» экстремизма, что привело в начале XXI в. к появлению такой его разновидности, как информационный экстремизм [5, с. 62]. Современные исследователи под «экстремизмом» понимают прежде всего жесткую радикальную позицию, пропаганду крайних политических мер [3; 4, с. 16]. Понятие «экстремизм» в правовом аспекте следует рассматривать как организацию и подготовку антигуманных и преступных деяний, а также подстрекательство к их совершению [6, с. 303].

Исследователи справедливо обращают внимание на такой качественный признак экстремизма, как способность к адаптации к социальным изменениям [5, с. 62]. Прежде в образе профессионального экстремизма присутствовали такие его отличительные черты, как руководство определенной идеологией, националистическими устремлениями, действие согласно определенным политическим целям и открытое финансирование со стороны правящих элит в некоторых странах. Теперь этот привычный образ постепенно исчезает. Поскольку в случае информационного экстремизма даже один человек, руководствующийся экстремистскими мотивами, потенциально может стать по своему масштабу более разрушительным, чем самые многочисленные группировки экстремистского толка [6, с. 305].

Под информационным экстремизмом понимается «деятельность, связанная с: а) созданием, хранением и (или) распространением информации, содержащей предусмотренные законом признаки экстремистской деятельности в политической, экономической и культурной сферах; б) использованием информации, обрабатываемой компьютером, компьютерной системы и (или) компьютерной сети, осуществляемым в целях воздействия на принятие решений органами государственной власти, органами местного самоуправления или международными организациями, сопряженным с различными формами психического или опосредованного физического насилия (кибертерроризм); в) использованием информации, оказывающей деструктивное влияние на психику людей, не осознаваемое ими» [4, с. 19-20; 5, с. 62-63]. Иными словами, «информационный экстремизм – это деятельность, осуществляемая с

использованием информационных технологий, сопряженная с формами социально-психического и опосредованного физического деструктивного влияния, результатом которого является достижение публично нелегитимных и противоправных целей. Признаком информационного экстремизма является нанесение законным интересам, правам и свободам граждан физического, материального, морального и иного ущерба» [7, с. 7].

Как отмечают исследователи, «информационный экстремизм характеризуется следующими общими и специфическими параметрами: 1) радикальностью (экстраординарностью) действий в достижении каких-либо целей, реализации интересов» 2) антисоциальностью, поскольку нарушает исторически сложившиеся (типичные), позитивные формы и модели социально-правового взаимодействия, подрывает существующий баланс интересов, создавая между ними конфликтогенное пространство взаимодействия; 3) аморальностью, т.к. всегда идет вразрез с духовно-нравственными нормами, направлен на их нивелировку и разрушение, поскольку кризис духовно-нравственного пространства, фрагментарность его функционирования открывает простор для интенсивного развития экстремистской деятельности; 4) институциональностью – он «вызревает» и институционализируется в пограничных условиях и маргинальных пространствах; 5) искажением политико-правового мышления, поскольку субъект экстремистской деятельности обладает чаще всего деформированным сознанием, что обусловливает его отчуждение от социально-культурных и политико-правовых норм и ценностей; 6) противоправностью результатов, поскольку функционирование информационного экстремизма в ряде случаем соответствует закону, но реализует предоставленные возможности в противоположных целях» [3; 4, с. 20; 5, с. 63; 7, с. 7].

Выделяются две основные формы информационного экстремизма: 1) информационная диверсия, направленная на разрушение информационных коммуникаций; 2) бескомпромиссная борьба за власть, направленная на подрыв ценностей общества за счет использования ИКТ, крайней мерой которой является информационный терроризм [6, с. 306]. Поиск сторонников, их сплочение, непримиримая борьба с противником, четкая формулировка и обстоятельное разъяснение собственной позиции – все это в полной мере определяет содержание экстремистской коммуникации. Объектами экстремистского воздействия могут быть как отдельные индивиды, так и население в целом. При этом субъектами экстремистского дискурса прилагаются усилия к тому, чтобы экстремистская аудитория была как можно более многочисленной, что связано с спецификой массового внушения и убеждения. Чем больше будет аудитория, тем больше будет исполнителей воли субъекта. Последнему нет большой разницы в том, на какие категории населения направлено его воздействие (рабочие, служащие, интеллигенция, мужчины, женщины, молодежь, пожилые люди и др.) [6, с. 307-308]. Однако в силу особой вовлеченности в сферу ИКТ сегодня наибольший социологический контингент

информационного экстремизма составляет именно молодежь, что вызывает особую тревогу [3; 4, с. 20; 5, с. 63].

Таким образом, информационный экстремизм – подготовительная ступень для других видов экстремизма – молодежного, националистического, политического, религиозного и др. Он формирует благоприятную среду для распространения и принятия экстремистских идей и идеалов [6, с. 311]. С учетом современного развития ИКТ данный вид экстремизма, к сожалению, имеет свое будущее, его потенциальные возможности не ограничены. Мощным инструментом противодействия информационному экстремизму может стать социокультурное, духовно-нравственное воздействие на личность, а также кропотливая, продуманная, продолжительная работа по реализации программ информационной безопасности.

Список источников:

1. Коваленя, А. Обеспечение национальной безопасности в контексте тенденций развития современного мира / А. Коваленя, В. Арчаков, А. Баньковский // Беларуская думка. – 2021. – № 8. – С. 54–60;
2. Коваленя, А. Обеспечение национальной безопасности в контексте тенденций развития современного мира / А. Коваленя, В. Арчаков, А. Баньковский // Беларуская думка. – 2021. – № 9. – С. 50–55.
3. Матвеева, Е. Ю. Информационный экстремизм: сущность и проявления / Е. Ю. Матвеева, И. В. Носова [Электронный ресурс]. – Режим доступа : http://www.oboznik.ru/?p=61182 . – Дата доступа : 12.11.2021.
4. Мигун, Д. А. Информационный экстремизм и информационная безопасность / Д.А. Мигун. – Минск : РИВШ, 2020. – 64 с.
5. Мозговой, В. Э. Информационный экстремизм как инновационная девиация социума начала XXI века / В. Э Мозговой [Электронный ресурс]. – Режим доступа : https://cyberleninka.ru/article/n/informatsionnyy-ekstremizm-kak-innovatsionnaya-deviatsiya-sotsiuma-nachala-xxi-veka. – Дата доступа : 12.11.2021.
6. Пономарев, В. А. Информационный экстремизм и информационный терроризм в пространстве PR-технологий, СМИ и открытой информационной сети (Интернет): концептуальный аспект / В. А. Пономарев // Вопросы теории и практики журналистики. – 2018. – Т. 7. – № 2. – С. 301–319 [Электронный ресурс]. – Режим доступа : http://jq.bgu.ru/reader/article.aspx?id=22031 . – Дата доступа : 12.11.2021.
7. Упорников, Р. В. Политико-правовые технологии противодействия информационному экстремизму в России : автореф. дис. … кандидата юридических наук : 23.00.02 / Р. В. Упорников. – Ростов-на-Дону, 2007. – 25 с.