

## **ВЫЗОВЫ СОВРЕМЕННОСТИ: КИБЕРЭКСТРЕМИЗМ**

**Мядель Александр Павлович,**

Витебский государственный технологический университет

(г. Витебск, Республика Беларусь)

*Раскрывается содержание понятия «экстремизм» и обосновывается особая опасность его разновидности – киберэкстремизма. Выявляются истоки киберэкстремизма и факторы его распространения в молодежной среде. Определяется роль системы образования в противодействии экстремистским проявлениям.*

Нестабильность социально-экономического развития, девальвация традиционных ценностей, идеологический вакуум как следствие разрушения тоталитарной идеологии в той или иной мере присущи всем государствам постсоветского пространства. Эти факторы создают питательную среду для разного рода экстремистских проявлений. Экстремизм – неизбеж-

ное порождение кризисного состояния социума. В широком смысле слова это понятие обозначает мировоззренческую установку, характеризующуюся радикальными взглядами и действиями преимущественно в политической сфере. На личностном уровне школа психоанализа связывает природу экстремизма с кризисом идентичности. Угроза потери индивидуальной или коллективной идентичности создает предпосылки агрессивных проявлений субъекта экстремизма по отношению к реальным или предполагаемым оппонентам. Таким образом, экстремизм предполагает самоутверждение через ненависть к носителям других взглядов. При этом американский исследователь-социолог Лейард Уилкокс выделяет до 22 симптоматических признаков экстремиста, которые позволяют выявить потенциальный источник угрозы [1, с. 17–19].

Развернутое правовое определение экстремизма содержит Закон Республики Беларусь «О противодействии экстремизму». Данный документ возможными субъектами экстремизма называет граждан Республики Беларусь, иностранных граждан или лиц без гражданства либо политических партий, других общественных объединений, религиозных и иных организаций, а экстремизмом – широкий спектр деятельности от насильственного изменения конституционного строя до публичных призывов к подобным действиям, включая создание экстремистских организаций, осуществление террористической деятельности, разжигание расовой, национальной, религиозной либо иной социальной вражды или розни и т.д. [2].

Бурное развитие информационных и телекоммуникационных технологий стимулировало появление качественно новой формы экстремизма – киберэкстремизма, т.е. экстремизма в киберпространстве. Данная форма экстремистской деятельности представляет особую опасность, поскольку затрагивает в значительной степени молодежь. Именно эта демографическая группа составляет большинство пользователей сети Интернет. Так, по результатам социологических исследований, приоритетным источником информации для 70% молодых людей в Беларуси является Интернет. При этом 77,2% заходят в Сеть ежедневно [3, с. 163]. Следует также иметь в виду, что за прошедшие десять с лишним лет со времени проведения данных исследований эти показатели, несомненно, выросли. Молодое поколение в то же время отличается повышенной эмоциональностью, которая преобладает над рациональными инструментами восприятия действительности. Для молодежи в силу ее возрастных особенностей характерен радикализм оценок и контрастность в отражении реальности. Завышенные ожидания в сочетании с невозможностью их немедленной реализации вызывают стремление уйти от реальных проблем в мир виртуальных иллюзий.

Особенностью киберпространства является его доступность: современные гаджеты позволяют заходить во всемирную паутину в любое время суток. Фактором риска выступает практически неограниченная свобода в сети Интернет, что способствует благоприятным условиям образования экстремистских интернет-сообществ и широкому распространению их влияния. Ощущение безграничной свободы и безнаказанности порождается также возможностью сохранения инкогнито в виртуальном пространстве. Использование разных никеймов, выход в Интернет с разных типов устройств обеспечивают высокую степень анонимности пользователей. Цензура в Интернете в этом случае представляется малоэффективной вследствие простоты и легкости создания новых сайтов экстремистской направленности взамен заблокированных.

Основными направлениями экстремистской деятельности в виртуальной среде являются распространение экстремистских материалов, призывов к насилию и кибератаки информационных ресурсов государственных структур, политических партий, общественных движений и организаций, персональных сайтов, страниц в социальных сетях государственных и общественных деятелей. Целью подобных акций является как хищение конфиденциальной информации, так и размещение на «взломанных» ресурсах недостоверных и клеветнических сведений. Крайним проявлением киберэкстремизма является кибертерроризм, который направлен на разрушение систем жизнеобеспечения, внедрение вирусов в компьютерные сети органов государственной власти и управления, координацию деятельности террористических группировок и т.п. От «обычной» киберпреступности терроризм в виртуальном пространстве всегда отличает наличие соответствующего идеологического обоснования.

Большинство молодых пользователей Интернета отдают предпочтение досуговым и развлекательным сервисам Сети. Это обстоятельство также может быть использовано в интересах экстремистских группировок. Речь идет о создании компьютерных игр, культивирующих агрессию и нетерпимость, разжигающих религиозную, национальную и социальную вражду. Внешне безобидные «стрелялки» формируют у молодых людей определенный образ врага, который подлежит неизбежному уничтожению.

Риски и угрозы, которые несут современные информационные технологии, вполне осознаются обществом и формируют запрос на создание эффективной системы противодействия им. В сфере законодательства требуется постоянное совершенствование правовой базы регулирования национального сегмента Интернета. В области высоких технологий представляется актуальным создание информационных продуктов, способных обнаружить и блокировать контент экстремистской направленности. Реше-

ние этой задачи возможно лишь при наличии качественного человеческого капитала – высококлассных специалистов в области информационной безопасности.

Особая роль в противодействии киберэкстремизму принадлежит системе образования. Именно в учебных заведениях закладываются основы правовой и политической культуры личности. При изучении дисциплин социально-гуманитарного цикла молодые люди получают теоретические знания о сущности и последствиях экстремистской деятельности. Крайне важно, чтобы этот теоретический багаж находил свое практическое применение во внеучебной деятельности: в структурах ученического и студенческого самоуправления, а также в волонтерских инициативах.

### **Список источников**

1. Кугай, А. И. Экстремизм: природа, симптоматика, опыт и условия противодействия / А. И. Кугай // *Управленческое консультирование*. – 2015. – № 2. – С. 16–26.
2. Закон Республики Беларусь «О противодействии экстремизму» // Национальный правовой Интернет-портал Республики Беларусь [Электронный ресурс]. – Режим доступа: <https://www.pravo.by/document/>. – Дата доступа: 06.11.2020.
3. Молодежь суверенной Беларуси: штрихи к портрету / Д. М. Булышко [и др.]; под ред. Д. М. Булышко, О. В. Иванюто, Д. Г. Ротмана. – Минск : Изд. центр БГУ, 2012. – 192 с.