УДК 343.3

ПРОФИЛАКТИКА ЭКСТРЕМИЗМА В СЕТИ ИНТЕРНЕТ

Морозов Андрей Владимирович,
Шкловский районный отдел
Следственного комитета Республики Беларусь
(г. Шклов, Республика Беларусь)

В статье раскрывается содержание понятия «экстремизм», акцентируется внимание на экстремизме в сети Интернет, т.е. на киберэкстремизм, выявляются истоки киберэкстремизма, факторы его распространения в молодежной среде, а также предлагаются мероприятия, необходимые для профилактики экстремизма в сети Интернет.

Сеть Интернет в настоящее время становится мощным средством преступной деятельности. Эта тенденция в полной мере коснулась и экстремизма. Экстремизм – неизбежное порождение кризисного состояния социума. В широком смысле слова это понятие обозначает мировоззренческую установку, характеризующуюся радикальными взглядами и действиями преимущественно в политической сфере. 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, осуществлением 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 (глобальная сеть Интернет). 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.

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, ко-

торый 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.

Риски и угрозы, которые несут современные информационные технологии, вполне осознаются обществом и формируют запрос на создание эффективной системы противодействия им. В сфере законотворчества 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. Решение 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.

Полагаем, что важно осуществлять борьбу с экстремизмом и терроризмом, использующими возможности сети Интернет, не только постфактум, но и в рамках криминалистического предупреждения. Для этого необходима выработка системы соответствующих правовых, организационных, технических и методических мер, носящих комплексный характер. Особую роль стоит отвести созданию специализированной программы профилактики таких преступлений. Ее основная функция должна быть сосредоточена на повышении уровня правовой культуры населения и противодействии распространению информации экстремистской или террористической направленности на популярных интернет-ресурсах. Простое закрытие сайтов, содержащих запрещенный контент, как это происходит в настоящее время, имеет низкую результативность. Полагаем, что применение специализированной программы профилактики таких преступлений будет более эффективным.

Риски и угрозы, которые несут современные информационные технологии, вполне осознаются обществом и формируют запрос на создание эффективной системы противодействия им. В сфере законотворчества 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. Решение 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. О противодействии экстремизму [Электронный ресурс] : Закон Республики Беларусь, 4 января 2007 г., № 203-З : в ред. Закон Республики Беларусь от 14 мая 2021 г., № 104-З // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2021.
3. Молодежь суверенной Беларуси: штрихи к портрету / Д. М. Булынко [и др.] ; под ред. Д. М. Булынко, О. В. Иванюто, Д. Г. Ротмана. – Минск : Изд. центр БГУ, 2012. – 192 с.