государства. В этом процессе ключевую роль должно играть административное право как инструмент, обеспечивающий правовую определенность, эффективный контроль и баланс интересов всех участников цифровых отношений.

Список использованных источников

1. Алексеев, С.С. Теория права / С.С. Алексеев. – М. : БЕК, 1995. – 320 с.

1. Куракин, А.Б. Административно–правовое регулирование в условиях цифровизации / А.Б. Куракин // Юридическая наука и практика. – 2023. – № 4. – С. 24–29.

2. Kütt, A. Digital Administration in Estonia: Legal and Organizational Framework / A. Kütt // Journal of E–Governance. – 2022. – Vol. 45. – P. 55–63.

3. Tan, W.L. Administrative Innovation in Singapore's Digital Government / W.L. Tan // Asia–Pacific Law Review. – 2023. – Vol. 31(1). – P. 10–25.

4. Марков, А.В. Цифровая трансформация административного регулирования: вызовы и перспективы // Административное и муниципальное право. – 2024. – № 2. – С. 34–40.

УДК 34

ПРОТИВОДЕЙСТВИЕ ЭКСТРЕМИЗМУ И ТЕРРОРИЗМУ В ИНТЕРНЕТЕ: ПОИСК ЭФФЕКТИВНЫХ ПРАВОВЫХ РЕШЕНИЙ В УСЛОВИЯХ АНОНИМНОСТИ

Л.А. Фомина
Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации,
специалист

В современном мире интернет стал не только мощным инструментом для коммуникации и образования, но и, к сожалению, благоприятной средой для распространения экстремистской и террористической идеологии. С каждым годом число преступлений, совершенных с использованием информационно–телекоммуникационных технологий, ставит новые рекорды. Так, согласно статистике МВД России, за 2025 г. зарегистрировано на 1,3% больше преступлений с использованием ИКТ по сравнению с январем–февралем 2024 г.

Данная проблема имеет несколько аспектов. Первым аспектом, который необходимо учитывать, является использование террористами сети Интернет для распространения экстремистской идеологии. Это важный аспект, поскольку молодежь России проводит достаточно много времени в интернете. Поэтому важно разрабатывать и внедрять меры по

борьбе с экстремизмом в онлайн–пространстве. С другой стороны, радикальные группировки используют информационно–коммуникационные технологии для вербовки новых членов, координирования атаки, финансирования деятельности, оставаясь при этом в тени благодаря анонимности, но это все касается планирования террористического акта в реальной жизни. Нельзя не отметить существование феномена информационного терроризма и, как верно отмечает Акулова Е.В., на данный момент не существует универсального общепринятого понятия. [1, с.51] Таким образом, третьим аспектом является совершение террористами диверсии непосредственно в интернете, а именно DDoS–атаки на информационные порталы. Согласно исследованиям в первом квартале 2025 г. зафиксирован рост числа информационных атак на 71% по сравнению с первым кварталом предыдущего года.

Представляется необходимым разграничить понятия «терроризм», «террористическая деятельность». Так, согласно ст. 3 ФЗ «О противодействии терроризму», под понятием терроризм законодатель понимает идеологию насилия и практику воздействия на принятие решения органами государственной власти связанные с устрашением населения и (или) иными формами противоправных насильственных действий. А что касаемо террористической деятельности, то здесь уже отмечается информационное пособничество в планировании, подготовке или реализации террористического акта, пропаганда идей терроризма, распространение материалов или информации, призывающих к осуществлению террористической деятельности либо обосновывающих или оправдывающих необходимость осуществления такой деятельности. Российское законодательство предусматривает ряд мер по противодействию экстремизму и терроризму в интернете, включая: Федеральный закон «О противодействии экстремистской деятельности» (№ 114–ФЗ); Федеральный закон «О противодействии терроризму» (№ 35–ФЗ); Федеральный закон «Об информации, информационных технологиях и о защите информации» (№ 149–ФЗ); Уголовный кодекс Российской Федерации (статьи, предусматривающие ответственность за террористическую и экстремистскую деятельность). Данные законы позволяют блокировать сайты с экстремистским контентом, привлекать к ответственности лиц, распространяющих такую информацию, и осуществлять оперативно–розыскные мероприятия для выявления и пресечения преступлений. Также утвержден Комплексный план противодействия идеологии терроризма в Российской Федерации на 2024–2028 г. Главной целью является формирование у населения неприятия идеологии терроризма и устойчивости к её пропаганде на основе традиционных российских духовно–нравственных ценностей, которые могут транслироваться через информационные ресурсы. Так к работа ведется в информационном пространстве с привлечением популярных

блогеров, СМИ, творческих объединений и др. для распространения материалов, нацеленных на формирование у населения антитеррористического мировоззрения.

Возвращаясь к проблеме информационного терроризма, необходимо согласится с мнением Пирумова В.С. в том, что под информационным терроризмом необходимо понимать действия, направленные на дезорганизацию работы информационных систем и сетей связи, что влечет за собой создание каких–либо общественно опасных последствий, в тех случаях, когда такие действия совершаются для оказания воздействия на принятие политических решений органами власти.[2, с.252] В настоящее время существуют примеры, подкрепляющие данное определение. Например, не так давно был осуществлен взлом всех информационных ресурсов Российской академии народного хозяйства и государственной службы, и, что немало важно, в день инаугурации президента, то есть данный акт имел политическую цель. А что, если это коснется таких критически важных интернет–порталов как «Госуслуги», содержащие в себе важные персональные данные? Такие действия могут повлечь за собой подрывание доверия населения к государству и дискредитации его работы в целом.

Представляет научный интерес ст. 369–1 Уголовного кодекса Республики Беларусь, в котором квалифицируется распространение заведомо ложной информации о Республике Беларусь, её органах власти, Вооружённых Силах, экономике, политике или обществе с целью дискредитации страны, может быть осуществлено через публичные выступления, СМИ, интернет или печатные материалы, нанося значительный ущерб государственным или общественным интересам, в то время как в Российской Федерации существует только статья о дискредитации Вооруженных Сил. Поэтому представляется необходимым создание подобного закона о дискредитации, так как с помощью данного инструмента будет эффективнее противодействие распространению заведомо ложной информации и фейков о Российской Федерации.

В период с января по март 2025 г. система, разработанная компанией CyberFirst, зафиксировала и зарегистрировала более 2600 DDoS–атак. В случае, если подобные атаки осуществляются с террористическими намерениями, возникает необходимость определения соответствующей статьи Уголовного кодекса. Однако в текущей редакции Уголовного кодекса Российской Федерации отсутствует статья, предусматривающая ответственность за совершение DDoS–атак с террористической целью. В контексте терроризма, согласно действующему законодательству, террористические акты включают в себя такие действия, как взрывы и поджоги. В связи с этим, предлагается рассмотреть возможность внесения изменений в Уголовный кодекс Российской Федерации, которые бы позволили квалифицировать DDoS–атаки как террористические преступления или как компьютерные преступления с террористической

целью. Это позволит более эффективно противодействовать угрозам, связанным с использованием информационных технологий в террористических целях.

Помимо всего в научном сообществе ведутся дискуссии касаемо баланса между правом на анонимность в интернете и необходимостью предотвращения террористических актов и воспрепятствования распространения экстремистской идеологии радикальными группировками. Некоторые деятели выступают за деанонимизацию, однако при этом важно соблюсти обеспечение защиты персональных данных пользователей. В связи с этим, дискуссии о балансе между анонимностью и безопасностью, инициированные Заместителем председателя Государственной Думы Российской Федерации И.А. Яровой, приобретают особую значимость. Ирина Анатольевна критикует «анонимные правоотношения», выступает за открытые, честные отношения. Красной нитью в ее выступлении проходит запрет на анонимность в сети Интернет. «Любой правоохранитель скажет: анонимность — это путь к введению в заблуждение», — отметила Яровая И.А. во время сессии «Роль искусственного интеллекта в противодействии пропаганде радикальной, экстремистской и террористической деятельности». Она также подчеркнула важность создания инструмента, способного автоматически обнаруживать в сети материалы экстремистского и агрессивного характера, что поможет правоохранительным органам в борьбе с информационными преступниками.

Таким образом, противодействие экстремизму и терроризму в интернете является одним из важнейших векторов развития в сфере обеспечения национальной безопасности Российской Федерации. Решение этой задачи требует комплексного подхода, включающего совершенствование правовой базы, развитие технологий выявления и блокировки экстремистского контента, усиление международного сотрудничества и поиск баланса между анонимностью и безопасностью в сети. Данный подход позволит создать устойчивую систему противодействия экстремистским и террористическим угрозам в интернет–пространстве, что будет способствовать повышению уровня национальной безопасности.

Список использованных источников

1. Акулова, Е.В. Правовое обеспечение противодействия использованию информационно–коммуникационных технологий в террористических целях как угрозе информационной безопасности : диссертация … кандидата юридических наук / Е.В. Акулова. – Москва, 2024. – 195 с.

2. Пирумов, В.С. Информационное противоборство. Четвертое измерение противостояния / В.С. Пирумов. – М.: «Оружие и технологии». 2010.