Обеспечение общественной безопасности в эпоху цифровизации: некоторые проблемные аспекты

Шеншин Виктор Михайлович
кандидат юридических наук, доцент, старший научный сотрудник Центра исследования проблем безопасности Российской академии наук

Кибертерроризм и киберэкстремизм – новое явление, угрожающее национальной безопасности России и такому ее виду как общественная безопасность. Количество преступлений, связанных с экстремизмом и терроризмом в интернете, ежегодно увеличивается. Основные формы данных видов преступности в интернет-пространстве: пропаганда экстремистских идей в социальных сетях; создание сайтов для финансирования преступной деятельности; управление преступной деятельностью через интернет; кибератаки на информационные системы. Сегодня борьба с кибертерроризмом и киберэкстремизмом затруднена рядом проблем. Среди таковых автор называет – недостаточное законодательное регулирование данных видов преступности; трудности блокировки экстремистских ресурсов, ввиду наличия специальных анонимных программ (например VPN); длительность признания контента экстремистским; проблемы взаимодействия с иностранными интернет-ресурсами; недостаточная защита информационных данных. Для решения указанных проблем предложен ряд мер: разработка нового состава преступления «кибертерроризм» в УК РФ; совершенствование ФЗ «Об информации, информационных технологиях и о защите информации, а также ФЗ «Об оперативно-розыскной деятельности; изменение порядка признания материалов – экстремистскими; автоматизация мониторинга экстремистских материалов; усиление защиты конфиденциальных данных через совершенствование законодательств, системы контроля и использование API-систем мониторинга утечек; заключение международных договоров о сотрудничестве в борьбе с киберпреступностью.

Ключевые слова: цифровизация; национальная безопасность; общественная безопасность; кибертерроризм; киберэкстремизм.

В настоящее время терроризм и экстремизм по своим масштабам и колоссальной разрушающей силе превзошли всевозможные угрозы общественным отношениям, таким образом, бросив вызов всему человечеству. Усиление процесса цифровизации в мировом сообществе и развитие новых систем общественных отношений в целом становятся потенциально опасными для всех людей, поскольку теперь они связаны с такими опасными явлениями, как терроризм и экстремизм.

Изменение баланса сил на политической арене, появление новых участников международной политики, развитие информационных технологий, разработка ядерного оружия и пр., обостряют проблему терроризма и экстремизма, заставляя уделять вопросам терроризма и экстремизма должное внимание.

Некоторые ученые склонны считать, что авторство термина «терроризм» принадлежит французскому мыслителю Ш. Монтескье, который перевел слово «террор» с латинского на французский язык для характеристики деспотического государства, которое представляет собой нагнетание атмосферы страха и террора правителем на подданных. Другие авторы придерживаются мнения, что «понятие террор» ввел Аристотель для обозначения особого типа ужаса, который овладевал зрителями трагедии в греческом театре.

В отечественном законодательстве понятие «терроризм» определяется как идеология насилия и практика воздействия на общественное сознание, на принятие решений органами государственной власти, органами местного самоуправления или международными организациями, связанные с устрашением населения и (или) иными формами противоправных насильственных действий (ст. 3 Федерального закона от 06.03.2006 № 35-ФЗ «О противодействии терроризму»).

Несмотря на существование этой дефиниции, некоторые ученые дают собственное определение терроризма, определяя его, например, как «многоструктурное социальное, идейно-политическое явление, направленное на разрушение существующей государственно-политической системы страны и использующее наиболее общественно опасные противоправные методы и средства для достижения своих политических целей».

В самом широком смысле терроризм можно определить как противоправную деятельность, направленную на публичное устрашение общества путем причинения либо угрозы причинения ему существенного урона с целью оказания воздействия на власть для принятия ею значимых решений в угоду террористам.

Посмотрим на некоторые формы киберэкстремистской и кибертеррористической деятельности, которые условно можно классифицировать по уровню организации на:

простой (неструктурированный) – преступное посягательство совершается одним лицом, посредством использования различных программ или систем (как правило, данная форма реализации киберэкстрпреступной деятельности происходит посредством использования уже известных программ), экономические, репутационные и иные последствия такой деятельности меньше, чем для остальных форм.

расширенный (структурированный) – характеризуется наличием организации, обладающей определенной структурой, включающей базовое обучение участников, и

Статья подготовлена в рамках реализации государственного задания «Комплексное исследование проблем общественной безопасности, как стратегического приоритета национальной безопасности Российской Федерации (FFFZ-2025-0001)»)

направленной на проведение хакерских атак более высокого уровня, а также созданием собственных инструментов взлома. Потери от реализации преступной деятельности существенно выше неорганизованных посягательств.

комплексный (координированный) – форма организации преступной деятельности, влекущая за собой наибольшую общественную опасность, в том числе угрозу государственной и общественной безопасности, как стратегическому национальному приоритету. Помимо наличия четко регламентированной и координируемой структурной организации деятельности участников включает выработку планов организованных хакерской атак на государственные учреждения, а также возможностью разработки собственного инструментария взлома систем государственных информационных систем. [Ильиных Н.А. С.68]

Киберэкстремизм и кибертерроризм, независимо от того, в каких формах они проявляются, стали одной из наиболее значимых проблем, с которыми Россия вошла в XXI век. Распространение радикальных и экстремистских взглядов и верований, провоцирование общественных беспорядков и этноконфессиональных конфликтов, террористические акты и призывы к их совершению, совершаемые посредством информационных технологий, а также выявленные правоохранительными органами приготовления к их совершению – все эти деяния представляют собой реально существующие и весьма актуальные угрозы и опасности для национальной безопасности России. Поэтому противодействие проявлениям цифрового экстремизма и терроризма в России является одной из наиболее значимых государственных задач по обеспечению национальной безопасности.

Между тем, несмотря на усилия государства, а также международных организаций, решение этой задачи затруднено множеством проблем, которые требуют скорейшего разрешения.

Вышеуказанные меры не всегда могут оказаться эффективными, поскольку на данный момент преступники имеют возможность регистрироваться на разных ресурсах, используя чужие персональные данные и применяя другие преступные способы. В связи с этим, более целесообразным, с нашей точки зрения является подписание международного договора по вопросам содействия в раскрытии киберпреступлений экстремистского и террористического характера. В частности, в рамках данного договора предполагается внесение пункта об оперативном предоставлении IP-адресов и иных значимых для раскрытия преступления сведений от владельцев иностранных Интернет-ресурсов, страны которых подписали данный договор.

Следует констатировать, что подписание подобного договора, возможно только с дружественными странами. Возможность подписания подобного договора с европейскими странами ставится под сомнение в силу сложившихся международно-правовых отношений. Так, например, недавно Вашингтон опубликовал многостраничную Стратегию международного киберпространства и цифровой политики США, где Россия и Китай названы главной угрозой для Соединенных Штатов. Оказывается, Россия угрожает «подрывом глобального авторитета США».

Даже при наличии уголовно-правовой охраны от кибертерроризма и киберэкстремизма, справиться с этими преступлениями невозможно без эффективной системы защиты личных данных граждан в цифровом пространстве. Это объясняется тем, что множество киберпреступлений террористической и экстремисткой направленности сопровождается кражей личных данных, (преступник может выдать себя за другое лицо и избежать последствий); получением доступа к финансовым средствам человека с целью финансирования террористической, экстремисткой деятельности; получением доступа к информации о человеке, с целью дальнейшей вербовки в преступные организации и пр.

Помимо применения вышеуказанных профилактических мер необходимо создать на территории России «штаб волонтеров», которые могли бы заниматься мониторингом социальных сетей и в целом сети интернет, и сообщать о «подозрительных» публикациях в правоохранительные органы и Национальный центр информационного противодействия терроризму и экстремизму в образовательной среде и сети Интернет, а также проводить иные профилактические мероприятия. Суть данного «штаба волонтеров» состоит в том, что мониторинг сети Интернет могли бы проводить все неравнодушные, а также граждане с высокой гражданской ответственностью, прошедшие обучение у специалистов в сфере борьбы с экстремизмом и терроризмом, психологов, IT-специалистов, создателей социальных сетей (например, Вконтакте) и т.д., и при выявлении экстремистской или террористической информации, передавать информацию правоохранительным органам. Данный способ способствовал бы увеличению скорости поиска «подозрительной» информации и блокирования доступа к ней. [Мельник С.С. С. 188]

Чат-боты и приложения, работающие на базе ИИ, способны взаимодействовать с лицами, оказавшимися на месте преступления или ставшими жертвами преступной деятельности, а также помогать правоохранительным органам в обнаружении потерпевших.

Так, например, во Франции было создано приложение «SAIP», которое содержит только систему оповещения и информирования населения, а также инструкции к действиям в тех или иных случаях, связанных с терроризмом. Но разработчиками не исключается возможность введения системы, позволяющей гражданам самим информировать власти о каких-либо подозрительных действиях. При этом такая идея взаимного сотрудничества гражданского общества и государства в сфере антитеррористических действий не нова. Изначально она была использована в приложении, разработанном специально для штата Нью-Йорк (США). Само приложение называется «See Something, Send Something» от компании My Mobile Witness. Оно позволяет пользователю присылать фотографию или заметку напрямую в отдел полиции штата, где будет проверяться каждая из них. [Терновсков В.Б., Вертий Е.А., Борода С.А. С.10]

Таким образом, цифровизация не только предоставляет участникам террористических группировок возможности для коммуникации, вербовки и обучения новых членов, не говоря уже о кибертерроризме, она также служит эффективным инструментом для противодействия экстремизму и терроризму в условиях современности.

Анализ судебной практики показал, что в 2020-2024 гг. судами рассматривались уголовные дела, как о преступлениях террористического характера, так и экстремисткой направленности, а также ряд административных дел, связанных с экстремизмом. Чаще, всего с использованием информационных технологий совершаются противоправные деяния экстремисткой направленности. [4] Поэтому противодействие проявлениям цифрового экстремизма и терроризма в России является одной из наиболее значимых государственных задач по обеспечению общественной безопасности, в частности, и национальной безопасности в общем. Между тем, решение этой задачи затруднено множеством проблем, которые требуют скорейшего разрешения. Среди них:

Проблема признания «контента», содержащего экстремистскую или террористическую информацию и призывающего к противоправной деятельности. Проблема заключается в том, что экспертизы и выяснение истинного

характера информации могут занимать довольно долгий период времени, в течение которого с данным материалом сможет познакомиться большое количество пользователей. А пока размещенный материал не будет признан экстремистским, правоохранительные органы не могут осуществлять свою деятельность по привлечению виновных к ответственности и блокированию опасного ресурса. [5] На основании этого, предлагается внести в ст. 13 ФЗ «О противодействии экстремистской деятельности», законодательную возможность ограничения подозрительных (по мнению правоохранительных органов) материалов до момента признания их судом – экстремистскими. В частности, можно ввести следующую поправку: «При наличии достаточных оснований полагать, что материалы являются экстремистскими, правоохранительные органы вправе ограничить доступ к информационному ресурсу, на котором они расположены». Более эффективно могла бы бороться с распространением таких материалов программа, автоматически направляющая подозрительные экстремистские материалы на почту правоохранительных ведомств с целью оперативно определить, стоит ли ограничить доступ к подобным материалам без судебного решения.

Проблема получения сведений о зарубежных интернет-ресурсах. На практике, чтобы установить преступника необходимо получить данные от владельца Интернет-ресурса и IP-адресе пользователя сети, от имени которого размещен текст экстремистского (террористического) содержания или совершены иные действия противоправного (экстремистского, террористического характера). При этом сведения об IP-адресах возможно истребовать только от организаций российского сегмента сети Интернет. Получить данные об IP-адресах и другие имеющие значение для расследования сведения от владельцев иностранных ресурсов («Youtube», «WhatsApp», «Telegram») не представляется возможным. В таких случаях злоумышленнику часто удается избежать уголовной ответственности. Для частичного решения этой проблемы в 2023 г. принят Федеральный закон № 406-ФЗ в котором предусматривается, что регистрация на информационных ресурсах возможна только при соблюдении отдельных правил авторизации. [Клименко А.И. С. 43-54]

Вышеуказанные меры не всегда могут оказаться эффективными, поскольку на данный момент преступники имеют возможность регистрироваться на разных ресурсах, используя чужие персональные данные и применяя другие способы.

Недостаточное обеспечение защиты конфиденциальной информации. Даже при наличии уголовно-правовой охраны от кибертерроризма и киберэкстремизма, справиться с этими преступлениями невозможно без эффективной системы защиты личных данных граждан в цифровом пространстве.[Ирошников Д.В. С. 11-22] Это объясняется тем, что множество киберпреступлений террористической и экстремисткой направленности сопровождается кражей личных данных, в свой черед, сопровождающейся кражей личности (преступник, например, может выдать себя за другое лицо и избежать последствий).

Рост возможностей цифровизации, который мы наблюдаем на сегодняшний день приводит к увеличению случаев кибертерроризма и киберэкстремиза. Между тем, нельзя отрицать, что цифровизация помогает в борьбе с терроризмом и экстремизмом по ряду следующих направлений анализ данных; распознавание моделей преступления; наблюдение и мониторинг; защита от кибератак; биометрическая идентификация, анализ голоса и поведения; дроны и робототехника для охраны правопорядка; чат-боты и виртуальные приложения для общения с гражданами и пр. Таким образом, цифровизация не только предоставляет участникам террористических группировок возможности для коммуникации, вербовки и обучения новых членов, не говоря уже о кибертерроризме, она также служит эффективным инструментом для противодействия экстремизму и терроризму в условиях современности.

Литература

1. Ильиных Н.А. Киберэкстремизм: понятие и разграничение с иным информационным деструктивным воздействием на человека в киберпространстве // Известия Юго-Западного государственного университета. Серия: История и право. – 2023. – №1. – С. 68
2. Мельник С.С. Правовое регулирование киберэкстремизма и кибертерроризма: проблемы и перспективы // Юридическая наука и практика: Вестник Нижегородской академии МВД России. – 2024. – № 1. – С. 188.
3. Терновсков В.Б., Вертий Е.А., Борода С.А. Использование цифровых технологий (в том числе мобильных приложений) для борьбы с терроризмом // Молодой ученый. – 2020. – № 45 (335). – С. 10.
4. Гирько, С. И. Общественная безопасность Российской Федерации: состояние и дальнейшие шаги развития / С. И. Гирько // Административное право и процесс. – 2023. – № 8. – С. 3-8. – DOI 10.18572/2071-1166-2023-8-3-8.
5. Харламов, С. О. Конституционно-правовое регулирование использования QR-кодов в противодействии экстремизму и терроризму / С. О. Харламов, С. А. Егоров // Вестник экономической безопасности. – 2022. – № 4. – С. 239-243. – DOI 10.24412/2414-3995-2022-4-239-243.
6. Клименко, А. И. Взаимосвязь первого и второго поколений прав человека / А. И. Клименко // Укрепление традиционных российских духовно-нравственных ценностей и обеспечение прав человека в условиях современных вызовов : Сборник научных статей. – Смоленск : Смоленский государственный университет, 2023. – С. 43-54.
7. Ирошников, Д. В. Безопасность как категория международного публичного права: теоретический аспект / Д. В. Ирошников // Право. Безопасность. Чрезвычайные ситуации. – 2022. – № 1(54). – С. 11-22.

Ensuring Public Safety in the Digital Age: Some Problematic Aspects

Shenshin V.M.

Center for Security Studies of the Russian Academy of Sciences

Cyberterrorism and cyber extremism are a new phenomenon that threatens Russia's national security and its kind like public safety. The number of crimes related to extremism and terrorism on the Internet is increasing every year. The main forms of these types of crime in the Internet space are: propaganda of extremist ideas on social networks; creation of websites for financing criminal activities; management of criminal activities via the Internet; cyber attacks on information systems. Today, the fight against cyberterrorism and cyber extremism is hampered by a number of problems. Among these, the author names insufficient legislative regulation of these types of crime; difficulties in blocking extremist resources due to the presence of special anonymous programs (for example, VPN); the duration of recognition of extremist content; problems of interaction with foreign Internet resources; insufficient protection of information data. A number of measures have been proposed to solve these problems: the development of a new corpus delicti of "cyberterrorism" in the Criminal Code of the Russian Federation.; improving the Federal Law "On Information, Information Technologies and Information Protection, as well as the Federal Law "On Operational Investigative Activities; changing the procedure for recognizing extremist materials; automating the monitoring of extremist materials; strengthening the protection of confidential data through improving legislation, control systems and the use of API leak monitoring systems; concluding international agreements on cooperation in combating with cybercrime.

Keywords: digitalization; national security; public safety; cyberterrorism; cyber extremism.

References

1. Ilinykh N.A. Cyber-extremism: the concept and differentiation from other informational destructive effects on humans in cyberspace // Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta. Series: History and Law. – 2023. – No. 1. – p. 68
2. Melnik S.S. Legal regulation of cyber extremism and cyberterrorism: problems and prospects // Legal science and practice: Bulletin of the Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia. – 2024. – No. 1. – p. 188.

3. Ternovskov V.B., Vertiy E.A., Boroda S.A. The use of digital technologies (including mobile applications) to combat terrorism // Young Scientist. – 2020. – № 45 (335). – P. 10.
4. Girko, S. I. Public security of the Russian Federation: state and further steps of development / S. I. Girko // Administrative law and process. - 2023. - No. 8. - P. 3-8. - DOI 10.18572/2071-1166-2023-8-3-8.
5. Kharlamov, S. O. Constitutional and legal regulation of the use of QR codes in countering extremism and terrorism / S. O. Kharlamov, S. A. Egorov // Bulletin of Economic Security. - 2022. - No. 4. - P. 239-243. - DOI 10.24412/2414-3995-2022-4-239-243.
6. Klimenko, A. I. The relationship between the first and second generations of human rights / A. I. Klimenko // Strengthening traditional Russian spiritual and moral values and ensuring human rights in the context of modern challenges: Collection of scientific articles. - Smolensk: Smolensk State University, 2023. - P. 43-54.
7. Iroshnikov, D. V. Security as a category of public international law: theoretical aspect / D. V. Iroshnikov // Law. Security. Emergencies. - 2022. - No. 1 (54). - P. 11-22.