

ББК 67.408.131.11

*В.К. Гавло, В.А. Мазуров*

## **Уголовно-правовые и криминологическо-криминалистические аспекты противодействия терроризму**

*V.K. Gavlo, V.A. Mazurov*

## **Criminal, Criminological and Forensic Aspects of Counteracting Terrorism**

Анализируются тенденции, качественные изменения преступности террористической направленности. На основе исследования нормативных правовых, научных, официальных источников сформулированы выводы и предложения по совершенствованию уголовного законодательства и правоприменительной практики противодействия терроризму в современной России.

**Ключевые слова:** терроризм, кибертерроризм, кибертерракт.

В Концепции противодействия терроризму в Российской Федерации, утвержденной Президентом РФ от 5 октября 2009 г. (далее – Концепция), терроризм рассматривается как угроза национальной безопасности России. В этом документе указаны основные тенденции современного терроризма: увеличение количества террористических актов и пострадавших от них лиц; повышение уровня организованности террористической деятельности; усиление взаимосвязи терроризма и организованной преступности, в том числе транснациональной; стремление субъектов террористической деятельности завладеть оружием массового поражения; разработка новых и совершенствование существующих форм и методов террористической деятельности, направленных на увеличение масштабов последствий террористических актов и количества пострадавших [1, с. 14].

Актуальность рассматриваемого вопроса заключается в том, что в последние годы произошли качественно-количественные изменения показателей преступности террористической направленности не только в России, но и в ряде ведущих государств Европы, Азии, Америки. В этой связи в России проведен ряд конкретных организационно-правовых мероприятий, направленных на противодействие терроризму. К ним можно отнести расширение сотрудничества по борьбе с преступлениями террористической направленности между Российской Федерацией и ведущими государствами мира. На качественно новом уровне проводятся антитеррористические мероприятия. С учетом полученных результатов этой деятельности формируется законотворческая и правоприменительная практика противодействия терроризму. Одним из

The paper analyzes trends and quality changes of the terrorism. Based on the study of legal, scientific and official sources the authors formulate some conclusions and proposals to improve the criminal law and practice in order to counteract terrorism in modern Russia.

**Key words:** terrorism, cyber-terrorism, cyber-terrorist act.

направлений совершенствования правовых мер борьбы с преступлениями террористической направленности является деятельность по совершенствованию российского уголовного законодательства.

Уголовная ответственность за преступления террористической направленности предусмотрена в Уголовном кодексе РФ в ст. 205 «Террористический акт», ст. 205-1 «Содействие террористической деятельности», ст. 205-2 «Публичные призывы к осуществлению террористической деятельности или публичное оправдание терроризма», ст. 207 «Заведомо ложное сообщение об акте терроризма», ст. 277 «Посягательство на жизнь государственного или общественного деятеля», ст. 360 «Нападение на лиц или учреждения, которые пользуются международной защитой».

Для характеристики указанных составов преступлений и разработки предложений по совершенствованию уголовного законодательства необходимо рассмотреть основные понятия, которые нашли свое отражение в международных, российских нормативных правовых актах, официальных документах, научных источниках.

Терроризм – насилие или угроза его применения в отношении физических лиц или организаций, а также уничтожение (повреждение) или угроза уничтожения (повреждения) имущества и других материальных объектов, создающие опасность гибели людей, причинение значительного имущественного ущерба либо наступление иных общественно опасных последствий, осуществляемые в целях нарушения общественной безопасности, устрашения населения или оказания воздействия на принятие органами власти решений, выгодных террористам, или удо-

влетворения их неправомерных имущественных или иных интересов; посягательство на жизнь государственного или общественного деятеля, совершенное в целях прекращения его государственной или иной политической деятельности либо из мести за такую деятельность; нападение на представителя иностранного государства или сотрудника международной организации, пользующихся международной защитой, а равно на служебные помещения либо транспортные средства лиц, пользующихся международной защитой, если это деяние совершено в целях провокации войны или осложнения международных отношений.

Террористическая деятельность – деятельность, включающая в себя:

- организацию, планирование, подготовку и реализацию террористических акций;
- информационное или иное пособничество в организации и проведении террористического акта;
- организацию незаконного вооруженного формирования, преступного сообщества, преступной организации, организованной преступной группы для совершения террористических актов, а равно участие в такой акции;
- подстрекательство к террористической акции, вербовку, вооружение, подготовку и обучение террористов;
- финансирование заведомо террористической организации, группы или иное содействие им;
- пропаганду и публичные призывы к осуществлению террористической деятельности.

Террористическая акция – непосредственное совершение преступления террористического характера в форме взрыва, поджога, применения или угрозы применения взрывных устройств, радиоактивных, химических, биологических, токсических, отравляющих, сильнодействующих ядовитых веществ; уничтожение, повреждение или захват транспортных средств, важных стратегических объектов; посягательство на жизнь государственного или общественного деятеля, представителя национальных, этнических, религиозных или иных групп населения; захват заложников, похищение человека; создание опасности причинения вреда жизни, здоровью или имуществу неопределенного круга лиц путем создания условий для аварий и катастроф техногенного характера.

Во исполнение Федерального закона РФ «О противодействии терроризму», иных нормативных правовых актов и официальных документов Российской Федерации, с учетом положительного опыта борьбы с терроризмом, криминогенной обстановки в современной России, в УК РФ федеральными законами Российской Федерации от 27.12.06 №153-ФЗ от 30.12.08 №321-ФЗ от 27.12.09 №377-ФЗ внесены существенные изменения и дополнения [2, с. 12].

Так, ст. 205 и 205-1 УК РФ получили новые названия – «Террористический акт» и «Содействие

террористической деятельности», что, по нашему мнению, вполне соответствует содержанию диспозиций указанных норм уголовного закона. В ч. 1 ст. 205 УК РФ внесено дополнение, в соответствии с которым уголовная ответственность наступает за совершение террористического акта в целях воздействия на принятие решений международными организациями. В ст. 205-1 УК РФ расширен перечень составов преступлений, за склонение к которым предусмотрена уголовная ответственность по данной статье (ст. 278 УК РФ «Насильственный захват власти или насильственное удержание власти» и ст. 279 УК РФ «Вооруженный мятеж»).

Важным, на наш взгляд, для квалификации преступлений террористической направленности и минимизации судебных ошибок являются дополнения в примечания к ст. 205 и 205-1 УК РФ, в которых указаны обстоятельства, освобождающие от уголовной ответственности, а в примечании к ст. 205-1 УК РФ раскрывается содержание такого уголовно наказуемого деяния, как «финансирование терроризма». Под финансированием терроризма понимается предоставление или сбор средств либо оказание финансовых услуг с осознанием того, что они предназначены для финансирования организации, подготовки или совершения хотя бы одного из преступлений, предусмотренных ст. 205, 205-1, 205-2, 206, 208, 211, 277–279, 360 УК РФ, либо для обеспечения организованной группы, незаконного вооруженного формирования, преступного сообщества, созданных или создаваемых для совершения хотя бы одного из указанных преступлений. В примечании к ст. 205-2 УК РФ «Публичные призывы к осуществлению террористической деятельности или публичное оправдание терроризма» отмечается, что под публичным оправданием терроризма понимается публичное заявление о признании идеологии и практики терроризма правильными, нуждающимися в поддержке и подражании.

В ч. 2 ст. 205-2 УК РФ в качестве квалифицирующего признака данного состава преступления предусмотрена ответственность за публичные призывы к осуществлению террористической деятельности или публичное оправдание терроризма, совершенные с использованием средств массовой информации. Известно, что достаточно большой объем информации такого рода размещен в сети Интернет, который не является СМИ. В качестве СМИ в Интернете можно рассматривать сайты газет, журналов, информационных телевизионных программ. Представляется, что с указанной информацией имеет возможность ознакомиться огромное количество россиян. Наибольшую общественную опасность данное обстоятельство представляет потому, что Интернетом наиболее активно пользуются молодые люди, которые в большей степени подвержены негативному влиянию такого рода информации. Проблематичным в сни-

жении негативного влияния указанной информации, размещенной в Интернете, является и то, что зачастую весьма непросто установить ее авторов. Учитывая это и ряд других обстоятельств, международные и российские террористические и экстремистские организации активно используют Интернет, ЭВМ, систему, сеть ЭВМ и новейшие достижения научно-технического прогресса в сфере высоких технологий в пропагандистских целях своей деятельности, оправдании терроризма и экстремизма.

В этой связи считаем целесообразным внести дополнение в п. «к» ст. 63 УК РФ «Обстоятельства, отягчающие наказание»: «к) совершение преступлений с использованием оружия... специально изготовленных технических средств, ЭВМ, системы, сети ЭВМ...».

Указанное дополнение, на наш взгляд, будет иметь принципиальное значение при квалификации преступлений террористической и экстремистской направленности. В последнее время зарегистрировано и реализовано в судах большое количество уголовных дел по ст. 207 УК РФ «Заведомо ложное сообщение об акте терроризма», совершенных с использованием ЭВМ, системы и сети ЭВМ. Особенность таких деяний, в отличие от ложных сообщений об акте терроризма, совершенных иным более «традиционным» способом (например по телефону), заключается в том, что лицо имеет возможность отправить такое сообщение не только в регионе, в России, но и за ее пределы. Данное обстоятельство может иметь негативные последствия для граждан другой страны, повлиять на межгосударственные отношения и т.п. Использование ЭВМ, системы и сети ЭВМ при совершении данного преступления, иных преступлений террористической направленности и не только этих преступных деяний создает определенные проблемы в установлении виновного лица, требует привлечения значительных средств, технического обеспечения.

Глобализация экономики, компьютеризация таких важных сфер деятельности общества, как связь, энергетика, транспорт, система хранения и транспортировки нефти и газа, финансовая и банковская системы, оборона и национальная безопасность, переход на методы электронного управления технологическими процессами в производстве, по мнению российских и зарубежных экспертов, становятся причиной все большего распространения террористических акций с помощью высоких технологий. По мнению специалистов-практиков и ученых-правоведов, терроризм с использованием последних достижений в сфере высоких технологий не менее опасен, чем ядерный или бактериологический терроризм. В настоящее время существует весьма мало информационных систем, которые можно назвать надежно защищенными.

В научной юридической литературе проблемы компьютерного терроризма (кибертерроризма), на наш взгляд, рассматриваются не на должном уровне.

Ряд авторов (В.А. Голубев, Ю.В. Гаврилов, Л.В. Смирнов) определяют кибертерроризм как совокупность противоправных действий, связанных с покушением на жизнь людей, угрозами расправ, деструктивными действиями в отношении материальных объектов, искажением объективной информации или рядом других действий, способствующих нагнетанию страха и напряженности в обществе с целью получения преимущества при решении политических, экономических или социальных задач. Сущность кибертерроризма заключается в оказании противоправного воздействия на информационные системы, совершенного с целью создания опасности причинения вреда жизни, здоровью или имуществу неопределенного круга лиц путем создания условий для аварий и катастроф техногенного характера либо реальной угрозы такой опасности. Под термином «кибертерракт» понимаются, как правило, действия по дезорганизации информационных систем, устрашающих население и создающих опасность гибели людей, причинения значительного имущественного ущерба либо наступления иных тяжких последствий в целях воздействия на принятие решения органами власти или международными организациями, а также угроза совершения указанных действий в тех же целях [3, с. 24–25]. Повышенная общественная опасность кибертерракта заключается в том, что он не имеет границ, кибертеррорист способен в равной степени угрожать информационным системам, расположенным практически в любой точке земного шара. Обнаружить и нейтрализовать виртуального террориста весьма проблематично из-за слишком малого количества оставляемых им следов в виртуальном пространстве.

В киберпространстве могут быть использованы различные приемы для совершения террористического акта:

- нанесение ущерба отдельным элементам киберпространства, разрушение сетей электропитания, наведение помех, использование специальных программ, стимулирующих разрушение аппаратных средств;

- хищение или уничтожение информационного и технического ресурсов киберпространства, имеющих стратегическую значимость, путем преодоления систем защиты, внедрения вирусов, программных закладок;

- воздействие на программное обеспечение и информацию с целью их искажения или модификации в информационных системах и системах управления; раскрытие и угроза опубликования закрытой информации о функционировании информационной инфраструктуры государства, общественно значимых и военных информационных систем, кодов шифрования, а также о принципах работы системы шифрования;

- захват каналов телекоммуникационного вещания с целью распространения дезинформации, слухов,

демонстрации мощи террористической организации и объявления своих требований;

– уничтожение и активное подавление линий связи, неправильная адресация, искусственная перезагрузка узлов коммуникации, воздействие на операторов, разработчиков информационных систем с целью совершения ими перечисленных выше действий [4, с. 29–37].

Таким образом, высокотехнологичные террористические акции представляют сегодня реальную серьезную опасность, именно поэтому требуется своевременное принятие конкретных мер противодействия таким акциям, в том числе и путем совершенствования правовой базы противодействия терроризму, прежде всего уголовного законодательства.

Сегодня террористы имеют возможность не только осуществлять террористические акции в киберпространстве, пропагандировать свою террористическую деятельность, но и с помощью современных информационных технологий получать необходимую для проведения терактов информацию ограниченного доступа. В этой связи весьма важными и своевременными являются предложения Правительства РФ о внесении изменений в Федеральный закон «О государственной тайне», направленные на противодействие терроризму. Предлагается включить в перечень сведений, составляющих государственную тайну, информацию: о защищенности критически важных и потенциально опасных объектов инфраструктуры от террористических и диверсионных угроз; о формах, методах и условиях организации и планировании террористической деятельности; о результатах финансового мониторинга в отношении организаций и физических лиц, полученных в связи с проверкой их возможной причастности к террористической деятельности [5]. Эти предложения обусловлены тем, что в данном законе не обозначены положения о защите сведений в области противодействия терроризму. В связи с этим и предлагаются указанные поправки, которые направлены на единый подход в общегосударственной системе противодействия терроризму. Выделение этих сведений в самостоятельную категорию и охрана ее в режиме государственной тайны обусловлены и тем, что работа по противодействию терроризму существенно шире разведывательной, контрразведыва-

тельной и оперативно-разыскной<sup>1</sup> деятельности, которые отнесены к государственной тайне. Она включает в себя функции органов государственной власти, в том числе по выявлению и устранению причин и условий, способствующих совершению террористических актов, ликвидации их последствий и не имеющих права на проведение оперативных и иных мероприятий, предусмотренных Федеральным законом РФ «Об оперативно-разыскной деятельности».

Принятие федерального закона, предоставляющего право органам ФСБ выносить официальное предостережение физическим лицам, которые еще не совершили преступление, но стоят на пути его совершения, на наш взгляд, будет способствовать проведению ранней профилактики в отношении лиц, вынашивающих террористические или экстремистские намерения. Представляется, что данная мера профилактики особо важна при работе с несовершеннолетними правонарушителями [6].

На встречах с руководителями думских партий в апреле 2010 г. Президент РФ Д.А. Медведев предложил ужесточить уголовную ответственность пособников террористов [7]. До настоящего времени не внесены поправки в УК РФ. В этой связи считаем возможным внести дополнение в ч. 1 ст. 205-1 УК РФ в следующей редакции: «1. Склонение..., а равно финансирование и пособничество терроризму – наказываются...». Под пособничеством следует понимать деятельность лица, связанную с предоставлением информации, средств или орудий совершения преступления, оружия, боеприпасов, радиоактивных, отравляющих и иных средств для совершения терактов, обеспечение продовольствием, медицинской помощью, заранее обусловленное обещание скрыть следы преступления, а равно иную деятельность, способствующую проведению террористических акций. Соответственно, необходимо увеличить срок наказания в виде лишения свободы с восьми до десяти лет.

<sup>1</sup> Написание слова оперативно-разыскной дано в соответствии с современными правилами русского языка. См.: Правила русской орфографии и пунктуации. Полный академический справочник / под ред. В.В. Лопатина. М., 2006. С. 53 (§40). В названии документов орфография сохранена. – *Прим. ред.*

### Библиографический список

1. Концепция противодействия терроризму в Российской Федерации [утв. Президентом РФ от 5.10.2009] // Российская газета. – 2009. – 20 окт.
2. О противодействии терроризму : Федеральный закон от 06.03.2006 №35-ФЗ // Российская газета. – 2006. – 10 марта.
3. Гульбин Ю. Преступления в сфере компьютерной информации // Российская юстиция. – 1997. – №10.

4. Вехов В.Б. Компьютерные преступления: способы совершения, методики расследования. – М., 1998.
5. Ямшанов Б. Терроризм под грифом «секретно» // Российская газета. – 2010. – 21 сент.
6. Егоров И. Предостережение от ФСБ // Российская газета. – 2010. – 2 июня.
7. Кузьмин В. Без снисхождения // Российская газета. – 2010. – 5 апр.