11. *Щедрин Н.В.* Меры безопасности как средство предупреждения преступности: Автореф. дис. … д-ра юрид. наук. – Екатеринбург, 2001.

Д.В. Фатхи

ИНФОРМАЦИОННЫЙ ТЕРРОРИЗМ КАК НОВАЯ ФОРМА ТЕРРОРИЗМА

В настоящее время терроризм представляет одну из серьезнейших проблем безопасности человечества, являясь квинтэссенцией современной насильственной преступности. Среди угроз национальной безопасности в России терроризм сегодня занимает ведущее место.

Деятельность террористических организаций имеет трансграничный характер, она «обезличена» и представляет опасность не для конкретного человека или страны, а является глобальной проблемой всей цивилизации. Для террористических организаций террор является образом жизни и смыслом существования, а значит и борьба с ним должна иметь многоплановый характер. Необходимо отметить возрастающее с каждым днем многообразие способов осуществления террористической деятельности, направленной на возникновение межнациональных и межконфессиональных конфликтов, основной целью которой является дестабилизация обстановки в обществе, запугивание населения, провокации военных конфликтов, а в конечном счете передел власти или разрушение территориальной целостности государства.

В XXI в. весь мир вступил в эпоху глобализации, которая стала возможной не только благодаря ликвидации экономических национальных барьеров, сопровождающейся удешевлением технических достижений и связи, но и в связи с все более захватывающим процессом компьютеризации общества, когда средства телекоммуникаций приобретают исключительную роль. Наступила новая эпоха – эпоха «цифровой информации», результатом которой стало возникновение нового способа осуществления террористической деятельности – информационного терроризма. В настоящее время для террористов легко уязвимы практически все компьютерные средства создания, обработки, передачи и хранения информации. Банковские, биржевые, архивные, исследовательские, управленческие системы, Интернет, средства коммуникации от спутников до пейджеров, электронные средства массовой информации, издательские комплексы, всевозможные базы персональных данных – все это может подвергаться атаке при соответствующей квалификации террориста с одного единственного компьютера [1].

Информационный терроризм – это достаточно хорошо освоенные формы и приемы действий, применяемых для решения довольно широкого круга задач как локального, так и стратегического характера. Особую опасность в сложившихся условиях представляет собой использование значительного уровня информационного развития государства в целях, направленных не на всеобщее благо. Информационный терроризм представляет собой угрозу безопасности человечества, сравнимую с ядерным, бактериологическим и химическим оружием, причем степень этой угрозы в силу своей новизны не имеет достаточно точной характеристики.

Информационный терроризм представляет собой четкое и целенаправленное воздействие на компьютерную информацию, системы, программы и данные, а также компьютерные сети, направленное не на физическое уничтожение людей и ликвидацию материальных ценностей, а на дестабилизацию общественного порядка, широкомасштабное нарушение работы коммуникационных сетей и систем,

навязывание властным структурам своей воли. Информационный терроризм характеризуется анонимностью, высокой степенью латентности и относительной простотой осуществления террористических актов. Особую озабоченность у правоохранительных органов вызывает деятельность террористических организаций, связанная с использованием глобальной сети Интернет, из открытых источников которой можно получить сведения относительно технологии изготовления взрывчатых веществ, биологического, химического и даже ядерного оружия террористов, а также тактики осуществления террористических актов.

Террористические акты в информационном пространстве могут совершаться не только отдельными лицами или террористическими группами, но и одним государством против другого. В этом информационный терроризм ничем не отличается от любого другого вида терроризма. Экстремистские группировки, сепаратистские силы, проповедники идей, противоречащих общечеловеческим ценностям, интенсивно используют современные технологии для пропаганды своей идеологии и ведения информационных войн.

Для борьбы с информационным терроризмом необходимо создание эффективной системы взаимосвязанных антитеррористических мер, направленных на защиту информационных ресурсов от неправомерного использования и несанкционированного вмешательства.

Одним из важнейших обстоятельств, определяющих в правовом государстве успех предупреждения, выявления и пресечения возможных проявлений информационного терроризма, является создание адекватного социально-политической и криминальной обстановке в стране национального антитеррористического законодательства, основывающегося на общепризнанных всеми государствами антитеррористических принципах. Систему правового регулирования информационной безопасности составляет совокупность правовых норм, регулирующих отношения в области защиты информации, правоотношения, возникающие на основе применения соответствующих правовых норм, и соответствующие правоприменительные акты.

Несмотря на неоспоримую необходимость законодательного регулирования информационной безопасности, в России только в 2000 г. Президентом РФ была подписана Доктрина информационной безопасности, которая, по сути, и сегодня является единственным правовым регулятором защиты информации в России. Однако Доктрина информационной безопасности в РФ производит впечатление далеко не полностью разработанного и осознанного правового документа. Это связано, прежде всего, с тем, что значительное количество юридических категорий, например таких как «информационная сфера», «информационная инфраструктура» и т. д., не имеют четкой формулировки.

Следует отметить, что сегодня в России начато формирование базы правового обеспечения информационной безопасности. Приняты Федеральные законы «Об информации, информатизации и защите информации», «Об электронной цифровой подписи», «Об участии в международном информационном обмене», Закон Российской Федерации «О государственной тайне», Основы законодательства Российской Федерации об Архивном фонде Российской Федерации и архивах, ряд других законов. Однако анализ действующего законодательства на соответствие задачам, сформулированным в Доктрине информационной безопасности в РФ, подтверждает слабое нормативно-правовое обеспечение ее положений.

Также в настоящее время проводится работа по созданию механизмов реализации правого обеспечения информационной безопасности, разработке и подготовке законопроектов, регламентирующих общественные отношения в информационной

сфере, осуществляются мероприятия по обеспечению информационной безопасности в федеральных органах государственной власти, органах государственной власти субъектов Российской Федерации, на предприятиях, в учреждениях и организациях независимо от формы собственности, обеспечивается по мере возможности ознакомление населения с основными принципами обеспечения информационной безопасности и т. д. Помимо этого, обеспечению информационной безопасности Российской Федерации способствуют государственная система защиты информации, система защиты государственной тайны, системы лицензирования деятельности в области защиты государственной тайны и системы сертификации средств защиты информации.

Несмотря на все вышеперечисленное, состояние обеспечения информационной безопасности в Российской Федерации оставляет желать лучшего. Уровень правовой защищенности информационных ресурсов не соответствует сложившимся потребностям населения, а также постоянно набирающему обороты информационному и техническому прогрессу.

Исправить сложившуюся ситуацию представляется возможным только при соответствующем законодательном закреплении положений Доктрины информационной безопасности массивом нормативно-правовых актов. Необходимо дать четкую правовую характеристику таким категориям, как «информационный терроризм», «информационная война», «информационное оружие» и т. д. Для этого необходимо в первую очередь обеспечить целенаправленную деятельность всех государственных органов и общественных организаций по существующим аспектам информационной безопасности.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Газизов Р.Р.* Информационный терроризм // Материалы Международной научно-практической конференции 16–17 октября 2003 г. Часть I. – Уфа: РИО БашГУ, 2003. – 280 с.

С.С. Бойко

ОРГАНИЗАЦИОННО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ГОСУДАРСТВЕННОЙ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ «ПРАВОСУДИЕ»

В связи с изменениями социально-экономической обстановки в России, ростом преступности, увеличением и качественным изменением содержания судебных дел, расширением возможностей обжалования в суде неправомерных действий должностных лиц информационная нагрузка на суды возрастает с каждым годом. В этих условиях одним из основных путей повышения эффективности работы судов является внедрение новых информационных технологий и электронного документооборота в деятельность суда (т. е. проведение работ по информатизации). Судебный департамент при Верховном Суде Российской Федерации с самого начала своей работы уделял постоянное внимание проблеме информатизации судов общей юрисдикции, а начиная с 2004 г. активно ведутся работы по разработке и внедрению Государственной автоматизированной системы «Правосудие».

В Постановлении Совета судей РФ от 9 декабря 2005 г. № 144 «О ходе выполнения работ по информатизации судов и системы Судебного департамента при Верховном Суде Российской Федерации, проводимых в рамках федеральной целевой программы «Развитие судебной системы России» на 2002–2006 годы» Судеб-