

2.7. ИНФОРМАЦИОННЫЙ ТЕРРОРИЗМ КАК УГРОЗА НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Бураева Людмила Александровна, канд. физ.-мат. наук. Должность: доцент. Место работы: Северо-Кавказский институт повышения квалификации. Филиал: филиал Краснодарского университета МВД России. Подразделение: кафедра деятельности ОВД в особых условиях. E-mail: luda_n1@mail.ru

Аннотация: В статье рассмотрены актуальные проблемы противодействия информационному терроризму в современных условиях, которые затрагивают широкий круг не только частных и корпоративных интересов, но и угрожают национальной безопасности Российской Федерации. Обозначены главные тенденции развития информационных угроз в современном глобальном информационном пространстве и меры, необходимые для их нейтрализации. Приведен правовой аспект вопросов противодействия информационному терроризму в Российской Федерации.

Ключевые слова: *информационный терроризм, информационные угрозы, национальная безопасность, информационная безопасность, глобальное информационное пространство, терроризм, кибертерроризм, кибербезопасность.*

INFORMATIONAL TERRORISM AS THE RUSSIAN FEDERATION NATIONAL SECURITY THREAT

Burayeva Lyudmila Aleksandrovna, PhD in Math and Physics. Position: Associate Professor. Department: Police actions in special circumstances chair. Place of employment: North-Caucasian Institute of Advanced Training. Branch: Krasnodar University of MIA Russia branch. E-mail: luda_n1@mail.ru

Annotation: The article deals with actual problems of combating information terrorism in modern conditions, which affect a wide range of not only private and corporate interests and threaten the national security of the Russian Federation. Identifies the main trends in the development of cyber threats in today's global information space and the measures necessary to neutralize them. Given the legal aspect of combating information terrorism in the Russian Federation.

Keywords: *informational terrorism, information threats, national security, information security, global information space, terrorism, cyber-terrorism, cyber-security.*

На современном этапе информационный терроризм представляет серьезную угрозу безопасности и жизненно важным интересам как личности, так и общества и государства в целом. Степень опасности информационного терроризма стремительно возрастает в современных условиях глобализации, в которых средства телекоммуникаций приобретают исключительно важное значение. Сегодня мы наблюдаем активное проникновение и усиливающееся влияние новых информационно-коммуникационных технологий во все сферы человеческой деятельности. Всемирная паутина и мобильные телефоны стали неотъемлемой и обязательной частью нашего существования. По данным аналитиков сегодня глобальное информационное пространство, представляющее совокупность инфор-

мационных ресурсов и инфраструктур, составляющих как государственные и межгосударственные компьютерные сети, телекоммуникационные системы и сети общего пользования, так и иные трансграничные каналы передачи информации, насчитывает уже около 3,2 миллиардов пользователей [0]. Поэтому в условиях глобализации и информатизации общества, при которых барьеры контроля и управления информационными потоками практически отсутствуют, а национальные границы государств нивелированы, в частности, в коммуникативном аспекте, для развития информационного терроризма появились дополнительные факторы, усиливающие воздействие на сознание и поведение людей.

Рассматривая понятие информационного терроризма предполагают, прежде всего, форму негативно-го воздействия на личность, общество и государство в целом, с использованием всех видов информации. При этом прямое воздействие на психику и сознание людей проводится для формирования требуемых мнений и суждений, которые впоследствии определенным образом направляют поведение людей. На практике, под информационным терроризмом, как правило, подразумевают определенное насильственное пропагандистское воздействие на психику человека, которое не дает ему возможности критически оценивать получаемую информацию. При этом в стремлении добиться своих целей злоумышленники используют не качество манипулятивного воздействия, а объем откровенно тенденциозной информации. В своем распространении информационный терроризм, как правило, опирается на распространение определенного типа слухов, цель которых – многократно усилить атмосферу страха и ужаса, на создание которой направлены усилия террористов. Обычно в рамках информационного терроризма наиболее часто используемыми разновидностями слухов являются слухи с целью запугать, посеять панику. Подобного рода слухи вызывают выраженные негативные, пугающие настроения и эмоциональные состояния, которые отражают какие-либо актуальные, однако нежелательные ожидания аудитории, в которой они возникают и распространяются. Как правило, указанные слухи возникают или специально «запускаются» силами, развязывающими информационный террор, в массовое сознание людей в периоды социального напряжения, например, во время террористических актов, войн, стихийных бедствий. Быстрое распространение такого рода слухи приобретают во время проведения сложных политических и социальных реформ, смены власти, режима или социально-политической системы в целом. Например, грядущее неизбежное повышение цен на продукты питания, их скорое исчезновение или приближающийся голод. Доверяя таким слухам, население бросается закупать продукты в неразумно огромных объемах, что приводит впоследствии к искажению конъюнктуры рынка. Вследствие чего, товары стремительно исчезают с прилавков магазинов или быстро растут в цене, в результате чего может возникнуть голод. «Продуктовая паника», вызванная слухами о том, что в ночь произойдет повышение цен на продукты на 20-50% , наблюдалась в Улан-Удэ в декабре 2014 года [0]. Поддавшись действию «сарафанного радио», многие горожане в буквальном смысле ринулись закупаться самыми необходимыми продуктами, в результате чего ближе к вечеру в отдельных крупных магазинах города полки с продуктами были опустошены, были раскуплены все «стратегические» запасы –

крупы, макароны, масла и прочие продукты первой необходимости.

Сложным явлением, влияющим на национальную безопасность государства, является «банковская паника», заключающаяся в массовом изъятии депозитов вкладчиками в связи с утратой доверия к конкретному банку или банковской системе в целом, опасением неплатежеспособности или банкротства банка, падением курса национальной валюты, усилением инфляции, нестабильностью функционирования финансовой системы государства. Последствия банковской паники являются разрушительными для всей экономической системы страны. По подсчетам специалистов МВФ, расходы на ликвидацию последствий крупных кризисов, которые начинались с банковских паник, в период с 1970 по 2007 годы в среднем составляли около 13% ВВП пострадавшей страны. Ярким примером может служить политическая нестабильность на Украине, которая в 2014 году привела к обострению банковской паники в стране. Спусковым крючком для этого стал отток капиталов бывшей властной верхушки. Набеги на банки повлекли за собой падение ликвидности и ухудшение финансового состояния, и как следствие – цепочку банкротств наиболее слабых банков Украины. Давление макрофинансовых шоков, связанных с обесцениванием гривны, падением промпроизводства и уровня жизни населения, умноженное на многочисленные военные угрозы, тектонические политические сдвиги и ограничительные меры регуляторов, создало атмосферу страха – идеальные условия для паники среди клиентов банков. Так разворачивалась крупнейшая в истории Украины XXI века банковская паника, уроки которой стоит усвоить всем государствам мира для обеспечения национальной безопасности [0].

Особую роль в рамках информационного терроризма играют слухи, которые непосредственно связаны с реальным террором. Обычно они основываются на ожидании повторения уже происшедших террористических актов. Основная задача данных слухов: запугать население, усилить атмосферу террора в сфере информационного воздействия, создать и усилить хаос, неразбериху, реальную угрозу национальной безопасности страны.

Агрессивные слухи – это слухи конкретно направленные на стимулирование агрессивного эмоционального состояния и поведения, жесткого агрессивного действия. Указанные слухи, как правило, возникают во время острых противоречий, связанных с межэтническими, межнациональными, социальными межгрупповыми конфликтами, они ведут к нарушению общественного порядка [0] и угрожают национальной безопасности.

Основная задача агрессивных слухов состоит в направленной пропаганде агрессивных, террористических действий [0] типа геноцида и массовых убийств. Обычно слухи такого рода строятся отрывочно и представляют собой короткие, рубленые фразы, сообщающие о конкретных «фактах», «взывающих к отмщению». Они несут мощный эмоционально-отрицательный заряд, который формирует аффективную общность из «нормальных людей» в противовес «зверствующим нелюдям». Агрессивные вызывают к ответной агрессии. Как пример, можно привести слухи о зверствах федеральных войск в Чечне. Так, 14 января 2003 года были распространены слухи о расстреле с блокпоста федеральных сил автобуса Грозный-Гудермес, в результате чего был убит водитель и ранены четверо пассажиров [0]. Вскоре информация о

мифическом расстрелянном автобусе была опровергнута администрацией Гудермеса, а чеченские врачи заявили, что поступления к ним раненых не было. Бездарно спланированная провокация провалилась, однако в сознании многих людей прочно закрепился тезис о зверствах федералов в Чечне. Аналогично распространялись слухи о «зверствах чеченских боевиков» в отношении федеральных войск.

В настоящее время к устройствам наиболее высокой степени уязвимости в плане информационного терроризма относятся мобильные устройства. Повсеместно используемая программная платформа для мобильных устройств Android, доля которой составляет на рынке около 80%, основана на «открытом» коде, подконтрольном специальным службам США. Данное явление создаёт реальную угрозу для национальной безопасности страны, переводя её под контроль иностранных спецслужб. При этом доля разрабатываемых вредоносных программ для операционной системы Android, нацеленных на Android-устройства, стремительно растет. С целью слежки за людьми, пользующимися современными средствами связи, вредоносное программное обеспечение скрыто устанавливается на мобильные устройства. При этом по данным издания «Wall Street Journal», ФБР располагает технологиями, которые позволяют удаленно включать микрофон на смартфонах и планшетах под управлением операционной системы Android и вести запись. То есть, фактически, мобильный телефон превращается в «жучок», который вы носите при себе повседневно. Тревогу по данному вопросу уже забили власти КНР, которые усмотрели национальную угрозу в платформе Android. Обеспечение кибербезопасности в данном направлении состоит в развитии производства электронных изделий и каналов сбыта инфокоммуникационных решений внутри страны. В целях комплексного решения проблемы необходимо организовать ряд системных НИОКР среди компетентных предприятий для обеспечения вывода на рынок востребованных продуктов мирового уровня. Это позволит государству на федеральном уровне сформировать защищенную инфраструктуру информационной безопасности и обеспечить развитие экономики на основе производства отечественных инфокоммуникационных решений.

Все большие обороты набирают преступления террористической и экстремистской направленности [0, 0, 0] в сети Интернет. Уже к 1998 году примерно 30 террористических организаций имели свои интернет-сайты [0], в настоящее время в мировой сети представлены все активно действующие террористические и экстремистские организации, при этом многие из них имеют более одного сайта на нескольких языках.

Правовая база противодействия информационному терроризму и обеспечения информационной безопасности в России последовательно развивается с 2000 года, когда была принята Доктрина информационной безопасности Российской Федерации [0]. С 2008 года действует Указ Президента РФ от 17 марта 2008 года № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» [0]. В 2013 году утверждены «Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года» [0].

Однако, проблемы, имеющиеся в сфере противодействия информационному терроризму, на совре-

менном этапе, не могут быть полноценно решены традиционными методами. Они требуют системного подхода при формировании комплексной системы безопасности, способной противостоять многочисленным информационным угрозам.

Список литературы:

1. Абазов, И.С. Особенности и специфика тактических действий подразделений ОВД при обеспечении охраны общественного порядка на массовых мероприятиях // Теория и практика общественного развития, 2016. – № 2. – С. 75-78.

2. Бураева, Л.А. О некоторых вопросах обеспечения кибербезопасности в современных условиях / Л.А. Бураева // Теория и практика общественного развития, 2015. – № 13. – С. 96-99.

3. Бураева, Л.А. Террористические объединения в глобальном информационном пространстве / Л.А. Бураева // Пробелы в российском законодательстве, 2014. – С.274-276.

4. Гаужаева, В.А. http://elibrary.ru/author_items.asp?authorid=681401ризнаки терроризма, формирующие его понятие в нормативных и научных источниках // Актуальные вопросы юридических наук в современных условиях. Сборник научных трудов по итогам международной научно-практической конференции. г. Санкт-Петербург, 2015. – Инновационный центр развития образования и науки. – С.69-72.

5. Доктрина информационной безопасности Российской Федерации: утв. Президентом РФ В.В. Путиным 9 сент. 2000г. № Пр-1895 // Рос. Газ.–2000. – 28 сент.

6. Как творятся легенды о «зверствах» федералов. Информационное агентство «Утро» (свидетельство о регистрации СМИ Эл №ФС 77-57207). [Электронный ресурс]. URL: <http://www.utro.ru/articles/2003/01/23/123493.shtml> (дата обращения: 29.06.2016г.).

7. Карданов, Р.Р. Роль судебно-криминалистических экспертиз в антитеррористической деятельности // Доклады Адыгской (Черкесской) Международной академии наук. 2014. – № 1. – Т. 16. – С. 92-96.

8. О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена: указ Президента РФ от 17 марта 2008г. № 351 (ред. от 22.05.2015) // Собр. законод. РФ. – 2008. – № 12. – Ст. 1110.

9. Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года: утв. Президентом РФ 24 июля 2013г. № Пр-1753// Правовая база «КонсультантПлюс».

10. «Продуктовая паника» в Улан-Удэ спровоцирована ритейлерами? Портал деловой информации (свидетельство о регистрации СМИ ИА Эл. № ФС77-54407). [Электронный ресурс]. URL: <http://asiarussia.ru/news/5409/> (дата обращения: 29.06.2016г.).

11. Токбаев, А.А. Современные аспекты противодействия терроризму// Актуальные проблемы гуманитарных и естественных наук, 2013. – № 10-2. – С. 134-136.

12. Уроки и последствия банковской паники в Украине. Независимое информационное издание. [Электронный ресурс]. URL: <http://mediavektor.org/6405-uroki-i-posledstviya-bankovskoy-paniki-v-ukraine.html> (дата обращения: 29.06.2016г.).

13. Шагапсов, З.Л. Современные контуры системы противодействия различным проявлениям террориз-

ма: учеб.пособие /З.Л. Шагапсов, Б.А. Тарчоков.– Нальчик: СКИ (ф) КрУ МВД России, 2012. – 136 с.

Рецензия

на статью «Информационный терроризм как угроза национальной безопасности Российской Федерации», подготовленную доцентом кафедры деятельности ОВД в особых условиях Северо-Кавказского института повышения квалификации (филиал) Краснодарского университета МВД России, Бураевой Людмилой Александровной

В статье, представленной на рецензирование, автором Бураевой Л.А. рассмотрены актуальные проблемы противодействия информационному терроризму в современных условиях, которые затрагивают широкий круг не только частных и корпоративных интересов, но и угрожают национальной безопасности Российской Федерации.

В современных условиях глобализации, когда средства телекоммуникаций приобрели исключительное значение, степень опасности информационного терроризма стремительно возросла. Сегодня наблюдается активное проникновение и усиливающееся влияние новых информационно-коммуникационных технологий на все сферы человеческой деятельности. Вследствие этого, в условиях глобализации и информатизации общества, при которых барьеры контроля и управления информационными потоками практически отсутствуют, а национальные границы государств нивелированы, в частности, в коммуникативном аспекте, для развития информационного терроризма появились дополнительные факторы, усиливающие воздействие на сознание и поведение людей.

В статье автором рассмотрены основные тенденции развития информационных угроз в современном глобальном информационном пространстве и меры, необходимые для их нейтрализации. Приведен правовой аспект вопросов противодействия информационному терроризму в Российской Федерации.

Считаю, что в статье «Информационный терроризм как угроза национальной безопасности Российской Федерации», представленной Бураевой Л.А. рассматриваются достаточно актуальные на сегодня проблемы и она может быть рекомендована к опубликованию.

Начальник кафедры специальных дисциплин Северо-Кавказского института повышения квалификации (филиал) Краснодарского университета МВД России к.ю.н., полковник полиции М.М. Ардавов