ВЗГЛЯД. РАЗМЫШЛЕНИЯ. ТОЧКА ЗРЕНИЯ

УДК 343.985

Владимир Олегович ДАВЫДОВ,
заместитель начальника
Управления МВД России по Тульской области,
доктор юридических наук, доцент,
Почетный сотрудник МВД России,
лауреат премии МВД России в области науки
VladDv71@yandex.ru

КОГНИТИВНЫЕ ТЕХНОЛОГИИ ТРАНСФОРМАЦИИ СОЦИАЛЬНОГО ПОВЕДЕНИЯ В МЕХАНИЗМЕ ПРЕСТУПНОЙ ДЕЯТЕЛЬНОСТИ ЭКСТРЕМИСТСКОГО И ТЕРРОРИСТИЧЕСКОГО ХАРАКТЕРА: КРИМИНАЛИСТИЧЕСКИ ЗНАЧИМЫЕ СВЕДЕНИЯ

COGNITIVE TECHNOLOGIES OF TRANSFORMING SOCIAL BEHAVIOR IN THE MECHANISM OF CRIMINAL ACTIVITY OF EXTREMIST AND TERRORIST NATURE: FORENSICALLY SIGNIFICANT DATA

В статье рассматриваются криминалистически значимые аспекты механизма когнитивных технологий трансформации социального поведения. Исследуются способы преступных действий подобного рода, реализуемые членами экстремистских и террористических формирований. Полученные автором результаты могут быть использованы в процессе выработки комплекса мер превентивного характера, в том числе в информационно-телекоммуникационном пространстве сети Интернет.

The article considers forensically significant aspects of the mechanism of cognitive technologies of transforming social behavior. The ways of criminal activities of this kind carried out by the members of extremist and terrorist groups are studied. The results obtained by the author can be used in the process of developing a set of the preventive measures, as well as in the information and telecommunication space of the Internet.

Ключевые слова: информационные технологии, когнитивные технологии, экстремизм, терроризм, криминалистика, способ, механизм преступления.

Keywords: information technologies, cognitive technologies, extremism, terrorism, Criminalistics, a way, mechanism of a crime.

Глобальная информатизация социума, обусловленная развитием технологий телекоммуникации, привела к беспрецедентному расширению возможностей доступа к разнообразному спектру информационных ресурсов. Безусловно, подобное свободное доведение и потребление информации детерминирует усиление социальной активности

граждан, служа созидательным целям повышения эффективности общественных и государственных институтов.

В то же время любой прогресс имеет и обратную, негативную сторону. В современном информационном обществе IT-технологии активно используют экстремистские и террористические формирования, по сути, изменяя механизм преступной деятельности рассматриваемого рода.

Обратим внимание на то, что еще в конце 90-х годов прошлого столетия американский эксперт Уэйн Раш, специализирующийся на публикациях в сфере технологий, прогнозировал, что в будущем радикальные группы полностью адаптируются к использованию сети Интернет как инструмента коммуникации, организации, вербовки, сбора денежных средств, стратегического позиционирования, связи с медиа [1, с. 4].

Несколько позднее (2002 г.) технология применения функционала сети Интернет в интересах террористических организаций стала предметом исследования американского ученого Тимоти Томаса в статье «Аль-Каида» и Интернет: опасность «киберпроектирования» [8].

Габриэль Вайман, профессор коммуникаций университета г. Хайфе (Израиль), сотрудник Международного центра Вильсона (США), начавший отслеживать и изучать террористические web-сайты еще с середины 1990-х годов, в книге «Террор в Интернете: новая арена битвы, новые вызовы» (2006 г.) указывал уже на восемь типовых направлений, по которым террористы реализуют свои цели в сети Интернет, а именно: проведение психологической войны; поиск информации; обучение; сбор денежных средств; пропаганда; вербовка; организация сетей; планирование и координация действий [2, с. 8].

Не вдаваясь в полемику по поводу научных публикаций подобного рода, полагаем возможным сделать вывод о том, что в условиях развития процессов глобализации способы интернет-коммуникации стали одним из узловых элементов в механизме преступной деятельности экстремистского и террористического характера. Этому в немалой степени способствовало наличие у информационно-телекоммуникационных технологий следующего «криминально привлекательного» функционала:

– возможность беспрепятственного доступа (в том числе носящего анонимный характер) к информационным ресурсам и, как следствие, масштабная аудитория пользователей;

– высокая скорость распространения информационных потоков;

– мультимедийность среды коммуникации;

– практическое отсутствие цензуры ввиду недостаточной эффективности традиционных механизмов контроля;

– постоянно возрастающие технологические возможности, позволяющие в числе прочих дистанционно координировать действия менее четко организованных радикальных структур и отдельных лиц, намеренных осуществлять преступные действия децентрализованно.

Результаты проведенного нами исследования позволяют говорить о том, что способы подобной коммуникации, осуществляемой в экстремистских и террористических целях, все чаще включают инструменты трансформации социального поведения, основанные на функционале когнитивных технологий [3; 6].

Криминалистически значимой чертой использования последних является определенная повторяемость поведенческих актов преступников. Именно это обстоятельство, на наш взгляд, позволяет выделить типичные способы действий, целью которых является оказание деструктивного воздействия на устойчивые личностные структуры и оперативные мотивации индивидов и социальных групп:

– способы, направленные на трансформацию ценностных ориентаций;

– способы, направленные на дезорганизацию социального поведения;

– способы, направленные на организацию опосредованной подготовки индивидов к радикальным действиям и их последующий ввод в общее поле «насыщающего террора» в стране-мишени (так называемая «Интифада социальных сетей»).

Несколько подробнее остановимся на совокупности преступных действий, лежащих в основе указанных способов.

Первое – совокупность действий по намеренному афишированию последствий реаль-

ных экстремистских и террористических актов (фактов смерти, получения телесных повреждений, физических и психических страданий и т.п.) в целях деструктивного воздействия на сознание социума и, как следствие, формирования негативного отношения к органам власти и правопорядка, не способным обеспечить надлежащую защиту граждан.

Наглядный пример подобных действий связан с афишированием трагических последствий террористического акта, связанного с захватом более 1100 заложников (детей, родителей, работников учебного заведения) в школе N 1 г. Беслана (Северная Осетия). И хотя большинство заложников были освобождены в ходе штурма, в результате теракта погибли 314 человек (в том числе 186 детей) [9, с. 87]. Практически непрерывный показ детских страданий на протяжении трех суток по различным информационным каналам привел к возрастанию в массовом социальном сознании стрессорных психоэмоциональных реакций.

Второе – совокупность действий по производству и распространению постановочного медиа-контента в информационно-телекоммуникационных ресурсах. Такой медиа-контент имеет как внутрирегиональную, так и международную направленность и направлен на реализацию следующих целей, в том числе значимых в аспекте формирования экстремистской мотивации:

– демонстрация материалов о жестоких казнях – деморализация противника, привлечение сторонников, желающих присоединиться к действительно «влиятельной» силе (например, значительный резонанс получают шокирующие ролики террористической организации ИГ в стиле эпического видео с эффектом «slow motion» (замедленное движение) с показательным обезглавливанием «западных крестоносцев»);

– демонстрация материалов об успешной коммерческой деятельности (например, в сфере бизнеса, сельского хозяйства и т.п.) – привлечение сторонников, в основе мотивации которых лежит корыстная заинтересованность;

– демонстрация материалов о жестоких наказаниях за нарушение догматов Корана (например, публичное отрубание конечностей за воровство, побивание камнями за измену и т.п.) – привлечение сторонников, в основе мотивации которых лежит поиск «торжества справедливости»;

– пропаганда идей торжества законов Шариата, фундаменталистских основ средневекового Ислама – привлечение сторонников, в основе мотивации которых лежит желание стать частью салафитского ислама, и другие.

Третье – действия по созданию и использованию игровых контентов альтернативной реальности «ARG» (Alternate Reality Games) в экстремистских и террористических целях, ключевым аспектом построения которых является так называемый принцип «tinag» (от англ. «this is not a game» – «это не игра») – участники до конца сомневаются в игровом характере происходящего, а ход игры в альтернативной реальности контролируется непосредственно разработчиками, а не искусственным интеллектом, как в компьютерных или консольных видеоиграх.

Одним из подобных масштабных игровых ресурсов, сочетающим виртуальные и реальные действия игроков, стал web-сайт «Большая игра. Сломай систему» (www.msigra.org, адрес регистрации – г. Чикаго, США), который в декабре 2009 г. в установленном законом порядке был признан экстремистским [5, с. 47]. Согласно сюжетной линии «Большой игры» игроки, входящие в игровой клан «белой расы» («земляне»), должны были в реальной действительности на первых шести уровнях совершать действия, направленные на причинение ущерба представителям кавказских и азиатских национальностей («пришельцы»), объектам органов государственной власти («система»). Начиная с седьмого уровня, игровые задания уже носили индивидуальный характер и рассылались игрокам непосредственно на личные электронные почтовые ящики.

Иными словами, в режиме игры осуществлялся подбор потенциальных сторонников, их вербовка или отсев, обучение практическим навыкам, опосредованное вовлечение в реальную экстремистскую и террористическую деятельность. Так, на web-сайте были размещены инструкции по изготовлению муляжей взрывных устройств и радиоуправляемых гир-

лянд из больших петард (раздел «Самопал своими руками»), фотоотчеты игроков о реально совершенных действиях и другие материалы аналогичной направленности.

Проведенное с позиций криминалистики системно-структурное изучение интерфейса web-ресурса «Большая игра. Сломай систему» позволило сделать некоторые выводы, имеющие, на наш взгляд, значение в аспекте выработки рекомендаций по профилактике преступной деятельности рассматриваемого рода криминалистическими средствами и методами:

– «игровой» ресурс был создан за пределами территории Российской Федерации; к его разработке привлекались как специалисты – носители русского языка (например, свойственна ориентация на молодежный сленг, характерный для России начала 2000-х годов), так и эксперты – носители английского языка (использование специфичных англоязычных словосочетаний, например, в сфере менеджмента термин «лучшие практики» (от англ. «best practice», передовой опыт») в аспекте «лучшие сценарии»);

– web-сайт был нацелен на охват аудитории Российской Федерации и Восточной Украины;

– ресурс был рассчитан на потенциальный охват молодежной аудитории в возрасте от 14 до 20 лет;

– тактическая цель ресурса: определение репрезентативной группы, потенциально готовой к протестным насильственным действиям в отношении федеральных и местных органов власти (их должностных лиц), лиц некоренной национальности, количественный и качественный анализ такой группы;

– стратегическая цель ресурса: запуск механизма эскалации насилия в конкретном географическом регионе;

– вероятные мишени радикальной активности: территории крупных федеральных и областных центров.

Вышеназванные выводы достаточно объективно указывают на то, что разработчики «игрового» ресурса занимались изучением ситуации именно применительно к регионам Российской Федерации, а сам проект, по всей видимости, являлся составной частью программы формирования ультранационалистического молодежного движения, деятельность которого предполагалось направить на дестабилизацию социально-политической ситуации в стране.

Акцентируем внимание и на том, что в ближайшее время неотъемлемым элементом «игровых» технологий «ARG», используемых в экстремистских и террористических целях, может стать краудфандинг – коллективное сотрудничество индивидов, добровольно объединяющих ресурсы, как правило, посредством информационно-телекоммуникационного пространства сети Интернет, в целях поддержки усилий других реципиентов. Например, в целях обеспечения криминальной безопасности необходимые для совершения террористического акта функции (например, разведки, рекогносцировки местности, доставки компонентов взрывных устройств и т.п.) можно анонимно делегировать ничего не подозревающим игрокам, участвующим в интерактивном квесте.

Четвертое – действия по разработке и использованию разнообразных смарт-форм пресоциализации, направленных на неосознаваемую индивидом смену социальных ролей и статусов (наглядный пример современной действительности – флешмоб, от англ. «flash mob», дословно «мгновенная, слепая толпа»).

Принято считать, что идея организации флешмоба посредством использованием коммуникационного потенциала сети Интернет принадлежит разработчику web-сайта «FlockSmart.com», программисту из г. Сан-Франциско (США) Робу Зазуэту. Заметим, что последний, как и американский социолог Говард Рейнгольд – автор научных исследований о возможностях использования киберпространства, предпочитает не использовать термин «flash mob», а называет подобные массовые акции «smart mob», т.е. «умная толпа» [7, с. 12].

Думается, что в числе криминалистически значимых характеристик смарт-технологий, используемых в деструктивных целях представителями экстремистских и террористических организаций, следует выделить:

– мобильность, достигаемую посредством использования разнообразных средств дистанционной коммуникации;

– использование в качестве основной потенциальной группы активистов (так называемой движущей силы) молодежи в возрасте от 17 до 20 лет, а в качестве «детской массовки» протестной активности – несовершеннолетних в возрасте от 13 до 16 лет;

– отсутствие стихийности самоорганизации – действия участников акции определяются заранее разработанным сценарием и носят пошаговый последовательный характер, завуалированно подводящий индивидов к совершению актов прямого насилия (например, скрытно принести, разлить и поджечь бензин на входе в избирательные участки; найти торговые павильоны, в которых предпринимательскую деятельность осуществляют лица некоренной национальности, заблокировать их двери, забросать павильоны петардами и т.п.);

– наличие в сценарии стратегической и нескольких тактических целей (в числе последних, например, задание прийти в назначенное место, занять конкретное помещение, развесить баннеры, нанести знаки и надписи в хорошо просматриваемых публичных местах и т.п.), акцентуированных в большинстве случаев на националистической мотивации;

– повсеместное применение тактики «осиного роя», основанной на организации множества действий («укусов»), носящих деструктивный характера, каждое из которых по своей сути незначительно, но их массовость и системность создают эффект тотального присутствия и в действительности оказывают дестабилизирующее влияние на состояние оперативной обстановки и деятельность структур, обеспечивающие общественный порядок;

– использование, в том числе и на подготовительном этапе, политтехнологических приемов, направленных на публичную дискредитацию лиц, занимающих должностные посты в органах власти и управления (в числе таких способов, например, так называемое «шельмование» (принижение роли), создание и распространение «черных списков» и др.);

– ограниченность действий по времени (участники акции приходят в указанное место, выполняют действия, предусмотренные сценарием, и одновременно расходятся).

Подчеркнем, что рассмотренные смарт-технологии активно применялись при организации «бархатной» революции в Югославии (2000 г.), «революции роз» в Грузии (2003 г.), «оранжевой» революции на Украине (2004 г.), «тюльпановой» революции в Киргизии и «революции кедров» в Ливане (2005 г.), при попытках «васильковой» революции в Белоруссии (2006 г.) и «цветной» революции в Армении (2008 г.), «укропной» революции в Молдавии (2009 г.), второй «дынной» революции в Киргизии и «жасминовой» революции в Тунисе (2010 г.), «твиттерной» революции в Египте и «демократической» революции в Ливии (2011 г.).

Пятое – действия по использованию технологии «Интифады социальных сетей». Данная технология начала активно формироваться на основе результатов анализа локального опыта палестинской «Интифады ножей» (другие названия: «Волна террора», «Интифада одиночек»), показавших, что террористические атаки в большинстве случаев осуществлялись спонтанно, достаточно часто террористы не принадлежали ни к одному из формальных политических движений.

Современные когнитивные технологии и сетевые средства коммуникации вывели процессы интифады на принципиально новый уровень: так как террористические атаки в израильско-палестинском конфликте (2015-2016 гг.) носили индивидуальный характер, то и подстрекательство к ним целесообразно осуществлять посредством использования функционала социальных сетей, определенное число пользователей которых можно отнести к так называемому «пассивному рою».

О данной категории мы ранее упоминали в исследовании, посвященном проблемам формирования методики расследования транснациональной преступной деятельности экстремистского характера, подразумевая под ней массовый псевдоструктурный уровень, объединяющий последователей в различных географических регионах, непосредственно не скрепленных функциональными связями с экстремистскими либо террористическими формированиями, но являющихся его потенциальными приверженцами [4, с. 130].

Узловой принцип механизма «Интифады социальных сетей» подразумевает, что индивид должен самостоятельно «созреть» для тер-

рористического акта, самостоятельно выбрать доступное для себя орудие (средство) его совершения, место и время. «Помощь» в данном процессе индивиду оказывают «собеседники» (представители профильных функциональных элементов экстремистских и террористических структур, отвечающие за вербовочную деятельность и пропаганду). При этом первичный отбор потенциального круга бойцов, как правило, ведется в автоматическом режиме, на основе выборки персональных данных социальных аккаунтов (место рождения и проживания, место работы, образование, семейное положение, хобби, направленность политических и религиозных взглядов, степень их радикализации и т.д.).

На следующих этапах, после формирования требуемого психологического профиля на основе технологий «больших данных» (в их числе, например, программное обеспечение «Hadoop», используемое для реализации поисковых и контекстных механизмов высоконагруженных сайтов, NewSQL платформа «HANA», обеспечивающая высокую скорость обработки поисковых запросов и т.д.), производится персональная отработка (так называемая «накачка») выбранных индивидов, их подготовка к радикальным действиям и последующему вводу в общее поле «насыщающего террора» в стране-мишени. Заметим, что практически одновременно технология «интифады социальных сетей» стала развиваться как в русле радикального ислама, так и в русле ультранационализма.

Изучение сведений открытых информационных источников позволяет говорить о том, что к числу преступных деяний террористического характера, реализованных по данной схеме, следует отнести теракт, совершенный Андерсом Брейвиком в г. Осло и на о. Утейа (Норвегия, 2011 г.), использование грузовых автомобилей для наездов в местах массового пребывания граждан в Ницце (Франция, 2016 г.), Берлине (Германия, 2016 г.), Лондоне (Великобритания, 2017 г.), Стокгольме (Швеция, 2017 г.). На территории Российской Федерации террористическим актом подобного рода можно считать нападение на приемную регионального управления ФСБ (г. Хабаровск, 2017 г.), совершенное А. Коневым. Результаты расследования показали, что на этапе подготовки преступник активно участвовал в сетевой игре, где подробно разбирался ролевой сценарий аналогичного нападения.

Обобщая сказанное, позволим тезисно высказать мнение по поводу перспективных направлений противодействия деструктивным технологиям рассмотренного рода.

Во-первых, основу рассмотренных способов трансформации социального поведения в экстремистских и террористических целях образует информационная компонента. Как следствие, эффективно реализовывать меры превентивного характера возможно лишь в форме информационного противоборства.

Во-вторых, данная информационная компонента находится в неразрывной связи с информационно-телекоммуникационной инфраструктурой и финансовыми ресурсами, находящимися в распоряжении экстремистских и террористических формирований. Налицо потребность в выработке системы мер, направленных на минимизацию инфраструктурной и ресурсной баз субъектов применения деструктивных технологий.

Особое место в научном осмыслении и выработке подобных мер должна занимать криминалистика – наука, задачей которой выступает разработка отвечающих современным реалиям борьбы с преступностью средств, методов, приемов и рекомендаций раскрытия, расследования и предупреждения преступной деятельности различных видов.

Библиографический список

1. Rash, W. Politic on the nets: Wiring the political process / W. Rash. – New York: W.H. Freeman, 1997.

2. Weimann, G. Terror on the Internet: The New Arena / G. Weimann. – Washington, DC: United States Institute of Peace Press, 2006.

3. Давыдов, В.О. Методика расследования транснациональной преступной деятельности экстремистского характера : дис. … докт. юрид. наук / В.О. Давыдов. – Ростов-на-Дону, 2019.

4. Давыдов, В.О. Методика расследования транснациональной преступной деятельности экстремистского характера : монография / В.О. Давыдов ; под науч. ред. А.Ю. Головина. – М.: Юрлитинформ, 2018.

5. Давыдов, В.О. Методика расследования экстремистских преступлений, совершенных в компьютерных сетях : монография / В.О. Давыдов ; под. науч. ред. А.Ю. Головина. – М.: Юрлитинформ, 2014.

6. Давыдов, В.О. Транснациональный экстремизм: криминалистический анализ : монография / В.О. Давыдов ; под науч. ред. А.Ю. Головина. – М.: Юрлитинформ, 2016.

7. Рейнгольд, Г. Умная толпа: новая социальная революция / Г. Рейнгольд. – М.: ФАИР ПРЕСС, 2006.

8. Томас, Т. Терроризм и Интернет: проблемы взаимодействия / Т. Томас // Право и безопасность. – 2001. – N 1. – URL: http://www.dpr.ru_1_9.htm (дата обращения: 14.04.2020).

9. Устинов, В.В. Россия: 10 лет борьбы с международным терроризмом / В.В. Устинов. – М.: Олма, 2008.