МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
АЛТАЙСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ЮРИДИЧЕСКИЙ ИНСТИТУТ
Региональный антитеррористический научно-методический центр
Кафедра уголовного права и криминологии

ЭКСТРЕМИЗМ И ТЕРРОРИЗМ В КИБЕРПРОСТРАНСТВЕ: УГРОЗЫ МИРУ И БЕЗОПАСНОСТИ ЧЕЛОВЕЧЕСТВА

Сборник материалов III Всероссийской студенческой научно-практической очно-заочной видеоконференции.

Барнаул 2020

УДК 343.9

ББК 67.51
Э 41

Редакторы:

Валерий Анатольевич Мазуров, член Экспертного совета по выработке информационной политики в сфере противодействия идеологии терроризма Антитеррористической комиссии Алтайского края, руководитель РАНМЦ «Антитерроризм», доцент кафедры уголовного права и криминологии Юридического института АлтГУ, кандидат юридических наук, «Почетный работник сферы образования РФ»;

Мария Александровна Стародубцева, ассистент кафедры уголовного права и криминологии юридического института Алтайского государственного университета, руководитель волонтерской организации «Антиэкстремизм».

Рецензенты:

А.А. Васильев, доктор юридических наук, доцент, директор юридического института, заведующий кафедрой теории и истории государства и права Алтайского государственного университета;

Е.А. Куликов, кандидат юридических наук, доцент кафедры уголовного права и криминологии Алтайского государственного университета, и.о. заведующего кафедрой;

А.П. Детков, доктор юридических наук, доцент, профессор кафедры уголовного права и криминологии юридического института Алтайского государственного университета;

Экстремизм и терроризм в киберпространстве: угрозы миру и безопасности человечества: сборник статей по итогам III Всероссийской студенческой научно-практической очно-заочной видеоконференции / под ред. В.А. Мазурова, М.А. Стародубцевой. – Барнаул: Изд-во Алт. ун-та, 2020. – 203 с.

ISBN 978-5-7904-2523-3

В сборник включены статьи участников проходившей 26 ноября 2020 г. в юридическом институте Алтайского государственного университета III Всероссийской студенческой научно-практической очно-заочной видеоконференции «Экстремизм и терроризм в киберпространстве: угрозы миру и безопасности человечества». В конференции приняли участие преподаватели и студенты Алтайского государственного университета, Барнаульского юридического института МВД России, Алтайского филиала Российской академии народного хозяйства и государственной службы при Президенте РФ, практические работники.

Сборник может быть полезен научным работникам, преподавателям, аспирантам, магистрантам, студентам юридических и других гуманитарных специальностей, работникам правоохранительных органов и всем, кто интересуется проблематикой экстремизма.

ISBN 978-5-7904-2523-3

УДК 343.9
ББК 67.51

СОДЕРЖАНИЕ

ПЛЕНАРНОЕ ЗАСЕДАНИЕ

Мазуров Валерий Анатольевич, член Экспертного совета по выработке информационной политики в сфере противодействия идеологии терроризма Антитеррористической комиссии Алтайского края,
руководитель РАНМЦ «Антитерроризм»,
доцент кафедры уголовного права и криминологии Юридического института АлтГУ,
кандидат юридических наук, «Почетный работник сферы образования РФ»,
г. Барнаул

Мазуров В.А. ПРОФИЛАКТИКА ЭКСТРЕМИЗМА И ИДЕОЛОГИИ ТЕРРОРИЗМА В ОБРАЗОВАТЕЛЬНЫХ ОРГАНИЗАЦИЯХ: ПРОБЛЕМЫ И ПУТИ ИХ РЕШЕНИЯ

В современном мире произошли серьезные изменения в международных отношениях. Локальные военные конфликты в ряде государств Ближнего Востока, Африки, противостояние между Республикой Израиль и арабским миром, политика вмешательства во внутренние дела указанных государств и насильственное свержение законных правительств, неизбежно привели к стремительному росту экстремизма, главным образом, религиозно-националистическому, религиозно-политическому и терроризму.

Отмечается активизация экстремистских и террористических проявлений и современной России, которые инспирируют внешние и внутренние деструктивные силы. Активная пропагандистская и вербовочная деятельность международных террористических организаций принимает новые организационные формы, для её ведения используются современные средства коммуникации. Объектами пропагандистских устремлений является современная молодежь, российские и иностранные студенты.

В этих условиях государство и общество сегодня проводит активную работу по минимизации националистических, экстремистских настроений и проявлений, противодействию распространения идеологии терроризма, преступлений экстремистской и террористической направленности. Сегодня можно констатировать, что в России создана действенная система мер по противодействию национализму, экстремизму и терроризму.

В этой работе отводится важное место образовательным организациям. Одним из важных официальных документов по организации профилактики идеологии терроризма с участием образовательных организаций является

Комплексный план противодействия идеологии терроризма в Российской Федерации на 2019-2023 годы, утвержденный Президентом Российской Федерации 28.12.2018 года № Пр-2665 (далее - Комплексный план).

Приоритетными задачами, на решение которых направлены мероприятия Комплексного плана и в которых принимают участие образовательные организации, являются:

- повышение эффективности профилактической работы с лицами, подверженными воздействию идеологии терроризма, а также попавшими под её влияние;

- реализация мер по формированию у населения Российской Федерации антитеррористического сознания;

- реализация мер информационно-пропагандистского характера и защиты информационного пространства Российской Федерации от идеологии терроризма.

В Алтайском крае принимаются меры по совершенствованию системы мер противодействия идеологии терроризму. По решению Антитеррористической комиссии Алтайского края, в 2019 году, сформирован и успешно работает Экспертные совет по выработке информационной политики противодействия терроризму (далее – Совет). Руководитель Совета – Министр образования и науки Алтайского края. В состав Совета входят два преподавателя Юридического института университета. По решению Антитеррористической комиссии края и Министерства образования и науки Алтайского края, на базе Юридического института университета образован Региональный антитеррористический научно-методический центр (далее – РАНМЦ), разработан и утвержден план работы центра на 2020-2023г.г.

В научно-методической и профилактической работе принимает участие ФГБОУ ВО «Алтайский государственный университет». Разработан долгосрочный план профилактики идеологии терроризма, приказом ректора создана рабочая группа по реализации плана. Активно и результативно работают студенческие волонтерские организации – «Кибердружина22» и «Антиэкстремизм». За активную профилактическую деятельность, руководителям этих организаций объявлена благодарность Министерства образования и науки Алтайского края.

В университете отработано взаимодействие с Антитеррористической комиссией Алтайского края, Экспертным советом по выработке информационной политики противодействия терроризму, вузами края, Барнаульской духовной семинарией. Ежегодно проводятся научно-практические конференции, семинары, конкурсы по проблемам противодействия экстремизму как идеологии терроризма и терроризму.

Указанные и ряд других мероприятий, позволяют говорить о том, что в университете в основном создана система мер профилактики экстремизма, идеологии терроризма и иных негативных проявлений в студенческой среде.

Вместе с тем, в целях совершенствования эффективности научно-исследовательской, методической и профилактической работы, предлагается

осуществить следующие мероприятия:

- в профилактическую работу вовлекать студенческую молодежь, причем на добровольной основе, а не по принуждению. Практика показывает, что в современной России растет число волонтерских студенческих организаций, которые ведут серьезную и результативную работу по профилактике национализма, экстремизма, идеологии терроризма и иных негативных проявлений в молодежной среде. Эффективность данной работы объясняется во многом потому, что с молодежью они значительно быстрее находят общий язык, точки соприкосновения, взаимопонимание. Активисты из числа молодежи служат примером, с точки зрения их гражданской позиции, правовых знаний, образа жизни и т.д.;

- серьезную опасность и негативное влияние на формирование мировоззрения, жизненной позиции российской молодежи оказывает информация негативного характера, распространяемая в сети Интернет. Имеются проблемы организационно-правового характера, позволяющие минимизировать распространение таких материалов. В этой связи, наряду с органами законодательной, исполнительной власти, в систему мер противодействия распространению материалов экстремистской, террористической и иной негативной информации в Интернете, могут вложить волонтерские и иные молодежные организации. Большую работу в этом направлении проводит российская молодежная организация «Кибердружина». Такая студенческая организация результативно работает в университете;

- в целях повышения эффективности научно-исследовательской, профилактической деятельности РАНМЦ, волонтерских и иных общественных организаций студентов в крае, а также с учетом п. 2.4. Комплексного плана, «осуществлять поддержку творческих проектов антитеррористической направленности, в том числе в рамках реализуемых грантовых программ»;

- практика молодежной политики в сфере профилактики негативных явлений, экстремизма, идеологии терроризма в образовательных организациях России показывает, что одним из эффективных методов проведения профилактических мероприятий является не запрещение или наказание, а предоставление возможности для творческой, интеллектуальной, спортивной самореализации. В этой связи, требуется целенаправленная, системная работа по организации занятости студенческой молодежи в общественно полезной деятельности – волонтерской, культурно-массовой, спортивной, научно-исследовательской и т.п. Создание при образовательных учреждениях медиацентров, которые формируют информационное образовательное пространство, с привлечением студентов к созданию контента. В этой работе приоритетное место должны занимать управление по внеучебной работе, лига студентов;

- в целях формирования эффективной системы профилактики, подготовить предложение в Министерство образования и науки Алтайского края и Антитеррористическую комиссию Алтайского края, по созданию онлайн курсов для специалистов в сфере противодействия радикальным идеологиям.

Дистанционная форма позволит обучающимся получить адресную экспертную поддержку.

Куликов Егор Алексеевич,
кандидат юридических наук,
доцент кафедры уголовного права и криминологии
Алтайского государственного университета,
и.о. заведующего кафедрой, г. Барнаул

Куликов Е.А. ЦИФРОВОЙ ЭКСТРЕМИЗМ: ОБЩЕЕ, ОСОБЕННОЕ И ЕДИНИЧНОЕ[1]

Готовность человека отстаивать свои взгляды перед другими людьми, доходя до крайности совершения преступлений, существовала во все времена. С появлением полноценных монотеистических религий такая готовность получила сильную сверхрациональную мотивацию, зачастую не требующую обоснования доводами разума, и не принимающую доводы разума. Религиозный экстремизм достиг апогея в эпоху религиозных войн периода Реформации, а в России - в эпоху раскола Восточной церкви. Новое время породило новые оттенки проявлений экстремизма.

Реформация в Западной церкви, раскол в Восточной и реформы Петра I - Екатерины II, привели к постепенному ослаблению церковной организации и замещению в некоторых сферах организациями секулярного толка. В дальнейшем они оформляются как политические партии и подобные им структуры.партийная структура во все времена существования партийных систем была сложной, но при любом политическом режиме в ней существовали радикальные течения. Так зарождается политический экстремизм и высшая точка его развития - политический терроризм. По сути, это такой же религиозный экстремизм, основанный на вере в сверхрациональное, но теперь уже в ином окрасе. На такое могут возразить: но ведь идеологическую основу политического экстремизма составляют рациональные теории, учения, тот же марксизм или народнический социализм.

Возможно для умеренных политических течений эти учения и имеют рациональное содержание. Но когда происходит радикализация, когда эта радикализация приобретает крайние формы экстремистского характера, рацио полностью проигрывает иррацио. Получается, что при формировании, наряду с религиозным, политического экстремизма, само явление качественно не меняется, просто приобретает особенности, и можно говорить также и об общем для них - об экстремизме как таковом.

Итак, политический и религиозный экстремизм соотносятся с явлением экстремизма как особенное и общее, а между собой - как видовые понятия

[1] Статья подготовлена прифинансовойподдержкеРоссийскогофондафундаментальныхисследований,научный проект№-00121«Теорияобщего,особенногоиединичноговуголовномправеРоссии:методологические,технико-юридическиеиприкладныеаспекты»

одного рода. В XIX веке, в связи с формированием народностей, развитием национального самосознания, и последующим образованием наций и национальных государств, появляется третий вид экстремизма - экстремизм национальный. Суть и смысл этого явления практически тот же, что и у двух других видов экстремизма, особенности имеет, опять же, идеологическая основа, которая здесь произрастает на национальной почве. Общее понятие экстремизма охватывает все его видовые разновидности и представляет собой идеологию и политику отстаивания своих взглядов и убеждений с возможностью применения крайних, радикальных, в т.ч. преступных методов. При этом виды экстремизма выделяются на определенной идейной основе, и каждый самостоятельный вид может считаться таковым только если идеологически отличается от ранее существовавших. Идеологическая наполненность, таким образом, это уже не количественная спецификация экстремизма, а качественная. И если есть такая качественная спецификация, значит имеются основания говорить об особенном в рамках экстремизма.

Исходя из этого определим, есть ли на сегодняшний день основания утверждать, что т.н. киберэкстремизм, или цифровой экстремизм, является самостоятельным видом экстремизма. Есть ли у него собственная идеологическая основа, отличающая от других видов экстремизма, определяющая его собственное качество? Думается, нет. С одной стороны, разговоры о цифровой эре, цифровой эпохе, цифровом обществе сейчас популярны. Отношения с искусственным интеллектом, биткоины - кибервалюта, в целом повышение роли информационных цифровых технологий в период “пандемии”, и многое другое, могут натолкнуть на мысль, что эти разговоры повествуют о действительно принципиально новом обществе.

С другой стороны, что содержательно поменялось в таком явлении, как экстремизм, с его проникновением в цифровую среду? Он приобрел цифровую форму, стал оставлять цифровой след, получил распространение повсеместно ввиду повсеместного распространения глобальной сети Интернет. Но как он был политическим, религиозным, национальным и т.п., так он таковым и остался. Содержание приобрело новую форму, но не образовало новое особенное в рамках общего понятия экстремизма. Таким образом, цифровой экстремизм - это не вид экстремизма, а его форма, наряду с печатным, вербальным, физическим и т.п. Разумеется, эта новая форма предполагает и совершенствование способов совершения преступлений экстремистской направленности, и корреспондирующее ему совершенствование тактики и методики, а также техники расследования такого рода преступлений, развитие системы предупредительных, профилактических мероприятий, и определенное трансформирование уголовного законодательства. Но все равно, это изменение не качественных, а количественных показателей экстремизма, при сохранении прежней его идеологической основы. В этом смысле цифровизация напоминает работу Иоганна Гутенберга и повсеместное развитие книгопечатания. Суть при этом остается неизменной.

Куранов Роман Юрьевич, руководитель Совета по профилактике негативных проявлений в молодежной среде
ФГБОУ ВО «Алтайский государственный университет»,
руководитель студенческой организации «Кибердружина 22»,
Юридический институт, АлтГУ, г. Барнаул

Куранов Р.Ю. МОЛОДЕЖНАЯ СТУДЕНЧЕСКАЯ ОРГАНИЗАЦИЯ В СИСТЕМЕ ПРОФИЛАКТИКИ ЭКСТРЕМИЗМА И ИДЕОЛОГИИ ТЕРРОРИЗМА В МОЛОДЕЖНОЙ СРЕДЕ – «КИБЕРДРУЖИНА 22»

В период изменений социально-психологической сферы человека, перехода к новой информационной культуре, отличающейся такими чертами, как глобализация, поликультурность, динамичность и нестабильность наблюдается рост кризисных ситуаций. Об этом свидетельствуют повышение уровня тревожности, агрессивности у подростков; рост явлений одиночества и отвержения, низкий уровень коммуникативной компетентности. Особые опасения вызывают факты и факторы потери смысла жизни, рост явлений девиации среди подростков и юношества. Это подкрепляется ослаблением многих факторов, обладающих потенциалом противодействия, нарастающим негативным влияниям. В их числе проявляется кризис института семьи и повышение негативного эффекта в информационном пространстве. В последнее время наблюдается увеличение отклоняющегося поведения среди подростков и старшеклассников. У молодых людей наиболее подверженных деструктивному влиянию, легче формируются радикальные взгляды и убеждения. Это приводит к тому, молодежь пополняет ряды экстремистских и террористических организаций. Экстремизм и терроризм – проблемы злободневные для России, которые угрожают не только нравственным и духовным устоям общества, но и жизни людей, целостности нашей многонациональной страны. Важнейшая задача современного образования – содействие полноценному личностному развитию детей, формирование человека – носителя гуманистических взглядов, идей толерантности в межэтнических отношениях.

В век новых информационных технологий социальные сети превратились в мощный инструмент управления сознанием и поведением молодых людей, в том числе и подростков. Этот инструмент активно, а главное, эффективно влияет на общественное мнение, как в России, так и за рубежом. Большинство террористических организаций ведут свою деятельность, в первую очередь используя Интернете. Так проще захватить умы молодых людей, учитывая доступность и популярность социальных сетей в молодежной среде. Террористические организации стремятся использовать любые коммуникационные возможности для пропаганды своих идей, привлечения

новых сторонников. В Интернете существует большое количество сайтов, не связанных напрямую с террористическими организациями, но разделяющих их идеологию.

Соцсети предоставляют экстремистским организациям большие преимущества длявовлечению молодых людей в их ряды. Это и простота доступа к информации, и независимость от географического расположения, и неограниченная потенциальная аудитория, и небольшие финансовые и материальные затраты. А еще анонимность общения, высокая скорость передачи информации, мультимедийность среды, позволяющая комбинировать различные типы передаваемой информации (текстовую, графическую, аудио и видеоматериалы). И что очень существенно, трудности в осуществлении контроля со стороны правоохранительных органов.

Вербовщики террористических организаций, активно используя личную информацию, вводимую пользователем при регистрации в соцсетях, анализируют отношение пользователя к той или иной проблеме и таким образом выявляют, подходит ли та или иная кандидатура для будущей вербовки.

На своих сайтах экстремисты размещают подробные сведения о своей деятельности, дают различные инструкции. Террористы практикуют работу на форумах различной направленности.

Таким образом актуальность данной проблемы не вызывает сомнений . И в связи с этим требуются решительные меры по активному противодействию, и предотвращению заявленной проблематики.

Для разрешения необходим комплексный подход, выраженный, прежде всего, в взаимодействии органов исполнительной власти и правоохранительных органов, учебных заведений и социально активной молодежи. На этом фоне депутаты Госдумы от "Единой России" подготовили законопроект о создании в России кибердружин, которые смогут вместе с правоохранительными органами выявлять в интернете противоправную информацию, в том числе экстремистского характера. По замыслу авторов, кибердружины будут создаваться по инициативе россиян в формате общественной организации, о деятельности которой нужно будет уведомить территориальный орган исполнительной власти, осуществляющего функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи. Документ обязывает прокуратуру, следственные органы, органы государственной власти и местного самоуправления сотрудничать с кибердружинами.

Как поясняют депутаты, сейчас в России формируется новое направление организации взаимодействия гражданского общества и уполномоченных органов власти в сфере противодействия распространению противоправной информации. Однако, несмотря на фактическое распространение деятельности кибердружин, существует ряд трудностей, связанных с непосредственной реализацией идеи. Прежде всего, авторы связывают это с отсутствием

соответствующего федерального закона, регламентирующего деятельность таких структур.

Для профилактической работы в интернете и социальных сетях в августе 2019 года студентами юридического института был подан проект «Выездная школа Кибердружины 22» на получение федерального гранта Росмолодёжи в рамках Всероссийского конкурса молодёжных проектов среди образовательных организаций высшего образования.

Основными целями данного проекта являются: Профилактика экстремизма и идеологии терроризма в социальных сетях среди подростков 14-18 лет; Противодействие распространению в сети Интернет противоправной информации.

Достижение указанных целей осуществляется посредством реализации следующих задач:

- Создание в общеобразовательных учреждениях Кибердружин;
- Осуществление подготовки (обучения) участников Кибердружин;
- Просвещение населения по вопросам безопасного поведения в сети Интернет, о действиях в случае обнаружения противоправной информации в сети Интернет, а также информации, способной нанести вред здоровью и развитию несовершеннолетних, о возможностях блокировки противоправной информации с помощью веб-фильтров;
- Оказание содействия территориальным органам федеральных органов государственной власти и органам государственной власти в борьбе с противоправной информацией;
- Участие в разработке законодательных инициатив, направленных на ликвидацию противоправной информации в сети Интернет.

Проект « Кибердружина 22» реализуется при поддержки НОЦ «Правовое обеспечение противодействия экстремизму и терроризму» при кафедре уголовного права и криминологии Юридического института ФГБОУ ВО «Алтайский государственный университет» , молодежного парламента Алтайского края .

В рамках реализации данного проекта с 11 по 23 ноября в Алтайском крае и Республики Алтай на базе двенадцати муниципальных образований состоялось важное образовательное мероприятие – «Выездная школа Кибердружины 22».

Команда проекта на протяжении двух недель проводила образовательные занятия в двенадцати муниципалитетах Алтайского края и Республики Алтай. Приняли участие более 800 школьников старших классов.

В программу школы входило:

- лекция «Личный СММ. Правила ведения социальных сетей»:

– лекция «Основы мониторинга. Блокировка сайтов, содержащих противоправный контент»:

– лекция «Профилактика экстремизма в учебных заведениях. Ответственность за распространение экстремистских материалов.

– встреча с приглашенными экспертами.
– викторина «По горячим следам»

По итогам Школы «Кибердружина 22» школьники получили все необходимые знания для безопасного времяпрепровождения в Интернете, а также сертификат Кибердружинника. Полученные знания ребята будут применять на практики у себя в школах, тем самым реализую основные цели и задачи социально значимого проекта. По завершении школы была создана интернет-площадка для сбора информации о сайтах с нежелательным контентом, составлен информационный буклет для рассылки по учебным заведениям, а также будут выпущены социальные видеоролики .

Стоит отметить, что реализация программ профилактики экстремизма требует достаточно высокого уровня подготовки субъектов, их интеграции в систему общей и специальной профилактики делинквентного поведения, а также умения и готовности адаптировать планы и программы с учетом быстро изменяющихся условий жизнедеятельности учащихся, местных и групповых особенностей.

Таким образом, можно отметить, что участие молодежных организаций в борьбе с экстремизмом и идеологией терроризма является основным и наиболее эффективным механизмом противодействия данным проявлениям.

Список литературы:

1.Указ Президента РФ от 12.05.2009 № 537 «О Стратегии национальной безопасности Российской Федерации до 2020 года».

2. Приказ МВД России от 14.07.2005 г. № 047 «О некоторых мерах по усилению борьбы с экстремизмом».

3. Обеспечение психологической безопасности в образовательном учреждении: практическое руководство / Под ред. И.А. Баевой. – СПб.: Речь, 2006. – 288 с.

Стародубцева Мария Александровна,
ассистент кафедры уголовного права и криминологии АлтГУ,
руководитель волонтерской
организации «Антиэкстремизм»,
г. Барнаул

Стародубцева М.А. О НЕКОТОРЫХ АСПЕКТАХ ПОДДЕРЖКИ РАЗВИТИЯ ВОЛОНТЕРСТВА В ОБЛАСТИ ОКАЗАНИЯ ЮРИДИЧЕСКИХ И СОЦИАЛЬНЫХ УСЛУГ В АЛТАЙСКОМ КРАЕ

Концепция развития добровольчества (волонтерства) в Российской Федерации до 2025 года определяет данную деятельность как безвозмездное исполнение работ либо услуг в определенных сферах [1]. На официальном уровне содействие расширению сети волонтерских организаций по стране является одним из приоритетных направлений социальной и молодежной политики. Поддержка добровольчества (волонтерства) осуществляется в рамках реализации Федерального закона «О благотворительной деятельности и добровольчестве (волонтерстве)» от 11.08.1995, Федерального закона «О некоммерческих организациях» от 12.01.1996, Распоряжения Правительства РФ от 29.11.2014 «Об утверждении Основ государственной молодежной политики Российской Федерации на период до 2025 года», Постановления Правительства РФ от 30.12.2015 «О государственной программе «Патриотическое воспитание граждан Российской Федерации на 2016-2020 годы», а также Резолюции Генеральной Ассамблеи ООН от 17.12.2015 «Интеграция добровольчества в дело мира и развития: план действий на следующее десятилетие и последующий период» [1].

В 2020 году, в связи с резким усложнением санитарно-эпидемиологической обстановки в мире и в России, деятельность волонтеров оказалась как никогда востребованной [2]. В частности, огромную популярность приобрели добровольцы в области социального обслуживания и социальной поддержки населения. Также стремительно набирает обороты оказание добровольных юридических услуг. Молодежь, в частности, студенты высших учебных заведений, организуют при содействии преподавателей правовые центры на базах юридических факультетов и институтов, объединяются в официальные организации со статусом юридического лица либо без такового.

Молодежные студенческие организации, волонтерские отряды считаются одной из форм студенческой самостоятельной организации и служат важным индикатором степени вовлеченности студентов в общественную жизнь

образовательного учреждения. Также это одна из форм профилактики интолерантного поведения в молодежной среде [3].

Рассмотрим некоторые аспекты волонтерской деятельности на примере студенческих организаций при высших учебных заведениях г. Барнаула.

В соответствии с государственной программой Алтайского края «Противодействие экстремизму и идеологии терроризма в Алтайском крае» основной волонтерской группой, объединяющей представителей разных высших учебных заведений г. Барнаула, является сводная инициативная группа «СИГОВАК». Она работает на базе сотрудничества с правоохранительными органами в антиэкстремистской и контртеррористической деятельности. Инициаторами создания указанной группы выступили студенты Алтайского педагогического университета. Основное поле деятельности волонтеров – работа с кураторами учебных групп, индивидуальная работа со студентами, входящими в группу риска [5].

Аналогичная инициативная группа существует и при Барнаульском юридическом институте (далее – БЮИ). Курсанты напрямую взаимодействуют с органами охраны правопорядка, работая общественными помощниками в следственных отделах. Также в сферу их работы входит участие в научно-практических и студенческих конференциях, активное вовлечение в них основной массы студенческой молодежи, выступление с лекциями в образовательных учреждениях г. Барнаула.

На базе юридического института Алтайского государственного университета (далее – АлтГУ) работают две независимые волонтерские организации контртеррористического характера – отряд «Антиэкстремизм» и «Кибердружина22». Волонтеры «Антиэкстремизма» преимущественно работают на базе колледжа АлтГУ с несовершеннолетними студентами, являющимися, вследствие недостаточно сформированной психологической устойчивости, первостепенным объектом вербовки в экстремистские и террористические объединения. Кибердружинники организуют выезды в населенные пункты Алтайского края и Республики Алтай, где в ходе «Школы Кибердружины» проводят мастер-классы по мониторингу социальных сетей на предмет выявления потенциально опасного контента [2].

Аналогичная работа проводится и в медицинском университете при поддержке Социально-психологической службы высшего учебного заведения. Учитывая большое количество обучающихся в Алтайском государственном медицинском университете (далее – АГМУ) иностранных граждан, было принято решение о выделении отдельного факультета иностранных студентов, с которыми отдельно работают волонтеры-психологи. Основной целью является адаптация иностранных граждан к учебному процессу и профилактика экстремистских и деструктивных проявлений. Отметим, что опыт АГМУ представляет особый интерес, поскольку данная образовательная организация является специализированным учреждением, подведомственным Министерству здравоохранения, и наличие в нем волонтерских групп, работающих с фактами

интолерантного поведения, указывает на взаимопроникновение двух, с виду совершенно изолированных друг от друга отраслей [4].

Однако, стоит отметить и немаловажную проблему. Все перечисленные студенческие организации слабо связаны между собой и практически не контактируют. Даже работающие на одном институте отряды «Антиэкстремизм» и «Кибердружина 22» почти не пересекаются. Только с 2018 г. налаживаются попытки взаимодействия между АлтГУ и АГМУ в рамках участия представителей медицинского ВУЗа в научно-практических конференциях юридического института. Причем, в данном сближении участвует только психологическая служба АГМУ, но никак не весь остальной массив ВУЗа. Что касается инициативной группы «СИГОВАК», с ней до сих пор волонтерами юридического института АлтГУ не налажено никаких связей. Так же и с курсантами БЮИ. Можно сделать вывод, что волонтерские объединения антиэкстремистской направленности в крае, безусловно, существуют, но целостной системы их сотрудничества не налажено до сих пор. Есть только отдельные попытки организаторов движений, не подкрепленные поддержкой со стороны руководства образовательных учреждений. Волонтерская инициатива – прекрасная вещь, но она требует детальной организации и регламентации, чего в настоящий момент явно недостаточно.

Обратимся теперь ко второму направлению волонтерской деятельности, широко развитому в Алтайском крае – социальная поддержка населения. И здесь, нужно признать, ситуация складывается гораздо лучше. В частности, в апреле 2020 года студенты АГМУ, являющиеся представителями Всероссийского общественного движения «Волонтеры-медики» и студенты Колледжа АлтГУ, состоящие во Всероссийской общественной организации «Молодая Гвардия Единой России», приняли участие во всероссийской акции взаимопомощи #МЫВМЕСТЕ.Была организована адресная помощь нетрудоспособным гражданам – пенсионерам – в доставке продуктов и лекарственных средств. Пожилым и малоподвижным жителям региона, находящимся на изоляции в период распространения инфекции COVID-19, были доставлены более двух тысяч бесплатных продуктовых наборов. В апреле 2020 года инициативная группа волонтеров проводила мониторинг цен на продукты первой необходимости в торговых сетях «Мария-Ра», «Ярче», «Магнит» и «Пятерочка». 09 мая волонтеры приняли участие во Всероссийской акции «Георгиевская лента», приуроченной к празднованию 75-й годовщины Дня Победы в Великой Отечественной войне.

30 мая 2020 года студенты провели ряд мероприятий по ремонту игрового оборудование, уборке мусора на детской площадке в рамках акции «Добро в действии».

01 июня 2020 года была проведена акция –поздравление детей, временно находящихся на лечении в Алтайской краевой клинической детской больнице, в рамках акции «Подари радость детям». Акция проводилась совместно с российской политической партией «Единая Россия» и региональным отделением всероссийского общественного движения «Волонтеры-медики».

18 августа 2020 года был проведен мониторинг спортивных площадок города Барнаул. Были проверены следующие школы: школа 88, школа 112, школа 75, школа 123, лицей «Сигма». В ходе проверки было проверено состояние спортивного инвентаря. Полученные данные были обработаны и переданы в органы Роспотребнадзора.

С 01 октября 2020 года волонтеры проводят обучение старшего поколения пользованию информационными системами в рамках месячника пожилого человека.

10 октября 2020 года добровольцы приняли участие в проекте по озеленению парка культуры и отдыха «Изумрудный» в рамках акции «ЭкоЛогично».

07 октября 2020 года в связи с неблагоприятной эпидемиологической обстановкой в Алтайском крае была возобновлена работа волонтерского штаба по оказанию помощи гражданам в условиях коронавирусной инфекции.

Можно увидеть комплекс разноплановых акций и мероприятий, проведенных инициативной группой волонтеров меньше чем за полгода. И это следует считать важным достижением в налаживании взаимодействия между высшими учебными заведениями г. Барнаула не только в научном, но и в практическом плане, так как концепция развития волонтерства говорит именно об этом.

В Алтайском крае в рамках работы всероссийской акции взаимопомощи #МЫВМЕСТЕ объединили свои усилия Управление молодёжной политики и реализации программ общественного развития Алтайского края, Общероссийский народный фронт в Алтайском крае, Алтайский центр развития добровольчества, Волонтёры Победы, Волонтёры-медики, партия «Единая Россия», Алтайский государственный медицинский университет, а также «Молодая Гвардия Единой России» Алтайского края.

Необходимо присоединять к этой работе и другие волонтерские организации ВУЗов. На базе юридического института с 2012 года работает бесплатная клиника правовой помощи по гражданским делам «Фемида», а с 2018 года – платный Центр правовой помощи по гражданским делам АлтГУ [2]. Алтайскому государственному университету и другим ВУЗам стоит, по нашему мнению, выработать единую программу помощи и поддержки волонтеров, чтобы эти мероприятия проходили не разово, а оформились в целостную систему. Необходимо учесть психологический фактор, без отдачи к добровольчеству быстро теряется интерес, первокурсников новых наборов не так просто заинтересовать оказанием бесплатной помощи, и в волонтерских рядах начинается мощный отток. А этого мы, как руководители данных организаций, не должны допускать.

Список литературы:

1. Распоряжение Правительства РФ от 27.12.2018 N 2950-р. Об утверждении Концепции развития добровольчества (волонтерства) в Российской Федерации до 2025 года. [Электронный ресурс]. – Режим доступа:

http://www.consultant.ru/document/cons_doc_LAW_314804/ (дата обращения: 09.10.2020).

2. Мазуров В.А., Стародубцева М.А., Горовой С.А., Горовая В.Ю. Система студенческих отрядов в противодействии экстремизму и идеологии терроризма//Современный ученый. -2019. - № 6. - С. 203-208.

3. МВД сообщило о росте числа террористических и экстремистских преступлений. [Электронный ресурс]. – Режим доступа: https://www.kommersant.ru/doc/4415890(дата обращения 03.10.23020).

4. Обеспечение психологической безопасности в образовательном учреждении: практическое руководство / Под ред. И.А. Баевой. – СПб.: Речь, 2006. – 288 с.

5.Обрывко Е.И. Воспитательная работа по формированию толерантности, культуры мира и межнационального согласия в студенческой среде вуза // Вестник Алтайского государственного педагогического университета. - 2015. - № 23. - С. 89-90.

СЕКЦИЯ «АКТУАЛЬНЫЕ ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ ЭКСТРЕМИЗМУ КАК ИДЕОЛОГИИ ТЕРРОРИЗМА В КИБЕРПРОСТРАНСТВЕ И ПУТИ ИХ РЕШЕНИЯ»

Исаева Алла Владимировна,
начальник отдела детского творчества
и дополнительного образования
Калининградского областного института
развития образования,
Почетный работник общего образования РФ

Исаева А.В. ДЕЯТЕЛЬНОСТЬ ОБРАЗОВАТЕЛЬНЫХ ОРГАНИЗАЦИЙ ПО ФОРМИРОВАНИЮ У ДЕТЕЙ И МОЛОДЕЖИ ОТРИЦАТЕЛЬНОГО ОТНОШЕНИЯ К ИДЕЯМ ЭКСТРЕМИЗМА И ТЕРРОРИЗМА НА ПРИМЕРЕ ОБЛАСТНОГО КОНКУРСА «БЕЗОПАСНАЯ РОССИЯ»

Одной из важных задач, стоящих перед образовательными организациям, является привлечение внимания детей и молодежи к вопросам террористической безопасности, вовлечение подрастающего поколения в созидательную, позитивную деятельность по профилактике экстремизма и терроризма, формирование основ поликультурного общения, осознанного отношения к миру и человеческим ценностям.

Не менее важна и другая задача – поставить заслон распространению идеологии терроризма и обеспечить раннее выявление очагов возникновения ситуаций, которые могут быть использованы для разжигания национальной и религиозной розни, а также не допустить психологического воздействия на молодёжь с целью распространения экстремистских идей. И крайне важно сформировать у детей и молодёжи устойчивое отрицание идей терроризма.

Для решения этих задач используются самые разнообразные формы работы, в числе которых проведение классных часов, уроков безопасности, реализация образовательных курсов и другие.

Еще один подход к этой работе – вовлечение детей, подростков, молодёжи в активную исследовательскую и творческую деятельность через участие в конкурсе «Безопасная Россия», который проходит в Калининградской области с 2016 года.

Конкурс проводитсяминистерством образования Калининградской области, институтом развития образования при поддержке аппарата Антитеррористической комиссиив рамках Государственной программы

Калининградской области «Безопасность» инаправлен наформирование гражданской позиции подрастающего поколения; активизацию деятельности образовательных организаций, творческих и общественных объединений; поддержку социально значимых идей и проектов, направленных на противодействие терроризму.

Конкурс проходит по нескольким номинациям: «Научно-исследовательская работа», «Социальный видеоролик», «Средства массовой информации», «Рисунок», «Сочинения» и его участниками являются учащиеся общеобразовательных организаций, организаций дополнительного и профессионального образования, студенты высших учебных заведений.

Конкурс вызывает неподдельный интерес у участников, которые в своих работах раскрывают важные и актуальные темы, в числе которых:

- Мы – за безопасные границы!
- Терроризм – зло против человечества
- Безопасность в наших руках!
- Личностный выбор каждого – залог безопасности страны
- Дети в интернете: контроль или свобода?
- Твой выбор: виртуальность? или реальность?
- Интернет: подводные камни и пропасти
- Интернет: не запутайся в сети!
- Мы разные, но мы вместе!
- Мирная планета для всех одна
- Когда мы едины - мы непобедимы.

Тема противодействия экстремизму и терроризму, так же, как и задача формирования у детей и молодёжи отрицательного отношения к проявлениям экстремизма, достаточно непростая и требует большой методической подготовки. Мы видим, как много делается педагогами для того, чтобы сформировать у детей и молодёжи устойчивое неприятие идей экстремизма и терроризма, и понимаем, что есть необходимость пополнения методической базы, а также выявления и систематизации лучшего опыта. Именно для этого с 2020 года было предусмотрено участие в Конкурсе педагогических работников, которые могут представить свой опыт в 2-х номинациях:

- методические разработки, направленные на противодействие идеям терроризма;
- методические разработки, направленные на обучение навыкам безопасного поведения в условиях террористической опасности.

Конкурс проводится уже пятый год, и помимо констатации увеличения количества участников, организаторы работают и над улучшением качества конкурсных работ, для чего предусмотрена серия семинаров и мастер-классов ведущих специалистов. Кроме того, для повышения качества конкурсных работ в 2020 году организаторами разработаны памятки участникам по каждой из номинаций – «10 советов как подготовить конкурсную работу».

Благодаря всем этим мерам возрос уровень представленных работ как в структурном, содержательном плане, так и в ценностно-смысловом отношении. От просто описательных работ сегодня участники конкурса пришли уже к глубоким размышлениям и, самое главное, к анализу проблемы и к осознанию того, что можно и нужно сделать, чтобы победить эти угрозы.

Представляемые на конкурс работы настолько серьезны, содержательны и глубоки, что было бы неправильно ограничить круг тех, кто познакомился с ними, только членами жюри. Поэтому в 2019 году было принято решение об издании сборника, в который вошли работы победителей в номинациях «Сочинения» и «Средства массовой информации», а в качестве иллюстраций были использованы рисунки участников Конкурса. Эта работа продолжена в 2020 году и уже подготовлен второй выпуск сборника, с электронной версией которого можно будет познакомиться на сайте Калининградского областного института развития образования.

Ход и результаты конкурса широко освещаются с использованием интернет-ресурсов министерства образования Калининградской области, института развития образования, аппарата АТК, а также с помощью телевидения, иных средств массовой информации. Кроме того, для представления работ участников и продвижения Конкурса была создана группа в социальной сети ВКонтакте: https://vk.com/konkursbr39, которая является неким примером позитивного и эффективного использования сети Интернет для продвижения идей противодействия экстремизма и терроризма. В этой группе размещается актуальная информация о конкурсе, проводятся творческие флешмобы, челленджи, акции, там же в этом году впервые проведен онлайн-конкурс – перекличка, в ходе которого участники представляли себя и свои коллективы и отправляли пожелания, в числе которых такие как: «Желаем всем мирного неба!», «Все зависит от нас самих! Удачи каждому!», «Детство, становись прекрасней, а Россия – безопасней!».

Выше было сказано, что конкурс стал уже традиционным, так же традиционным стало и проведение 3 сентября памятного мероприятия – День солидарности в борьбе с терроризмом, в ходе которого подводятся итоги конкурса «Безопасная Россия», награждаются победители, проходит чествование ветеранов вооруженных сил и правоохранительных органов, участников и ветеранов боевых действий и антитеррористических операций, педагогических работников за большую работу по патриотическому воспитанию, профилактике экстремизма и терроризма в детской и молодежной среде, что имеет сильное воспитательное воздействие на участников мероприятия – учащихся общеобразовательных организаций, организаций профессионального образования, студенты высших учебных заведений. Кроме того, здесь же в формате передвижной выставки экспонируются рисунки участников Конкурса.

Но сегодняшние реалии внесли свои коррективы, и в этом году организаторами проработан иной формат представления работ – это виртуальная выставка, размещенная на уже указанном ресурсе, а также на сайте

министерства образования Калининградской области, Калининградского областного института развития образования. В реалиях 2020 года в связи с ограничительными мерами и само памятное мероприятие в этом году прошло в онлайн формате в виде трансляции специального выпуска телевизионной программы «БЕЗОПАСНАЯ РОССИЯ». В рамках данного выпуска прошли тематические блоки, связанные с 75-летием Победы в Великой Отечественной войне, локальными войнами, состоялись интервью с ветеранами боевых действий и участниками контртеррористических операций, руководителем Аппарата Антитеррористической комиссии Правительства Калининградской области А.А.Толстовым, уполномоченным по правам ребенка при правительстве Калининградской области И.М.Ткаченко, руководителем Ассоциации воинов-интернационалистов «Боевое братство» ВВ.Кучером, учащимися образовательных организаций. Запись трансляции размещена на сайте Калининградского областного института развития образования, в уже указанной группе «Безопасная Россия» в социальной сети ВКонтакте.

Экстремизм и терроризм – это зло, с которым нужно бороться сообща, используя разные формы и методы. Мы понимаем, что эта тема очень сложная, и вести работу в данном направлении нужно очень корректно, с учетом психологических особенностей подросткового возраста, воздействуя на чувственно-эмоциональную сферу. И здесь важно и ценно то, что молодёжь сама задумывается над тем, как обезопасить себя и своих близких, как не дать вовлечь себя в экстремистские и террористические организации, как не поддаться на уловки сил, ведущих скрытую охоту и активно включается в данную работу.

Кот Е.А.,
аспирант кафедры уголовного процесса, криминалистики
и правовой информатики Балтийского федерального
университета им. И. Канта, Калининград

Кот Е.А. СИТУАЦИОННОЕ МОДЕЛИРОВАНИЕ В ИЗУЧЕНИИ ЛИЧНОСТИ ПОТЕРПЕВШЕГО НЕСОВЕРШЕННОЛЕТНЕГО ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ В СЕТИ ИНТЕРНЕТ, СВЯЗАННЫХ С ПОБУЖДЕНИЕМ К САМОУБИЙСТВУ

Ситуационное моделирование имеет важное значение в познавательной деятельности сотрудников правоохранительных органов по расследованию и раскрытию преступлений, представляя собой одну из основных форм познания действительности, а также эффективно применяется при разработке частных методик расследования отдельных видов преступлений.

Основателем школы криминалистической ситуалогии профессором Т.С. Волчецкой в научных трудах выделено несколько форм моделирования, такие как: материальное (предметное), логико-математическое и кибернетическое, информационно-компьютерное, мысленное (идеальное) и ситуационное[1].

Любое преступление представляет собой событие, произошедшее в объективной реальности, воплощающее модель «прошлого», имеющее не только определенную информационную структуру и механизм совершения преступного события, но и отражение типовых и индивидуально-психологических особенностей субъектно-объектных отношений в рамках сложившейся ситуации, обусловленных конфликтным взаимодействием.

По нашему мнению, именно мысленные модели составляют основу информационной модели преступления, связанных с суицидом, имея непосредственную связь с элементами криминалистической характеристики. Таким образом, мы выделили основные элементы криминалистической характеристики преступлений связанных с суицидом:

- типовая информация об обстановке совершения преступления,
- типовая информация о средствах, способах и механизме совершения преступлений,
- типовая информация о следах преступления,
- типовая информация о личности преступника и жертвы преступных посягательств.

Важное значение в построении мысленной модели события преступления имеет выявление типичных свойств и индивидуально-психологических

характеристик личности потерпевшего (несовершеннолетнего), которые играют важную роль в установлении криминалистически значимой информации о расследуемом событии, более того, находят основу в эффективной подготовке дальнейшего производства следственных действий и установления механизма преступного деяния. Допрос несовершеннолетних потерпевших имеет свои особенности, обусловленные спецификой подросткового возраста, к которой относятся: эмоциональная неустойчивость совпадающая с периодом неопределенности и вхождения во взрослую жизнь, повышенная сензитивность, а также отсутствия жизненного опыта и критического мышления. Кроме того, на формирование личности несовершеннолетнего, а также культурные, моральные, эстетические ценности, серьезное влияние оказывает сеть Интернет.

Уникальность ситуаций, в которых оказываются несовершеннолетние, состоит в том, что они непосредственно влияют на процесс принятия решения о суициде, ведь именно генерация суицидального поведения несовершеннолетнего, имеет форму эмоционального отклика на экстремальную ситуацию.

Сбор информации о личности несовершеннолетнего потерпевшего может осуществляться из различных источников, к примеру, в рамках изучения следовой картины преступления, обращая внимания на материальные следы преступления (книги, личные дневники, блокноты), идеальные следы (показания свидетелей, друзей, родственников, медицинских работников, сотрудников образовательных учреждений, а также сотрудников органов исполнительной власти) и электронные следы, находящие свое отражение в электронных носителях, компьютерах, смартфонах, в сети Интернет и др.).

На данном этапе развития информационного общества существенное влияние на формирование аутодеструктивного поведения несовершеннолетних оказывает именно цифровая среда. Цифровые технологии, мобильные устройства и социальные сети стали неотъемлемой частью повседневной жизни людей во всем мире. Важно отметить, что не смотря на все положительные стороны применения Интернет-ресурсов, широкое распространение в сети получил и феномен кибербуллинга, как наиболее часто встречающаяся форма психологического насилия в современном обществе. Данный факт находит свое отражение вгенерации и распространении в сети Интернет ложной информации, унижающей человеческое достоинство несовершеннолетнего, систематическом запугивании, оскорблении и организации публичной травли, распространении оскорбляющих сообщений или угроз через мессенджеры и др.Анонимность в Интернет-пространстве позволяет остаться незамеченным, что зачастую приводит к криминализации поведения агрессоров – лиц, оказывающих негативное влияние на жертв кибербуллинга[2]. Таковыми зачастую становятся именно несовершеннолетнее, подвергающиеся буллингу в реальной жизни.

Фиксируется увеличение числа суицидов среди детей и подростов, за счет увеличения вбросов и объемов деструктивного контента в социальные сети,

игровые платформы, мессенджеры. Это прежде всего связано с фактами распространения информации экстремистского содержания, суицидальной направленности, о наркотиках и иной информации, причиняющей вред здоровью и развитию несовершеннолетних[3].

Таким образом, типовая модель личности потерпевшего, как объект познавательной деятельности, рассматриваемого вида преступлений включает в себя следующие элементы:

- тендерные и возрастные особенности восприятия смерти детьми и подростками;
- наличие воздействия внутренних и внешних факторов, способных спровоцировать суицидальное поведение;
- индивидуальные личностные характеристики подростков, предопределяющие формы реагирования на конфликтную ситуацию;
- поведенческие особенности несовершеннолетнего в период формирования суицидальных намерений, иными словами - «маркеры суицидального поведения».

Ситуационный подход позволяет выявить типичную информацию о личности несовершеннолетних, путем установления факторов и мотивов, влияющих на формирование суицидального поведения, которые положат основу эффективной разработке и тактике проведения следственных действий, а также установления психологического контакта с потерпевшим [4].

Список литературы:

1. Волчецкая Т. С. Теоретические проблемы использования метода моделирования в криминалистической науке // Социальные и гуманитарные науки на Дальнем Востоке. 2012.№ 4 (36). С. 16-20.
2. Болвачев М.А., Кот Е.А. Кибербуллинг в социальных сетях/ В сборнике: VIII Балтийский юридический форум "Закон и правопорядок в третьем тысячелетии". Материалы международной научно-практической конференции. Калининградский филиал Санкт-Петербургского университета МВД России. 2020. С. 38-39.
3. Болвачев М.А. Особенности расследования преступлений экстремистской направленности, совершенных с использованием социальных сетей / В сборнике: Тенденции развития современной юриспруденции. Сборник научных трудов международной студенческой научной конференции Юридического института Балтийского федерального университета им. Иммануила Канта, научное электронное издание. Сер. "Трибуна молодых ученых" 2018. С. 168-173.
4. Бедризов А.Г., Волчецкая Т.С., Галяшин Н.В. и др. Криминалистическое изучение личности / Отв. ред. Я.В. Комиссарова. М., 2019.

Обернихина Олеся Валерьевна,
майор внутренней службы, преподаватель кафедры
уголовно-исполнительного права и криминологии
ФКОУ ВО Кузбасский институт ФСИН России, г. Новокузнецк

Обернихина О.В. КРИМИНОЛОГИЧЕСКАЯ ХАРАКТЕРИСТИКА КИБЕРЭКСТРЕМИСТСКОЙ ПРЕСТУПНОСТИ В РОССИИ И СПОСОБЫ ЕЕ ПРОФИЛАКТИКИ

Действенность системы мер по противодействию экстремизму в сети Интернет в настоящее зависит от объективности и глубины анализа данной преступной деятельности и изучения причин ее возникновения [1, С. 57].

Шанхайская Конвенция о борьбе с терроризмом, сепаратизмом и экстремизмом дает наиболее четкое понятие экстремизма как «какого-либо деяния, направленного на насильственный захват власти или удержание власти, а также на насильственное изменение конституционного строя государства, а равно насильственное посягательство на общественную безопасность, в том числе организация в вышеуказанных целях незаконных вооруженных формирований или участие в них» [2].

Исходя из положений ФЗ «О противодействии экстремистской деятельности» [3], а также Стратегии противодействия экстремизму в Российской Федерации до 2025 года, следует определить экстремизм как общественно опасные деяния, совершаемые физическими и юридическими лицами по мотивам политической, идеологической, расовой, национальной, религиозной ненависти или вражды, а также объективно опасные деяния, способствующие возникновению или обострению межнациональных, межконфессиональных и межрелигиозных конфликтов» [4].

Следует отметить, что на сегодняшний день с развитием технологий и телекоммуникаций, а также с изменениями развивающегося рынка, который опирается на инновационные технологии для оптимизации своей эффективности, экстремистская преступность приобретает новые формы существования, в частности, ее характеризуют следующие признаки:

- манипулирование общественным сознанием, выдвижение упрощенных вариантов решения сложных общественных проблем с помощью интернет ресурсов (как открытая, так и скрытая пропаганда);
- использование идеологии, социально-политической, национальной, расовой, религиозной ненависти или вражды, в том числе посредством сети Интернет;
- использование специальных знаний в сфере финансово-хозяйственной деятельности, в программном обеспечении банковской деятельности;

- применение (угроза применения) нелегитимного насилия для достижения выдвигаемых целей, в том числе посредством сети Интернет.

Кроме того, с точки зрения криминологии, уголовного и уголовно-исполнительного права преступность такого рода занимает три ниши, во-первых, ее смело можно называть профессиональной, во-вторых, ее следует относить к категории киберпреступность, в-третьих, современные способы и технологии возводят ее в ранг интеллектуальных преступлений.

Так, поскольку современные интернет технологии, по большому счету, прерогатива молодежи, то, как отмечают криминологи, преступность экстремистской направленности, тем более с использованием кибертехнологий значительно помолодела. Средний возраст преступника составляет 20-25 лет [5]. Более того, указанному противоправному явлению в теории права и среди научных исследователей дано, вполне обоснованное на наш взгляд, новое название – «киберэкстремизм» [6, С.89].

В связи с тем, что рассматриваемый вид преступности совершается молодежью, то совершенно обоснованным будет осуществлять профилактику именно среди указанной возрастной категории граждан. Для правильного развития политики профилактики киберэкстремизма, для того, чтобы она была принята положительно и приносила свои результаты, важно знать, как молодое поколение оценивает эффективность тех или иных мер. Представляется, что намного более эффективным способом решения межэтнических, межконфессиональных и подобных проблем будет профилактика данных явлений среди студентов, нежели ликвидация их ужасающих последствий [7,8 и др.].

В основе профилактических мероприятий по предупреждению киберэкстремизма лежит идея контролируемой социализации, когда профессионалы управляют социальными и психологическими процессами, происходящими с молодежью [9].

Для снижения проявлений экстремистских настроений среди молодежи, следует ориентироваться на:

– модернизацию молодежной среды в целом, её улучшение и создание в ней возможностей для формирования положительного настроя у подрастающего поколения и предотвращения проявления в ней насилия и жестокости;

- разработку методов анализа молодежного киберэкстремизмаи способов его разрушения;

- создание на его месте зон конструктивной социальной направленности;

- оказание влияния на социализацию личности, включение его социальное пространство и, как итог, формирование личности, обладающей высокой степенью толерантности, ответственности, успешности, личности, которая ориентирована на ценности гражданственности и патриотизма;

- создание плана психокоррекционных манипуляций, служащих профилактикой ненормативных агрессивных настроений молодежи;

- развитие её способности к социальному взаимодействию, рефлексивным и саморегуляционным методам, формирование толерантного поведения, выхода из культов и организаций деструктивной направленности [10,11,12].

В качестве основного направления профилактики киберэкстремизма следует считать усиление влияния воспитательного воздействия социальных институтов и СМИ на мировосприятие студентов [13,14 и др.].

Следует отметить, что профилактические меры в борьбе с кибнрэкстремизмом делятся на меры первичной и вторичной профилактики. Целью первичной профилактики является – предотвращение притока новых членов в экстремистские группы, например, посредством привития студентам иммунитета к экстремизму; укоренение в сознании молодежи антифашистской идеологии; формирование неприятия насильственных действий; создание негативного образа организаций экстремистской направленности и их глав [15, С.25]. Вторичная профилактика включает в себя работу с участниками формирований экстремистской направленности.

Представляется, что наибольший вес имеет первичная профилактика, предотвращающая рост численности и состава экстремистских групп. Всвязи с высоким уровнем латентности рассматриваемого вида преступности и профессионализма лиц, ее совершающих весьма сложно выделить единое основание для классификации всех существующих и гипотетических мер по профилактике киберэкстремизма. Между тем, анализ различных официальных и научных источников, нам удалось выделить некоторые основания для их классификации. Так, меры профилактики, направленные против экстремистской деятельности условно (поскольку иногда одну и ту же меру можно причислить к разным категориям) следует делить на: организационные, воспитательные, пропагандистские, нормативно-правовые и научно-методические [16, С.115; 17, С. 1134].

К организационным мерам относятся такие как: развитие экстремальных видов спорта с элементами риска; создание и внедрение новых субкультур, являющихся социально-позитивными, выступающих в противовес с субкультурами киберэкстремистской направленности; разработка и реализация комплексных мероприятий, направленных на развитие межнационального диалога; создание в вузах добровольные интернациональные студенческие дружины для поддержания общественного порядка и предупреждения конфликтов на почве этнической неприязни на территории учебных заведений, общежитий и студенческих городков; фильтрация электронного контента; организация персонифицированного доступа к ресурсам сети, которые могут быть потенциально опасными; организация факультативных курсов, посвященных антиэкстремистскому законодательству.

К воспитательным мерам относятся такие как: повышение правовой грамотности студентов; формирование навыков бесконфликтного общения; доведение до сведения учащихся опасности, которую влекут за собой преступления на почве ненависти для общества; формирование политической,

нравственной и правовой культуры личности; формирование навыков толерантности.

К пропагандистским мерам относятся такие как: проведение лекций в рамках учебного процесса, касающихся вопросов экстремизма; создание негативного образа глав экстремистских формирований и принципов их идеологии; обучение поведению в ситуациях проявления экстремизма; информирование в СМИ о результатах деятельности экстремистов в порицательном контексте.

К нормативно-правовым и научно-методическим мерам относятся такие как: разработка и утверждение нормативных документов, поддерживающих формирование почвы для успешной социализации личности; оказание поддержки одаренной молодежи, находящейся в трудных жизненных условиях; осуществление мониторинга учебных программ, преследующего цель выявить материалы, способные привести к разжиганию межнациональной розни; разработка исследовательских методов мониторинга социального самочувствия студентов, исследование отклонений в их поведении, анализ деятельности субкультур; организация и проведения научно-исследовательских конференций, касающихся исследования проблем экстремизма в молодежной среде [6, С.91].

Таким образом, в рамках настоящего исследования нами был проведен криминологический анализ киберэкстремистской преступности, выделены основные понятия и признаки рассматриваемого вида преступности, а также определены некоторые наиболее важные для профилактики характеристики личности киберэкстремистского преступника. Кроме того, все приведенные меры позволят постепенно снизить тенденцию развития молодежного экстремизма и использовать потенциал молодежи в созидательных целях, приведя к согласию интересы общества, государства и учащихся.

Указанное направление развития антиэкстремистской деятельности определено с тем, чтобы она была адекватно воспринята и проносила положительные результаты в борьбе с возникновением экстремизма, и киберэкстремизма в частности. Важно понимать, что предупреждение столь общественно опасной категории преступлений гораздо более действенная мера, чем борьба с ней, при этом следует усилить пропагандистскую деятельность в общеобразовательных учреждениях путем проведения мероприятий, касающихся вопросов киберэкстремизма, создания негативного образа глав экстремистских формирований и принципов их идеологии (данное направление представляется нам наиболее эффективным, поскольку молодежь подсознательно реагирует на формирование массового сознания и охотно, и, чтоне мало важно, быстро переключается на новое направление развития общественной мысли); обучения поведению в ситуациях проявления экстремизма. Следование этим рекомендациям позволит значительно сократить риск формирования экстремистских настроений среди молодежи, как одной из наиболее многочисленных групп субъектов подверженных совершению такого рода преступлений.

Список литературы:

1. Бутенко А.С. Экстремизм в сети интернет: понятие и сущность // Юристъ-Правоведъ. – 2019. - № 2(98). С. 57-61.

2. Шанхайская Конвенция о борьбе с терроризмом, сепаратизмом и экстремизмом от 15.07.2001 г., ратифицированная Российской Федерацией 10 января 2003 г. Статья 1. СПС «КонсультантПлюс».

3. Федеральный закон от 25 июля 2002 г. № 114-ФЗ «О противодействии экстремистской деятельности» СПС «КонсультантПлюс».

4. Стратегия противодействия экстремизму в Российской Федерации до 2025 года: Указ Президента Российской Федерации № 2753 от 28 ноября 2014 г.

5. Кубякин Е. О. Основания социологического обоснования феномена экстремизма.

Экстремперантность. Краснодар, 2014.

6. Желтякова М.В., Чусавитина Г.Н. Меры по предупреждению киберэкстремистской деятельности среди студенческой молодежи // В сборнике : Управленческие механизмы противодействия идеологии экстремизма и терроризма. матер. научн.-практич. Конференции. Под общей ред. Н.Р. Балынской. – 2018. С.89-93.

7. Полякова Н.Н. Киберэкстремизм в молодежной среде как социальная проблема // Политика, экономика и инновации. 2017. №5.

8. Лисина О.В. Проблемы противодействия молодежному киберэкстремизму в условиях интернетсоциализации: вопрос нравственного здоровья подрастающего поколения // Теория и практика общественного развития. 2017. №1.

9. Макашова В.Н., Чусавитина Г.Н. Педагогические механизмы профилактики идеологии киберэкстремизма среди студенческой молодежи // Современные информационные технологии и ИТ-образование. 2015. №11.

10. Бедрик А.В., Зарбалиев В.З. Факторы распространения молодежного экстремизма на Юге России на современном этапе // CaucasianScienceBridge. 2018. №1 (1).

11. Chernova E.V., Bobrova I.I., Movchan I.N., Trofimov E.G., Zerkina N.N., Chus avitina G.N. Teachers training for prevention of pupils deviant behavior in ICT // Proceedings of the 2016 Conference on Information Technologies in Science, Management, Social Sphere and Medicine (ITSMSSM 2016) Сер. «ACSR: Advances in Computer Science Research» Editors: Olga Berestneva, Alexei Tikhomirov, Andrey Trufanov. 2016. С. 294-297.

12. Челышева И.В. Кибербезопасность школьников в интернет-пространстве и проблемы семейного медиаобразования // CredeExperto: транспорт, общество, образование, язык. 2016. №4.

13. Арпентьева М.Р. Проблемы безопасности в интернете: цифровая беспризорность как причина цифровой зависимости и цифровой преступности // Вестник Прикамского социального института. 2017. №3 (78).

14. МОО «ЦСГПЭД» [сайт центра содействия государству в противодействии экстремистской деятельности]. – URL: http://www.csgped.ru/ekstremizm2.html (дата обращения: 24.11.2020).

15. Чусавитина Г.Н., Курзаева Л. В., Давлеткиреева Л. З., Чусавитин М.О. Подготовка будущих учителей к обеспечению информационной безопасности: монография. Магнитогорск: МаГУ, 2013. - 188 с.

16 Руденко О.Ю. Киберэкстремизм в молодежной среде // Практика коммуникативного поведения в социально-гуманитарных исследованиях: материалы международной научнопрактической конференции (Пенза – Сургут – Витебск). – М: Социосфера, 2013. С.114-116.

17 Овчинникова И.В., Курзаева Л.В. Профилактика киберэкстремизма в системе образования: базовые решения на основе компетентностного подхода // Фундаментальные исследования. – М: Академия Естествознания, 2013. – № 10-5. С. 1131-1135.

Воропаев Андрей Евгеньевич
Институт экономики и юриспруденции.
Вологодский государственный университет
г.Вологда

Воропаев А.Е. КИБЕРЭКСТРЕМИЗМ В МОЛОДЕЖНОЙ СРЕДЕ КАК СОЦИАЛЬНАЯ ПРОБЛЕМА

В последнее время общество довольно активно обсуждает проблему киберэкстремизма. Чаще всего при помощи интернета совершаются публичные призывы к осуществлению экстремистской деятельности, так как их размещение в глобальной сети не представляет особых сложностей. Через интернет может происходить возбуждение ненависти либо вражды, а равно унижение человеческого достоинства. А также может быть организовано экстремистское сообщество, например путем сговора и приискания соучастников. Не все знают, что за неосторожные высказывания и репост какой- либо картинки легко можно подвергнуться уголовному наказанию, особенно это относится к нынешней молодежи. Статистика Верховного суда о росте числа дел возбужденных по статьям уголовного кодекса связанных с экстремизмом на данный момент насчитывается десять экстремистских статей в уголовном кодексе. Ещё две в кодексе административных правонарушений.

Преступлений связанных с экстремизмом и терроризмом в киберпространстве становиться все больше с каждым годом, особенно сильный рост по статье 282 Уголовного кодекса Российской Федерации.возбуждение ненависти либо вражды, а равно унижение человеческого достоинства. Материалы которые приравниваются к экстремистской направленности в киберпространстве это могут быть: оскорбительные высказывания против религиозной направленности или национальной группе. Также публичные призывы к свержению власти, даже критику к власти в грубой форме можно расценить как преступления. Материалы размещенные в сети могут толковаться правоохранительными органами и экспертами очень широко. Такого контента ежедневно публикуется бесчисленное множество, не важно когда вы сделали публикацию. Полиция считает что, если публикация экстремистского и террористического характера находится у вас на странице и не была удалена, значит это является длящимся нарушением. Никакие сроки давности здесь не работают. Правоохранительным органам нужны количественные показатели для выявления нарушений. Им нужно отчитаться по борьбе с экстремизмом в цифрах, поэтому в социальных сетях они ведут поиск по ключевым словам и смотрят всех подряд, отыскивая ролики, различные публикации, сообщения, комментарии. На сайте Министерства Юстиции можно ознакомиться с реестрами экстремистских материалов. Сейчас в нем больше четырех тысяч позиций. Также на сайте Министерства юстиции

есть список запрещенных организаций в РФ. Публикации их символики тоже запрещены. Существует целая самостоятельная структура полиции, занимающаяся расследованием и борьбой в сфере экстремизма.

Говоря о проблеме развития киберэкстремизма в молодежной среде, можно сказать, что большинство несовершеннолетних лиц из – за своего не понимания, а также не знания, не давая оценку своим действиям, под влиянием эмоций своего характера могут с легкостью совершить ошибку, которая может повлиять на их жизнь в худшую сторону, тем самым испортив себе будущее. Это обусловлено рядом факторов.

Во-первых, молодые люди и девушки большую часть своего времени проводят в виртуальном мире, а именно: общаются в социальных сетях, «сидят» день и ночь в чатах, смотрят фильмы, видеоролики, качают софт для своего ноутбука или планшета, играют в он-лайн игры и многое другое.

Во-вторых немаловажным фактором является юношеский максимализм. В 15–20 лет молодёжь особенно трепетно относится к проблемам, воспринимает информацию больше эмоционально, нежели рационально. Поэтому чаще всего киберэктремизму подвержены молодые «горячие» головы, желающие изменить всё, всех, и сиюминутно.

В-третьих, любопытства молодым людям не занимать. Всё новое и неизведанное вызывает у них дикое желание попробовать, посмотреть, поучаствовать. Поэтому любое новое течение, навеянное модой, принимается нашей молодёжью на ура, ведь это такая прекрасная возможность выделиться, не быть как все, выразить свою точку зрения, проявить внутренние таланты, вступая в то или иное течение.

Отдельно среди причин развития киберэкстремизма можно отметить высокий потенциал киберпространства для культивирования экстремизма в целом, а учитывая интерес молодежи к всемирной паутине – и молодежного в частности. Эта среда в незначительной степени подвержена цензуре, любой ресурс здесь может быть в любой момент перемещен на новое место, и, кроме того, доступ к ресурсам не ограничен географически. Механизм, препятствующий публичному проявлению экстремизма на страницах общенациональных газет и телеканалов, не срабатывает столь же эффективно в киберпространстве. Это делает интернет благоприятной средой для пропаганды экстремистских идей. Таким образом, в настоящее время киберпространство стало расцениваться экстремистскими идеологами как наиболее привлекательная площадка для ведения идеологической пропаганды и борьбы. Результатом развития киберэкстремизма становится формирование и обострение у молодежи таких качеств, как жестокость, нетерпимость, вспыльчивость. В итоге молодые люди переносят применение насильственных действий из виртуального пространства в «реальную» действительность. Параллельно развитию киберэкстремизма растет преступность среди молодежи. Увлекшись борьбой и «расправой над всеми» в киберпространстве, человек не замечает, как начинает рушить все вокруг себя. Все чаще в СМИ встречаются сообщения о том, как школьник расстрелял (покалечил) своих

одноклассников или группа подростков издевалась над лицом без определенного места жительства и т.п. Таким образом, киберэкстремизм отрицательно влияет на функционирование общества, формируя негативные черты среди молодежи.

Как не нарушить закон? Довольно просто, от уголовного и административного дела человека могут спасти элементарная вежливость и соблюдение простых правил. Первое и пожалуй самое главное это осторожность высказывания. В любых высказываниях которые касаются: национальности, религии, расы нужно придерживаться элементарных норм вежливости. Любой материал который может возбудить не только ненависть но и унизить чье то достоинство, может быть расценен как преступление.

Рост масштабов проблемы, а также ее отрицательное влияние на развитие подрастающего поколения (ресурс национальной безопасности, гарант поступательного развития общества и социальных инноваций) свидетельствует о том, что она требует выработки конкретных решений по ее исправлению. Чтобы устранить проблему, необходимо в первую очередь ликвидировать или ослабить причины ее возникновения. Для решения данной проблемы необходимо:

1) улучшить уровень жизни населения (создать условия, при которых молодые люди могли бы быть уверенны в завтрашнем дне);
2) развивать доступную культурно-досуговую среду;
3) отслеживать и устранять информацию экстремистского характера;
4) ввести цензуру компьютерных игр;

5) повышать информированность молодых людей о данной проблеме, научить их противостоять ей.

Также я считаю, что эффективным способом ослабления и причин возникновения экстремизма в киберпространстве будет являться информирование (например видео-фрагмент, презентация) в дошкольном – школьном возрасте. Надеясь, на то что у будущего поколения, придет осознание того, как правильно вести себя в разных ситуациях в интернете, чтобы молодежь осознала понятие экстремизма и терроризма в киберпространстве. Данным информированием, молодежь будет уверенно, комфортно чувствовать себя в просторах интернета. Подобные явления распространяются именно среди старших школьников, накладываясь на подростковый максимализм и психологические особенности развивающейся личности. И в обязательном порядке необходимо проводить разъяснительную работу среди молодежи, привлекать их к выполнению различных проектов и решению задач, помогающих развить критическое мышление, просвещающих и в дальнейшем не позволяющих бездумно пополнять ряды киберэкстремистов

Таким образом экстремизм и терроризм в киберпространстве в молодежной среде играет существенную роль, где наша молодежь может незначительными действиями в интернете совершить преступление, даже не зная, что за это можно нести ответственность. Решение этой проблемы могут

поспособствовать правила, с помощью которых молодежь сможет защитить себя от угрозы быть подвергнутым наказанию по уголовному законодательству.

Томчук В.Д., помощник ректора по внеучебной работе
ФГБОУ ВО Алтайский ГАУ, г.Барнаул
Белокуренко Н.С., заместитель декана экономического факультета
ФГБОУ ВО Алтайский ГАУ, г.Барнаул
Вастьянова М.В., студентка
Экономический факультет, ФГБОУ ВО Алтайский ГАУ, г.Барнаул

Томчук В.Д., Белокуренко Н.С., Вастьянова М.В. ПОНЯТИЕ «ЭКСТРЕМИЗМ» И ЕГО ПРОФИЛАКТИКА В ВУЗЕ

В настоящее время экстремизм представляет большую опасность для государства и ее граждан, как одно из самых распространенных и жестоких преступлений в мире, несет реальную угрозу всему человечеству в целом. Негативные последствия экстремизма испытывают на себя практически все страны мира, включая и Россию.

В разных странах и в разные времена было дано много разных юридических и научных определений понятию «экстремизм» (табл.1). В настоящее время единого определения не существует.Экстремизм – это сложное явление (рис.1). В узком смысле экстремизм или экстремистская деятельность это - незаконная деятельность, направленная на насильственное изменение государственного строя и на разжигание национальной розни. В абстрактном смысле экстремизм - это приверженность к крайним мерам, действиям, взглядам и решениям, которые противоречат закону.

Таблица 1 – Определения понятия «экстремизм»

Автор (источник)	Дефиниция
Ожегов С.И. Толковый словарь русского языка [1]	Экстремизм – это приверженность к крайним взглядам, к использованию крайних мер (включая теракты и взятие заложников) для достижения своих целей
Большая советская энциклопедия [2]	Экстремизм – приверженность крайним взглядам, идеям и мерам, направленным на достижение своих целей радикально ориентированными социальными институтами, малыми группами и индивидами
Трофимов-Трофимов В.Д., со-координатор Международного движения по	Экстремизм – это идеология допустимости использования крайних мер, экстремумов социального поведения, для получения желаемого эффекта

защите прав народов [3]	
Лерой М., французский юрист [4]	Основным отличием экстремистских политических течений назвал требование от своих приверженцев абсолютной веры в исповедуемые политические идеалы
«Шанхайская конвенция о борьбе с терроризмом, сепаратизмом и экстремизмом» от 15 июня 2001 г. (в январе 2003 года подписана Россией) [4]	Экстремизм — какое-либо деяние, направленное на насильственный захват власти или насильственное удержание власти, а также на насильственное изменение конституционного строя государства, а равно насильственное посягательство на общественную безопасность, в том числе организация в вышеуказанных целях незаконных вооруженных формирований или участие в них, и преследуемые в уголовном порядке в соответствии с национальным законодательством сторон

Современное российское законодательство объединяет под одним термином экстремизм все виды экстремизма: политический, этнический, религиозный и другие.

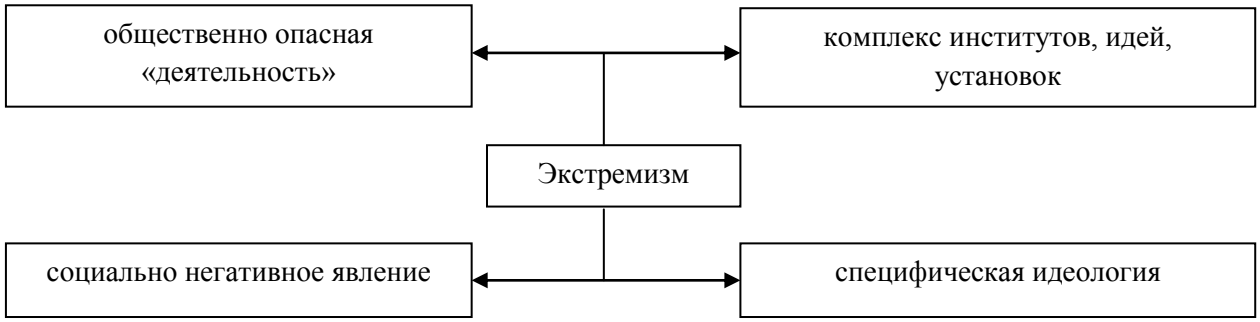

Рис. 1 – Группы определений понятия «экстремизм»

Согласно Федерального закона от 25 июля 2002 г. № 114-ФЗ «О противодействии экстремистской деятельности» (с изменениями и дополнениями) экстремистская деятельность (экстремизм) [5]:

- насильственное изменение основ конституционного строя и нарушение целостности Российской Федерации;
- публичное оправдание терроризма и иная террористическая деятельность;
- возбуждение социальной, расовой, национальной или религиозной розни;

- пропаганда исключительности, превосходства либо неполноценности человека по признаку его социальной, расовой, национальной, религиозной или языковой принадлежности или отношения к религии;
- нарушение прав, свобод и законных интересов человека и гражданина в зависимости от его социальной, расовой, национальной, религиозной или языковой принадлежности или отношения к религии;
- воспрепятствование осуществлению гражданами их избирательных прав и права на участие в референдуме или нарушение тайны голосования, соединенные с насилием либо угрозой его применения;
- воспрепятствование законной деятельности государственных органов, органов местного самоуправления, избирательных комиссий, общественных и религиозных объединений или иных организаций, соединенное с насилием либо угрозой его применения;
- совершение преступлений по мотивам, указанным в п. «е» ч.1 ст. 63 Уголовного кодекса Российской Федерации;
- пропаганда и публичное демонстрирование нацистской атрибутики или символики либо атрибутики или символики, сходных с нацистской атрибутикой или символикой до степени смешения, либо публичное демонстрирование атрибутики или символики экстремистских организаций;
- публичные призывы к осуществлению указанных деяний либо массовое распространение заведомо экстремистских материалов, а равно их изготовление или хранение в целях массового распространения;
- публичное заведомо ложное обвинение лица, замещающего государственную должность Российской Федерации или государственную должность субъекта Российской Федерации, в совершении им в период исполнения своих должностных обязанностей деяний, указанных в настоящей статье и являющихся преступлением;
- организация и подготовка указанных деяний, а также подстрекательство к их осуществлению;
- финансирование указанных деяний либо иное содействие в их организации, подготовке и осуществлении, в том числе путем предоставления учебной, полиграфической и материально-технической базы, телефонной и иных видов связи или оказания информационных услуг.

Коршунова О.К. рассматривая перечень экстремистских действий, приведенных в законе, подразделяет их на три группы [6]:

1. Физические действия: насильственное изменение основ конституционного строя и нарушение целостности России подрыв ее безопасности захват или присвоение властных полномочий создание незаконных вооруженных формирований осуществление террористической деятельности и т. д.
2. Действия, направленные на распространение в обществе экстремистских идей и мыслей

~~3.~~ Финансирование экстремистской деятельности и иное содействие для ее осуществления т. д.

Впервые понятие «экстремизм» появилось в Англии, еще в середине XIX века в политической прессе. После Англии экстремизм стал распространяться в США, когда бескомпромиссных представителей враждующих сторон Юга и Севера во время Гражданской войны (1861 - 1865 гг.) называли «экстремистами обеих частей страны». Понятие «экстремизм» во Франции вошло в оборот во время Первой мировой войны (1914 - 1918 гг.) [7]. Экстремизм в России появился и начал развиваться в начале XIX века.

Российская Федерация при обеспечении национальной безопасности в сфере государственной и общественной безопасности на долгосрочную перспективу исходит из необходимости постоянного совершенствования правоохранительных мер по выявлению, предупреждению, пресечению, и раскрытию экстремизма.

Одним из инструментов достижения этих целей, является правовая система. В настоящее время в Российской Федерации противодействие экстремизму регулируется большим количеством нормативных источников как на федеральном, так и региональном, а также муниципиальном уровнях.

Основополагающим нормативно-правым актом на федеральном уровне является ФЗ «О противодействии экстремистской деятельности», который неоднократно подвергался изменениям [5].

В целях противодействия экстремистской деятельности федеральные органы государственной власти, органы государственной власти субъектов Российской Федерации, органы местного самоуправления в пределах своей компетенции в приоритетном порядке осуществляют профилактические, в том числе воспитательные, пропагандистские, меры, направленные на предупреждение экстремистской деятельности.

Указом Президента Российской Федерации от 12 05 2009 № 537 утверждена «Стратегия национальной безопасности Российской Федерации до 2020 года» согласно которой основными источниками угроз национальной безопасности в сфере государственной и общественной безопасности являются, в том числе деятельность террористически организаций группировок и отдельны лиц направленная на насильственное изменение основ Конституционного строя РФ уничтожение военных и промышленных объектов, предприятий и учреждений, обеспечивающих жизнедеятельность общества устрашение населения в том числе путем применения ядерного и химического оружия либо опасных радиоактивных, химических веществ; экстремистская деятельность националистических, религиозных, этнических и иных организаций и структур направленная на разрушение единства и территориальной целостности Российской Федерации дестабилизацию внутриполитической и социальной ситуации в стране.

В Уголовном кодексе РФ включены статьи, предусматривающие ответственность за экстремистские действия [8].

На региональном уровне разрабатываются различные мероприятия по противодействию экстремизму. К полномочиям органов государственной власти субъекта Российской Федерации относится решение вопросов организации и осуществления на территории субъекта РФ мероприятий по предупреждению терроризма и экстремизма, минимизации их последствий.

На территории Алтайского края действует государственная программа «Противодействие экстремизму и идеологии терроризма в Алтайском крае», цель которой является организация эффективной системы мер антиэкстремистской направленности для предупреждения угроз экстремистских проявлений на территории края, в том числе распространения идеологии терроризма.

Основные задачи программы [9]:

- повышение уровня межведомственного взаимодействия по противодействию экстремизму и идеологии терроризма, достижение личной ответственности руководителей органов исполнительной власти Алтайского края, органов местного самоуправления за качество организации работы по противодействию экстремизму, идеологии терроризма, профилактике межнациональной конфликтности;
- совершенствование региональной политики в области профилактики распространения межнациональной конфликтности, экстремизма и идеологии терроризма с участием институтов гражданского общества;
- профилактика распространения идеологии экстремизма и терроризма в процессе социальной и культурной адаптации мигрантов;
- методическое обеспечение и укрепление материально-технической базы субъектов, реализующих мероприятия в области противодействия экстремизму и идеологии терроризма;
- вовлечение молодежи в реализацию системы мер по профилактике экстремизма и его крайней формы - терроризма, а также формирование нетерпимости к экстремистской и террористической идеологии.

В ФГБОУ ВО Алтайский ГАУ проводятся мероприятия по профилактике экстремизма. В частности, Советом по внеучебной работе организуются и проводятся встречи-лекции со студентами специалистами силовых структур края - ГУ МВД России по Алтайскому краю и Управления ФСБ России по Алтайскому краю.

Ежегодно проводятся лекции, круглые столы по профилактике экстремизма и терроризма совместно с ФГБОУ ВО Алтайский ГПУ. Программа данных мероприятий насыщена – и лекция, и дискуссия, и игра, и видеоматериалы.

В структурных подразделениях ВУЗа (библиотека, факультеты) проводятся тематические мероприятия, приуроченные Дню солидарности в борьбе с терроризмом – 3 сентября.

Помимо политического и религиозного экстремизма, существует этнический экстремизм. В этой связи ежегодно на экономическом факультете

ФГБОУ ВО Алтайский ГАУ проводится Фестиваль национальных культур. Цель фестиваля: повышение интереса студентов к истории народов, страны; воспитание ответственного отношения к окружающим; воспитание в студентах чувства гражданского долга, единения, национальной толерантности; активизация творческой инициативы. В программе фестиваля обозначены номинации: «Национальные традиции», «Национальный фольклор», «Национальный костюм», «Национальная кухня».

Студенты рассказывают зрителям о национальных традициях и обычаях русских, китайцев, греков, таджиков, алтайцев, немцев, армян и др. Презентации сопровождаются демонстрацией национальных костюмов, представлением национального фольклора (музыка, танцы, игры). В фестивале принимают участие студенты не только экономического факультета, но и агрономического, инженерного.

Мероприятие приурочено к двум датам ноября – Дню народного единства (4 ноября) и Международному дню толерантности (16 ноября).

В нашем университете обучаются студенты разных национальностей и вероисповеданий, и это многообразие является ценным даром. Каждый должен стремиться поддерживать принципы терпимости, взаимного уважения и мирного сосуществования. Проведение подобных мероприятий способствуют созданию атмосферы дружбы, взаимопониманию, взаимоуважению.

Таким образом, противодействие экстремистской деятельности основывается на следующих принципах:

-признание, соблюдение и защита прав и свобод человека и гражданина;

-законность;

-гласность;

- приоритет обеспечения безопасности Российской Федерации;

-приоритет мер, направленных на предупреждение экстремистской деятельности;

-сотрудничество государства с общественными и религиозными объединениями, иными организациями, гражданами в противодействии экстремистской деятельности;

-неотвратимость наказания за осуществление экстремистской деятельности.

Противодействие экстремистской деятельности осуществляется по следующим основным направлениям:

-принятие профилактических мер, направленных на предупреждение экстремистской деятельности, в том числе на выявление и последующее устранение причин и условий, способствующих осуществлению экстремистской деятельности;

-выявление, предупреждение и пресечение экстремистской деятельности общественных и религиозных объединений, иных организаций, физических лиц.

В заключение, следует отметить, что в ВУЗе на кураторских часах студентам доводится мысль о том, что в трудную минуту они не одиноки и всегда могут обратиться за помощью к педагогам.

Список литературы:

1. Толковый словарь Ожегова онлайн [Электронный ресурс] / Режим доступа: https://slovarozhegova.ru/
2. Большая советская энциклопедия онлайн [Электронный ресурс] / Режим доступа: https://bse.slovaronline.com/
3. Трофимов-Трофимов В.Д. Экстремизм. Трофосфера – автономный интернет-блог. [Электронный ресурс] / Режим доступа: http://ttrofimov.ru/2011/07/ ekstremizm
4. Гриценко Г.Д., Лукьянцев Е.В. К вопросу о понимании экстремизма в современной науке [Электронный ресурс] / Режим доступа: https://cyberleninka.ru/article/n/k-voprosu-o-ponimanii-ekstremizma-v-sovremennoy-nauke/
5. Федеральный закон от 25 июля 2002 г. № 114-ФЗ «О противодействии экстремистской деятельности» (с изменениями и дополнениями) [Электронный ресурс] / Режим доступа: https://base.garant.ru/
6. Коршунова О.Н. Преступления экстремистского характера: теория и практика противодействия. - СПб.: «Юридический центр Пресс», 2006.
7. Погорельцев В.И. Зарождение и развитие экстремизма в мире и в России [Электронный ресурс] / Режим доступа: https://cyberleninka.ru/article/n/zarozhdenie-i-razvitie-ekstremizma-v-mire-i-v-rossii/
8. Уголовный кодекс РФ от 13.06.1996 N 63-ФЗ (ред. от 27.10.2020) [Электронный ресурс] / Режим доступа: http://www.consultant.ru/
9. Постановление Правительства Алтайского края «Об утверждении государственной программы Алтайского края «Противодействие экстремизму и идеологии терроризма в Алтайском крае» от 31.12.2019 №546 [Электронный ресурс] / Режим доступа: https://www.altairegion22.ru/upload/iblock/5f9/-546-_PP_-31.12.2019.pdf

Мгдесян Светлана Славиковна
Психология управления, Алтайский филиал Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации, г. Барнаул

Мгдесян С.С. ПСИХОЛОГИЯ ЭКСТРЕМИЗМА И ТЕРРОРИЗМА В КИБЕРПРОСТРАНСТВЕ

Интернет, в силу своей специфики, людям «развязал языки». Общество чувствует безнаказанность и недосягаемость, совершая правонарушения в глобальной сети. Еще в 90-х годах появились деликты, связанные с распространением и функционированием сетевых сообществ террористической и экстремистской деятельности.

«Всемирная паутина» расширяется с каждой минутой, а цифровая реальность стремительно меняет мир. Каждый день создаются тысячи новых сайтов. Информация на них превращается не только в важнейший фактор производства, но и в средство манипулирования людьми. Знания, которые нужны людям для производства благ, в руках экстремистов и террористов превращаются в орудие преступления. В современном мире перед нами остро встали вопросы решения совокупности проблем человечества, от которых зависит дальнейшее существование цивилизации.

Любая социальная проблема требует ее немедленного целенаправленного разрешения или управления. Но проблема киберэкстремизма и кибертерроризма заключается в том, что их трудно держать под контролем, они очень быстро отыскивают единомышленников.

Прежде чем дать развернутое определение киберэкстремизму и кибертерроризму, необходимо обратить внимание на киберпространство.

Существование киберпространства доказывает, что двадцать первый век – век глобальной революции в индустрии информационных технологий.

Термин «киберпространство» ввел в 1984 г. У. Гибсон, американо-канадский писатель-фантаст, основатель стиля киберпанк. В первом романе «Нейромант», открывающем трилогию «Киберпространство», Гибсон описал киберпространство как «консенсуальную галлюцинацию», в которой виртуальный мир стал заменой реального, существующего только в умах пользователей компьютеров [1].

Киберпространство – это цифровая конструкция, в которой подключенные к сети компьютеры или мобильные устройства коммуницируют. В этой плоскости одновременно существует два вида объединений: положительное (взаимодействие ради производства общественных благ), негативное (агрессия,

вызванная несовместимостью интересов людей). К негативной кооперации относится кибертерроризм.

Термин «кибертерроризм» ввел в середине 1980 г.г. Б. Коллин, старший научный сотрудник американского Института безопасности и разведки. Определив его как «использование высоких технологий для того, чтобы парализовать работу важнейших национальных инфраструктур, запугать правительства или гражданское население» [4].

Под кибертерроризмом следует понимать явление, связанное с действиями лица или группы лиц, направленными на устрашение людей, оказание давления на правительства, причинение вреда посредством информационных технологий. Основным объектом данного преступления является общественная безопасность (то есть состояние защищенности жизненно важных интересов общества) и нормальное функционирование органов власти.

Значит, кибертерроризм – это терроризм в киберпространстве.

В современном обществе самой тяжелой общественно - политической задачей социума является - киберэкстремизм. Существует большое количество различных течений экстремистской деятельности. Можно выделить следующие формы экстремизма:

- политические;
- экономические;
- религиозные;
- экологические;
- информационные и др.

Политический экстремизм – это приверженность к крайним взглядам и действиям в политике. Он выступает против сложившихся общественно-политических структур, пытается подорвать их стабильность, свергнуть ради достижения своих целей силовыми методами. В свою очередь, политический экстремизм подразделяется на «правый» и «левый».

Экономический экстремизм направлен на достижение частных целей и дестабилизацию социально-экономических основ общества. Он сконцентрирован на подрыв многообразия и учреждение какой-либо одной формы собственности, единых методов хозяйствования, ликвидацию разнообразия форм собственности путем криминальных насильственных действий, оказание давления.

Основная цель религиозного экстремизма – признание своей религии ведущей и подавление других религиозных конфессий через их принуждение к своей системе веры. Проявляется в нетерпимости к представителям других конфессий или течений в рамках одной и той же конфессии.

Экстремисты экологического течения борются не только за воплощение в жизнь действенной природоохранной политики, но и против научно-технического прогресса.

Информационный экстремизм — это деятельность, связанная с использованием информации, оказывающей деструктивное воздействие на

психику людей. Необходимо подчеркнуть, что в чистом виде ни одной из форм экстремизма не существует.

Киберэкстремизм - это новая форма экстремизма, использующая для достижения своих целей компьютеры и электронные сети, новейшие коммуникационные технологии.

Существует три роли, которые исполняют террористы в террористических группах: лидер, авантюристы и идеалисты.

Лидер изначально переживает чувство собственной неадекватности и легко проецирует его на общество, думая, что общество неадекватно и должно быть изменено. Такие личности имеют ясное представление о целях террористической группы и о корнях ее идеологии. Роль лидера привлекательна для личностей нарциссического и параноидного типов.

Авантюрист обычно имеет все необходимые навыки для участия в террористической группе. Это антисоциальный тип личности, часто имеющий историю криминального поведения до вхождения в группу. Идеология в их поведении может существенно варьироваться или вообще отсутствовать. Поиск сильных ощущений в актах агрессии привлекает их больше всего.

Идеалистом является, как правило, подросток, который является благоприятной основой для воспитания крайних взглядов и который всегда неудовлетворен состоянием его общества или организации. Он является идеальным объектом для «промывания мозгов», так как юношеский возраст - сложный процесс перехода от детских забот к суровой взрослой жизни, в которой соединились разноречивые стремления. Для такого острого процесса характерны деструктивное девиантное поведение (социальная патология), негармоничность в развитии индивидуальности подростка. Подросток, готов к более активному социальному положению, он отстаивает свой новый статус, разрушая прежние связи, установившиеся ещё в период его детства [2].

Молодежь участвует в террористических актах, чаще всего, из-за наличия искаженных психологических потребностей (или дефектов личности), а не потому, что стремится к достижению улучшений или кардинальных изменений в политической и социальной сфере.

Нужно формировать процесс обеспечения информативной защищенности, а также увеличивать информированность подростков и родителей в этой сфере. Это можно сделать через социально-психологических тренинги и курсы. Очень важно подготовить и ввести в образовательный процесс систему программ, направленных на профилактику киберэкстремизма и кибертерроризма, усиление установок толерантного поведения среди молодежи.

Следует уделить внимание проведению социально-психологических тренингов и создания новых цифровых технологий обнаружения и предотвращения сетевых атак и их последствий.

Стремительный процесс глобализации поставил перед человечеством ряд сложных проблем. С учетом специфики их происхождения, подобные проблемы следует характеризовать как глобальные. Угрозы национальной безопасности в лице терроризма и экстремизма существовали всегда. Однако, с

развитием информационных технологий и возникновения Интернета, распространение которой вышло за пределы национальных границ, терроризм и экстремизм автоматически обрели инструментарий, который доступен любому пользователю сети.

Ни одно государство на сегодняшний день не может противостоять этой проблеме самостоятельно, только совместными усилиями стран, направив все свои силы на борьбу с кибертерроризмом и киберэкстремизмом, можно решить глобальную проблему на мировом уровне.

Список литературы:

1) Касьянов, В. В. Социология Интернета : учебник для вузов / В. В. Касьянов, В. Н. Нечипуренко. — Москва : Издательство Юрайт, 2020. — 424 с. — (Высшее образование). — ISBN 978-5-534-04944-2. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: http://biblio-online.ru/bcode/453914 (дата обращения: 20.11.2020).

2) Клейберг, Ю. А. Психология девиантного поведения : учебник и практикум для вузов / Ю. А. Клейберг. — 5-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2020. — 290 с. — (Высшее образование). — ISBN 978-5-534-00231-7. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: http://biblio-online.ru/bcode/449825 (дата обращения: 21.11.2020).

3) Психология и психопатология терроризма. Гуманитарные стратегии антитеррора : монография / М. М. Решетников [и др.] ; под редакцией М. М. Решетникова. — 2-е изд. — Москва : Издательство Юрайт, 2020. — 257 с. — (Актуальные монографии). — ISBN 978-5-534-10808-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: http://biblio-online.ru/bcode/454675 (дата обращения: 21.11.2020).

4) Степанов, О. А. Противодействие кибертерроризму в цифровую эпоху : монография / О. А. Степанов. — Москва : Издательство Юрайт, 2020. — 103 с. — (Актуальные монографии). — ISBN 978-5-534-12775-1. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: http://biblio-online.ru/bcode/448300 (дата обращения: 20.11.2020).

Мальцева Валерия Александровна
Юридический факультет;
Алтайский Филиал Российской Академии Народного Хозяйства и Государственной Службы при Президенте Российской Федерации
г. Барнаул

Мальцева В.А. ДОВЕДЕНИЕ ДО САМОУБИЙСТВА ПОСРЕДСТВОМ ИСПОЛЬЗОВАНИЯ ИНТЕРНЕТ-ТЕХНОЛОГИЙ

Глобальная информатизация и развитие компьютерной сети Интернет приводит к тому, что современное общество всё больше погружается в информационное пространство, что становится повседневной практикой. Совершенствование киберпространства приводит квсё большей его уязвимости. В Связи с этим контроль становится всё сложнее, а воздействие информатизации на общество становится всё больше и больше.

С новой проблемой борьбы с экстремизмом и терроризмом современное общество столкнулось в условиях локдауна и пандемией связанной с распространением новой короновирусной инфекцией, так как все рабочие и обучающие процессы перешли в режим онлайн. И большее количество времени подростки стали проводить в интернете. Проблема, связанная с приобщением подростков к работе в режиме онлайн заключается в том, что подростки находятся в возрасте открытом для внешнего воздействия. Они становятся легко восприимчивы к кибербуллингу, что впоследствии может привести к кибербуллициду. Поэтому одной из важных задачей является борьба с киберманипуляцией, приводящей к суициду подростков посредством интернет-технологий

По официальным данным количество самоубийств *с* начала 2020 года в России составляет около 2000 человек, из которых более трети — дети и подростки.Последнее время увеличивается рост подросткового суицида из-за закрытых «групп смерти» в социальных сетях. На них приходится *1% от общего числа смерте*й. Но с каждым годом это число увеличивается из-за стремительного развития технологий и все большего продвижения интернета в нашу жизнь.

Для криминологической науки, несомненно, представляют интерес те случаи самоубийств, в которых желание уйти из жизни было сформировано извне, путем умышленного создания другими лицами ситуаций, провоцирующих на совершение суицида. С развитием интернет-технологий появились и новые способы психического воздействия на потерпевших, такие,

например, как кибербуллинг и его крайняя форма — кибербуллицид, определяемый как «суицид, произошедший вследствие столкновения с прямой или косвенной агрессией онлайн» Их возникновению поспособствовала более высокая анонимность, которая так же исключает необходимость в территориальной близости. Еще одно специфическое явление, о котором говорилось ранее, создание групп деятельность которых направлена на доведение до самоубийства других пользователей посредством оказания психического воздействия на них в социальных сетях.

Пропагандируется идеология обесценивания жизни, её бессмысленности. Умаление таких ценностей, как любовь, дружба, семья, которые в период формирования подростка становятся болевыми точками, что и приводит легкой манипулируемости.

Подростковый возраст считается самым внушаемым, что позволяет модераторам этих групп внушать ненужность их жизни и воздействовать на них путём угроз.
« Группы смерти» распространяется в социальных сетях и преподносится как игра, которая связана с физическим повреждением или психологическим стрессом (нанесение ран на руках и просмотр фильмов ужасов, а также роликов суицидального направления).

После распространения «суицидальных групп» был принят ряд мероприятий, направленный на снижение активности данных сообществ в социальных сетях

В рамках нормативно правового регулирования была принята новая редакция УК.РФ. Законом изменена ст. 110 УК РФ, введены новые составы преступлений. Статья 110 УК РФ дополнена частью 2. Также уголовный кодекс дополнен статьями 110.1 и 110.2, содержащими описание новых способов противоправной активности: 1) склонение к совершению самоубийства путем уговоров, предложений, подкупа, обмана или иным способом при отсутствии признаков доведения до самоубийства; 2) содействие совершению самоубийства советами, указаниями, предоставлением информации, средств или орудий совершения самоубийства либо устранением препятствий к его совершению, а также обещанием скрыть средства или орудия совершения самоубийства; 3) организация деятельности, направленной на побуждение к совершению самоубийства путем распространения информации о способах совершения самоубийства или призывов к совершению самоубийства. Часть 1 ст. 110.2 содержит основной состав преступления, а ч. 2 ст. 110.2 устанавливает ответственность за то же деяние, связанное с публичным выступлением, использованием публично демонстрирующегося произведения, средств массовой информации или информационно-телекоммуникационных сетей (включая сеть "Интернет")

Данные изменение позволили снизить количество подросткового суицида, связанного с активностью групп смерти в социальных сетях. Но в период пандемии, связанной с распространением новой короновирусной инфекции, увеличивается вероятность завлечения подростков в эти группы.

Больший круг несовершеннолетних благодаря дистанционному обучению получили неподконтрольный доступ к интернет-пространству, получили дополнительное время, что формирует новые угрозы. В нашем случае это может поспособствовать увеличению интереса к группам и увеличению активности таких групп. В связи с этим нужно предотвратить благоприятные условия для возможного распространения суицидальных групп и уменьшению интереса у подростков к ним.

Так, как основной причиной увеличение интереса к суицидным группам служит увеличение свободного времени подростков, одним из возможных способов решения проблемы может стать увеличение занятости подростков. Этого можно добиться путём привлечения их к занятию творческой спортивной и любого другого рода деятельности. Но в связи с карантином, введённым из-за распространения COVID-19, работа социальных учреждений, досуговых клубов, организаций отдыха и оздоровления, частично или полностью приостановлена. Поэтому особый упор нужно сделать на снижение вероятности закрытия таких организаций. Подросток, погруженный в приятную для него среду и занимающийся любимым для себя делом, будет меньше обладаем негативом и обидам. Это позволит сократить количество времени проведённого подростком в интернете, что позволит приостановить процесс приобщения к группам подобного рода.

Но для того, чтобы предотвратить закрытие таких организаций нужно, в условиях диктуемых пандемией, грамотно организовать учебные процесс, которые бы снижали риск распространения новой короновируной инфекции.

Из всего выше сказанного можно сделать вывод о том, что в условиях локдауна и пандемией связанной с распространением новой короновирусной инфекцией, идёт вынужденное массовое приобщение к информационному пространству. Особое внимание нужно уделять подросткам и их неконтролируемой активности в интернете, которая в силу их открытости к внешнему воздействию становятся уязвимыми и легко манипулируемы, что вследствие может привести к активности в «Группах смерти». Чтобы это предотвратить, нужно создавать максимально безопасные условия для работы дополнительного образования, которое позволяет занимать большую часть свободного времени подростков, что снижает вероятность приобщения их к суицидальным группам.

Список литературы:

1. "Уголовный кодекс Российской Федерации" от 13.06.1996 N 63-ФЗ (ред. от 27.10.2020) // СПС КонсультантПлюс

Касимова Валерия Анатольевна
Юридический факультет
Алтайской академии народного хозяйства и государственной службы при
Президенте Российской Федерации
г. Барнаул

Касимова В.А. ПРОБЛЕМЫ ПРЕДУПРЕЖДЕНИЯ ЭКСТРЕМИСТСКИХ И ТЕРРОРИСТИЧЕСКИХ НАСТРОЕНИЙ В МОЛОДЕЖНОЙ СРЕДЕ

В настоящее время экстремистская и террористическая деятельность является наиболее острой проблемой. Прежде всего это вызвано разрастанием экстремистских организаций и террористических группировок по всему миру, включая и Российское государство. На данный момент Российское законодательство активно исследует проблему, пытаясь найти пути предотвращения террористических актов и экстремистских движений.

Согласно статье 1 Федерального закона «О противодействии экстремистской деятельности», экстремистская деятельность (экстремизм) характеризуется как насильственное изменение основ конституционного строя и (или) нарушение территориальной целостности Российской Федерации (в том числе отчуждение части территории Российской Федерации), за исключением делимитации, демаркации, редемаркации Государственной границы Российской Федерации с сопредельными государствами. Также экстремизм можно трактовать как публичное оправдание терроризма и иной террористической деятельности; возбуждение социальной, расовой, национальной или религиозной розни и др.

На сегодняшний день, по исследованиям И.В. Иванова-Петрова, основными участниками экстремистских и террористических группировок являются молодые люди младше 30 лет. Именно молодежь, являющаяся наиболее активной частью населения, ввиду своей неопытности в жизни и правовой неграмотности, поддается влиянию более опытных людей и групп, пропагандирующих идеи о вечной свободе слова и мысли, тем самым вовлекая их в различные незаконные организации. Из-за этого темпы распространения экстремистских и террористических настроений среди молодежи бьют все рекорды. По данным МВД России с января по июнь 2020 года в РФзарегистрировано 1 183 преступления террористического характера (на 21,7% больше, чем за аналогичный период 2019 года) и 442 преступления

экстремистской направленности (больше на 40,8%), - отмечается в материалах министерства. Стремительный рост экстремистского настроение обусловлен свойственному для молодежи деструктивному поведению, заключающемся в противопоставлении отдельного индивида обществу. Лиц, обладающих таким поведением, намного легче вовлечь в незаконную деятельность по нескольким причинам. Во-первых, у таких людей чаще всего отсутствует жизненный опыт, позволяющий понять, что данный вид действий незаконен и опасен. Во-вторых, из-за малолетнего возраста и детской наивности, они верят во все, что им говорят, а, следовательно, и в то, что могут им сказать в экстремистских организациях. Наиболее опасными для них являются каналы распространения экстремистских и террористических идей. К числу таких каналов можно отнести социальные сети в информационно-телекоммуникабельной сети Интернет. Зачастую вовлечение в данную деятельность происходит путем размещения материалов на страницах социальных сетей, к примеру, такая социальная сеть, как «Вконтакте». Нередко в данной социальной сети можно найти группы или сообщества, как открытого, так и закрытого плана, с названиями запрещенных экстремистских организаций. Одной из популярных (около 200 тыс. участников) социальных групп среди несовершеннолетних является криминальное движение «АУЕ» («Арестантский уклад един» или «Арестантское уголовное единство»).

«АУЕ» – это название или девиз существующей криминальной субкультуры и российского неформального объединения банд, состоящих из несовершеннолетних людей. Это молодёжное сообщество пропагандирует воровские и тюремные понятия российской криминальной среды, требуя от ребят соблюдения «воровского кодекса» и сбор денег в так называемый «общак», а взамен обещают хорошую жизнь и поддержку как в настоящем, так и в будущем.

Члены «АУЕ» обычно устанавливают свои порядки в учебных заведениях – вымогательствами и различными угрозами, они собирают деньги с детей в «общак», а отказывающихся наказывают. Также, существует Кодекс «АУЕ», который запрещает любое взаимодействие и помощь властным структурам, включая полицию. В любом районе действия данное сообщество пытается вербовать детей и собирать с них «налог», строить параллельную иерархию власти и порядка на основе понятий взрослых криминальных структур.

В социальной сети «Вконтакте» тематика данного экстремистского сообщества направлена на одурманивание воровской романтики, на пропаганду криминального образа жизни и уголовного мировоззрения. На сегодняшний день экстремистское сообщество «АУЕ» относят к числу опаснейших организаций для молодёжи. Это вызвано тем, что лица, связанные каким-то образом с криминалом, или лица, отбывающие срок в местах лишения свободы, настраивают ни в чем не повинных несовершеннолетних детей на совершения противозаконных действий. Так как уголовная ответственность наступает с 14 лет (в особых случаях, предусмотренных уголовным кодексом РФ), то члены сообщества «АУЕ» стараются использовать детей от 7 лет в своих корыстных

целях. Например, они могут заставить их украсть продукты питания, средства личной гигиены, одежду и т.п. Это порождает в них уверенность в том, что раз их не наказывают за совершенные проступки, значит им можно следовать «воровским правилам», установленными в данной экстремистской организации.

На самом деле это большая проблема, требующая скорейшего решения. В связи с этим можно предложить ряд мер, с помощью которых можно предотвратить вовлечения подрастающего поколения втакого рода экстремистские организации. Для начала необходимо ограничить доступ к социальным группам лицам, младше 16 лет, так как до этого возраста ребенок уязвим и легко поддается вербовке. Если такой возможности нет, то можно предложить профилактические меры борьбы. К примеру, можно создать организацию, которая даст возможность как мальчикам, так и девочкам из разных слоев населения принимать участия в волонтерских отрядах, помогать полиции и спасателям. Также, можно создать такие организации, в которых дети смогут реализовать себя в том, что позитивно влияет как на общество, так и на самих детей, и членство в которых будет считаться престижным.

Список литературы:

1. Федеральный закон "О противодействии экстремистской деятельности" от 25.07.2002 N 114-ФЗ // СПС КонсультантПлюс

2. Профилактика экстремизма в молодежной среде : учебное пособие для вузов / А. В. Мартыненко [и др.] ; под общей редакцией А. В. Мартыненко. — Москва : Издательство Юрайт, 2020. — 221 с. — (Высшее образование). — ISBN 978-5-534-04849-0. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/454111 (дата обращения: 25.11.2020).

Попова Елена Викторовна,
Барнаульский юридический
институт МВД России,
г. Барнаул

Попова Е.В. МУЗЫКА КАК КАТАЛИЗАТОР МИТИНГА

На сегодняшний день возможно встретить использование музыкальных композиций во время проведения акций и митингов.

Речь идёт не о фоновом сопровождении слов ораторов, а о песнях, подогревающих интерес нацеленных на митинг граждан. Обычно используются такие песни, которые по своему содержанию являются своеобразным призывом, могут каким-либо образом повлиять на эмоциональную составляющую личности митингующих, что в свою очередь может подтолкнуть толпу к действиям. Однако, встречаются и такие ситуации, когда текст песен давних лет используется с искажённым восприятием.

Для начала оговорим, что влияние музыки на психику человека – не абсолютно, виной всему нельзя назвать музыкальное творчество, но тем не менее оно имеет своё значение. Это подтверждается исследованием многих учёных, одним из которых является нейробиолог и музыкант Дениел Левитин. Он доказал, что музыка на нас влияет в том случае, когда отражает наше внутреннее состояние, является его проекцией.

Во время прослушивания музыки важен ритм песни, иногда его содержание. Важно учитывать эмоциональный фон человека, прослушивающего музыку, а также то, на что человек готов тратить свои силы и на сколько прослушивание музыки может замотивировать к этому.

С какой целью музыканты выступают на таких мероприятиях и к чему это может привести? Для ответа на этот вопрос рассмотрим музыкальные песни, использованные на митингах, разделив их условно на 2 категории.

Первой категории присущ такой вид песен, текст которых был создан относительно недавно, а содержание включает то, на чём акцентируется внимание общества – в данном случае это проблемы в государстве и отношение музыкантов к этим проблемам. Ярким примером будет являться группаIc3peak. Ажиотаж 2018 года вокруг срыва концертов данной группы перерос в выступление на митинге ужев Москве 10 августа 2019 года напроспекте Сахарова с требованием допустить до выборов незарегистрированных кандидатов в Мосгордуму, против так называемой «политической репрессии» и цензуры, и закрыть уголовное дело о массовых беспорядках,

возбужденное после несанкционированной акции 27 июля, под лозунгом «Допускай!», что «подогрело» интерес общества к данному мероприятию. На данном митинге выступали и другие исполнители (FACE, кровосток), почему мы говорим конкретно об IcЗpeak? Потому что солисты данной группы сами подтвердили, что их творчество – это личные взгляды, подкреплённые откликомнарода на ситуацию в государстве.Кроме того, стать «политичными», такими, какими их примут фанаты – хороший пиар-ход, который проявил себя после отмены концертов и актуален до сих пор. Песни группы не относятся к материалам экстремистской направленности, однако это не означает, что их песни не принесут вреда: радикальное выражение своей политической позиции косвенно отражается как на фанатах, адаптирующихся под мнение своего кумира, так и на гражданах, участвующих в митингах, психологически настроенных на собрании и замечающих его поддержку в речах таких исполнителей. Для данной группы выступление на митинге было не просто очередным золотым ресурсом, но и подходящим моментом для агитации своих взглядов, находящих отражение в их творчестве.

Такого рода песничаще всего используются на митингах и акциях, поскольку идея таких «собраний» отражается в словах песен. Люди психологически воодушевляются и их первоначальный настрой на реализацию целей мероприятия лишь увеличивается.

Вторая категория – это песни, смысл которых далёк от цели использования на несанкционированных сборах. Примером будет являться песни Виктора Цоя «Перемен» и польского исполнителя ЯцекаКачмарского «Рухнут стены». Песня Виктора Цоя не раз звучала на протестах и митингах в поддержку оппозиции в Беларуси во время предвыборной агитации. В конце концов, данная песня стала гимном всех несогласных после 6 августа. Тогда организованный властями праздник «Калейдоскоп творчества» в Киевском сквере превратился в митинг оппозиции, к которому неожиданно присоединились и диджеи из Дворца молодежи: Кирилл Голанов и Владислав Соколовский, которые и включили данную песню. Сам текст песен не содержит призыва к смене политических установок, вряд ли Цой в период её создания вкладывал какой-либо политический оттенок. Данная песня стала гимном несогласных лишь потому, что она отражает в главной своей строчке «перемен требуют наши сердца» желание протестующих изменить направление политики в своём государстве, это подтверждается тем, что присутствующие встретили воспроизведение песни скандированием: "Жыве Беларусь!" («Да здравствует Беларусь!»), " Верим! Можем! Победим" и непосредственно скандирование строчки песни.

Песни из данной категории отражаются на сознании тех людей, которые буквально ищут подходящий аудиофон для тех событий, в которых они находятся. Им неважно о чём песня, каких взглядов придерживался исполнитель. Они слышат подходящую часть песни и скандируют её. Песни такой категории могут быть опасны во время митингов лишь в том случае, когда и без того взбудораженные митингующие после песни воодушевившись до конца решаться на какие-либо действия.

Таким образом, песни, используемые на митингах, либо содержат призыв изначально и их воспроизведение нацелено на подогрев идеи самого митинга, на провокацию, так как исполнители песен могут придерживаться определённых политических взглядов, либо песня становится гимном собрания стихийно, имея в своём содержании не призыв, а лишь какую-либо строчку/куплет, отражающую каким-либо образом события, из-за которых организован митинг.Музыка на митинге может быть толчком к действиям, являться дополнительной пропагандой, но не будет являться решающим фактором, так как влияние музыки на психологию человека не абсолютно.

Кроме того, считаю необходимым добавить, что применяется так называемая «расшифровка» текстов песен, в которой читателю подобной статьи предоставляют вариант того, что автор песни якобы хотел донести до публики. На деле же чаще всего нет информации о том, что такая расшифровка является верной и исходит от первоисточника (т.е. автора). Данные сайты стоит анализировать с правовой точки зрения, так как информация в расшифровках искажается до абсурда – возникновение сцен, которых в песне/видеоклипе нет, но текст может расцениваться как провокация. Более того, сайты находятся в свободном доступе.

Подводя итог, стоит сказать, что внимание необходимо обращать именно на первую группу песен, поскольку их содержание направлено накакого-либо рода призывы, что вполне успешно будет в том случае, если аудитория и ситуация располагает к восприятию таких призывов, а сами исполнители нацелены на дальнейшее развитие пропаганды своих взглядов. Это опасно именно для той аудитории, чьи взгляды и убеждения ещё не сформировались либо достаточно гибкие и подвержены искажению, взгляды заимствуются и восполняются от влиятельных для такой аудитории людей, в том числе и от кумиров.

Мулюкина Анна Евгеньевна
Факультет подготовки сотрудников полиции
и следователей,
Барнаульский юридический институт МВД России г. Барнаул

Мулюкина А.Е. РОЛЬ ИНТЕРНЕТ-РЕКРУТИНГА В ОРГАНИЗАЦИИ НЕСАНКЦИОНИРОВАННЫХ МИТИНГОВ

У митингов, которые становятся день ото дня все более кровавыми, нет каких-то явных лидеров или партийной организации, тем не менее протесты идут. И координируются они достаточно профессионально.

В настоящее время для координации протестных акций активно используются социальные сети, мессенджеры, интерактивные карты и даже приложения для знакомств. Накануне митингов и шествий оппозиционные активисты распространяют через закрытые Telegram-каналы методички, подробно объясняющие, как привлечь к участию в акциях своих родственников, друзей и нейтрально настроенных граждан. По мнению социологов, агитация направлена на молодое поколение, организаторы играют на потребности молодёжи повысить самооценку и испытать новые эмоции[1].

Молодые люди в возрасте до 30 лет стали самой активной частью протестов. Именно они чаще всего вступали в конфронтацию с полицией, выкрикивали лозунги и заводили толпу.

«Мария Филь, RT социолог, директор группы компаний «НИИ социологии, объясняет это тем, что молодёжь в любом обществе — наиболее протестный электорат. Здесь имеет место поколенческий конфликт, потому что власть ассоциируется с неким доминированием старших, которые якобы навязывают свои правила игры, порядок поведения. То есть в широком смысле это проблема отцов и детей: молодёжь хочет заявить о себе, хочет иметь больше возможностей, и ей кажется, может быть, с подачи ряда пропагандистов, что эти возможности сейчас не столь доступны, как были бы доступны в случае смены власти. Оппозиционные лидеры берут на вооружение образ современного продвинутого человека. Самые яркие кандидаты, такие как Любовь Соболь, позиционируют себя именно так».

В митинге на проспекте Академика Сахарова участвовали в основном люди молодого возраста, следует из опроса, который проводился во время мероприятия, «однако нельзя сказать, что это были в основном школьники или даже студенты». Из 306 опрошенных 50% оказались моложе 33 лет.

Состав участников несанкционированных «гуляний» в Москве 27 июля и 3 августа 2019 года, по наблюдениям RT, был ещё моложе.

По мнению Марии Филь, участники митингов и шествий руководствовались скорее эмоциональными причинами, нежели рациональными.

Большинство приходят, потому что их это зацепило эмоционально. Они не анализируют глубоко, почему отказали в регистрации кандидатам, какие были юридические основания или какие у кандидатов были возможности оспорить это решение. Сам факт, что «нас лишают права выбора», очень сильно эмоционально задевает. Если спросить участников нынешних акций, кого они знают, к примеру, из этих недопущенных 57 кандидатов, назовут в лучшем случае пять-семь фамилий. Но именно такой массовый отказ в регистрации в глазах общества выглядит, будто этих кандидатов организованно убрали в сторону [4].

64% опрошенных узнали о митинге из Facebook, Instagram, Telegram, YouTube или «ВКонтакте». Для молодёжи большую роль играл мотив хайпа. Протест усилиями лидеров общественного мнения превратился в тренд. В отсутствие известных лидеров оппозиции явку на митинг на проспекте Сахарова и атмосферу на нём обеспечили сверхпопулярные исполнители с многомиллионной армией подписчиков — IC3PEAK, Oxxxymiron и группа «Кровосток».

Ещё одной отличительной чертой протеста стала его геймификация — намеренная попытка обернуть незаконные призывы к массовым акциям в игру. Протестующих звали «гулять» по Бульварному кольцу, используя в целях агитации даже приложения для знакомств.

«Выходите в 14:00 гулять на проспект Сахарова: послушаем Face, «Кровосток» и IC3PEAK, а после погуляем по Москве», — пишет 20-летняя девушка в Tinder. А тем временем на «прогулке» протестующих встречают маски омоновцев, дубинки и автозаки.

«Призывы на митинг активно тиражировались в социальных сетях, причём очень часто в историях Instagram, людьми, далёкими и от политики, и от столичной проблематики, — отмечает Мария Филь. — Среди них были звёзды шоу-бизнеса и просто публичные люди, потому это приобрело характер снежного кома».

Подобная ситуация происходит и в Беларуси, где площадка для коммуникации между противниками Лукашенко — мессенджер Telegram. На оппозиционных публичных каналах озвучиваются планы действий митингующих. Там же даются советы, что делать в конкретный момент массовых беспорядков, куда бежать, где собираться.

Кроме того, каналы выполняют пропагандистскую функцию — постоянно говорят о зверствах власти, иллюстрируя это яркими видео и фото. При всем этом данные сообщества полностью анонимны. То есть ведутся не от имени конкретных людей или политических сил [3]. Что резко отличается от майдана на Украине, где анонимные сообщества хоть и влияли на массовое сознание, но намного более значимую роль играли вполне конкретные личности, которые лично на майдане присутствовали ну или хотя бы изредка туда

наезжали. На этом поле в Белоруссии сегодня лидирует Telegram-площадка Nexta.

Для координации в реальном времени используются чаты мессенджеров, где обсуждается тактика поведения, места сбора и прочая важная информация.

При этом призывы зачастую звучат максимально агрессивно.

Пользователи, отправляющие такие сообщения, как правило, выступают под вымышленными именами и не настоящими фотографиями. Они заводят молодёжь и делятся секретами уличного протеста. Агитаторы заранее накаляют обстановку, как будто готовя участников не к мирной акции, а к побоищу. Некоторые призывают не просто к беспорядкам и насилию, а к формам настоящего политического террора.

Для вовлечения нейтральной, «условно недовольной» аудитории, которую можно сагитировать прийти на акцию протеста, используются боты, реклама и накрутка.

Например, накануне митинга на проспекте Академика Сахарова 10 августа 2019 года на ресурсах, где платят за накрутку лайков и комментариев, появились новые объявления. На подобных сервисах пользователь может фактически продать свои страницы в социальных сетях. Заказчики на таких онлайн-биржах публикуют задание поставить лайк к фотографии в Instagram, написать любой осознанный комментарий к записи во «ВКонтакте» или в Facebook.

Так, в пятницу, 9 августа 2019 года, блогер Юрий Дудь опубликовал ролик-обращение с призывом приходить на Сахарова. К вечеру на бирже были размещены заказы на написание провокационных комментариев к этому сообщению. Например, кто-то за 40 баллов, что гораздо выше средней стоимости заказов на бирже, захотел под постом Дудя увидеть призывы «рушить и кромсать, бить витрины». Дудь — сетевой инфлюенсер, у него миллионы подписчиков, поэтому шанс на то, что такой комментарий увидят и, возможно, он возымеет нужный эффект, в разы выше.

Накануне несогласованных протестов 27 июля и 3 августа в совершенно аполитичных группах в соцсети «ВКонтакте» были размещены заказные публикации с явно оппозиционным подтекстом.

Например, в группе интернет-магазина, который продаёт кроссовки, появились записи с призывами поддержать оппозицию и псевдоанализом социально-экономических явлений с уклоном в полемику «до чего страну довели».

«Политические» посты с идентичным содержанием и фотографиями появлялись в пяти нейтральных группах автомобильной и музыкальной тематики и ещё в одном онлайн-магазине, выяснил RT. Посты публиковали в период с 15 по 30 июля. Самая распространённая публикация — фото, на котором женщина держит плакат с узнаваемым оформлением в стиле сторонников Навального и надписью, критикующей налоговую реформу и повышение пенсионного возраста. Под фотографией администрации групп размещали одинаковую надпись: «Давайте поддержим!»

По данным волонтёрской организации «Белый счётчик», в «прогулке по Бульварному» приняли участие до 60 тыс. человек. Согласно опросу, 14% участников получали информацию от знакомых, родных или соседей.

Незадолго до акций по соцсетям активно распространялась инструкция, как уговорить своих родственников прийти на митинги и как вовлечь в протесты нейтрально настроенных граждан. Одним из главных действующих лиц этого проекта стал сотрудник штаба незарегистрированного кандидата в депутаты Мосгордумы Любови Соболь Алексей Миняйло (арестован на два месяца по обвинению в организации массовых беспорядков). Распространение методички осуществлялось через закрытый чат в Telegram-канале «Команда А».

После сбора заявок на участие в «Команде А» Алексей Миняйло пригласил всех заинтересованных в отдельный Telegram-чат через рассылку по почтовым адресам.

Далее следовала подробная инструкция. Сначала от участника требовали составить список из десяти знакомых, которые, как ему кажется, с наибольшей вероятностью готовы будут пойти на митинг. Разговор с ними нужно начинать издалека: знают ли они о ситуации вокруг выборов в Мосгордуму? Если не знают, рассказать и начать расспрашивать дальше: довольны ли они положением дел, хотят ли что-то менять и поддерживают ли оппозицию? В случае если собеседник попадался аполитичный, требовалось использовать более приземлённые аргументы.

«Если человек, по твоей оценке, политически активен, используй аргументы скорее про демократию и ценности. Если человек не очень интересуется политикой, начинай разговор с конкретной пользы, которую твой собеседник и Москва получат от присутствия оппозиции в Мосгордуме», — говорилось в методичке.

Существенную долю текста занимает психологический разбор: приводится десять вариантов аргументов и контраргументов для людей, которые не хотят идти на незаконную акцию и пытаются спорить на эту тему с агитатором.

Заведующий отделом клинической психологии РАМН, кандидат психологических наук Сергей Ениколопов изучил приёмы, использованные при составлении методички, отмечает, что они нацелены на создание у человека ощущения собственной важности и исключительности.

«Привет, боец!» — это не абстрактный призыв, а конкретный. Людям всегда приятно, когда к ним обращаются лично. Сама военная лексика — «боец», «особая миссия» — накручивает не просто на митинг. Когда вам говорят «боец», вы начинаете ощущать противостояние, подсознательно противопоставлять «мы» и «они». Причём «они» деперсонализируются, превращаются в Мордор, «чёрную силу», а «мы» — светлые, конечно. За счёт этого повышается самооценка и внутренняя готовность быть «бойцом». Происходит героизация поступка, возникает готовность к каким-то конкретным действиям. Можно предположить, что этот документ составляли профессионалы, хорошо знающие психологию», — рассказал RT Ениколопов.

Методички подобного рода напоминают заветы американского политтехнолога Джина Шарпа — идеолога применения «мягкой силы». Шарпа считают отцом «цветных революций». Он анализировал, как происходят такие массовые мероприятия и как реализуются протестные сценарии. Его книга содержит конкретные технологии ненасильственного свержения действующей власти. Эти методы уже опробованы в Египте, Тунисе, Югославии и Грузии. То, что мы видим в этом документе, — по сути, переработанная под современные реалии версия его концепции [2].

Исходя из вышеизложенного следует сделать вывод, что массовый рекрутинг в различные несанкционированные протестные акции посредством сети Интернет является одним из наиболее опасных видов вовлечения. Благодаря использованию социальных сетей вербовке подвергается огромное количество людей разных возрастных категорий. Также перед правоохранительными возникает проблема изобличения конкретных лиц-организаторов и координаторов таких акций, но, ввиду анонимности проводимых преступниками операций, задача по их поиску становится практически невыполнима.

Список литературы:

1. Дубровский К. Г. Политический аспект массовых протестных акций в современной России. URL: http://www.skags.ru/Damp/autoref Dubrovskiy.doc (дата обращения: 12.11.2020).
2. Даффлон Дени Молодежь России. Портрет поколения на переломе // Вестник общественного мнения. Данные. Анализ. Дискуссии. 2008. №5. URL: https://cyberleninka.ru/article/n/molodezh-rossii-portret-pokoleniya-na-perelome (дата обращения: 13.11.2020).
3. Соловей Валерий Дмитриевич Социальные сети как инструмент политических перемен: возможности и ограничения // Коммуникология. 2017. №5. URL: https://cyberleninka.ru/article/n/sotsialnye-seti-kak-instrument-politicheskih-peremen-vozmozhnosti-i-ogranicheniya (дата обращения: 13.11.2020).
4. Статистические данные опроса о количестве участников московских протестов. URL: https://www.vedomosti.ru/opinion/articles/2019/08/11/808586-prishel-saharova (дата обращения: 12.11.2020).

Лаптева Дарья Николаевна
Институт социальных наук
АлтГУ
Г. Барнаул

Лаптева Д.Н. КИБЕРТЕРРОРИЗМ КАК ГЛОБАЛЬНАЯ ПРОБЛЕМА СОВРЕМЕННОСТИ

Понятие терроризм существует уже более трех столетий. Прогресс не стоит на месте, современные технологии развиваются, государства принимают меры по сокращению преступности и ее предотвращению, при этом сами преступники становятся все более изощрёнными. Научно-техническая революция дала плодородную почву для развития нового вида терроризма. Вчерашние «страшилки будущего» стали для нас уже реалиями, сегодня мы говорим о кибертерроризме.

В типологии обществ наше называют не только постиндустриальным, но и информационным. Главное в нашем мире — это информация и знания, которыми можно владеть. Люди хранят всё в сети, начиная от номера телефона, заканчивая паспортными данными. Вся наша жизни связана со «всемирной паутиной». А если мы говорим не о конкретной личности, а о многомиллионной компании или государстве, тогда угроза киберпреступлений приобретает общенациональный характер. Для преступников Интернет это настоящая находка, потому что действительно защищенных систем очень мало. Все коды пишет человек, а значит, человек может их взломать.

В 2020 году угроза кибертерроризма стала еще более актуальной. Вирус COVID-19 изменил жизни всех людей в мировом сообществе. Если раньше некоторые не пользовались Интернетом, или никогда не указывали важных данных в сети, то сегодня изоляция вынудила всех воспользоваться электронными кошельками и банками, для общения многие завели страницы в социальных сетях, больше времени люди стали проводить за компьютером и телефоном, а значит стали более подвержены влиянию пропаганды. Террористам важно получение любой несанкционированной информации, доступа к тем или иным ресурсам или оборудованию — все это цель преступников. Необходимо обратить пристальное внимание на глобальную проблему человечества, чтобы определить масштабы угрозы и разработать стратегически верные пути установления и сохранения безопасности.

Стоит определить, что же является кибертерроризмом. Впервые термин «кибертерроризм» был употреблен в 80-х годах прошлого столетия научным сотрудником американского Института безопасности и разведки Бэрри Коллином для обозначения террористических действий в виртуальном

пространстве. Ученый считал, что термин будет полностью раскрыт и использован в начале XXI века, однако уже в 90-х года XX века произошли первые кибератаки.

«Д. Деннинг, профессор Джорджтаунского университета и один из самых авторитетных экспертов в области компьютерной преступности и кибербезопасности в книге “Активность, хактивизм и кибертерроризм: Интернет как средство воздействия на внешнюю политику” говорит о кибертерроризме как о “противоправной атаке или угрозе атаки на компьютеры, сети или информацию, находящуюся в них, совершенной с целью принудить органы власти к содействию в достижении политических или социальных целей”» [1, с.133].

Стремительное развитие науки вывело угрозу кибертерроризма из лабораторий университетов в повседневную жизнь. Простота использования сети Интернет, полное отсутствие цензуры, анонимность и транслирование пропаганды большому количеству людей способствует популяризации киберпреступлений. Тенденция увеличения кибератак будет расти по мере развития технологий. Их опасность заключается в том, что действовать террористы могут из любой точки мира, это может быть ваш сосед или начальник, а может госслужащий или крупный бизнесмен.

Из определений можно сделать вывод, что кибертерроризм используется прежде всего для устрашения, подавления, шантажа или принуждения народа и правительства. Поэтому преступникам необходимо иметь «рычаг давления»: ценную информацию или способность нанести урон критическим инфраструктурам. Чтобы обеспечить доступ к этим данным, киберпреступники должны быть хорошо подготовлены и иметь серьезное оборудование. Взломать систему безопасности НАТО с обычного компьютера не так просто. Антитеррористические организации всех стран тоже не стоят на месте, лучшие кибер-гении следят за безопасностью правительственных данных. Для составления конкуренции контртеррористическим структурам преступникам необходимы ресурсы, а это может привести к раскрытию их анонимности и срыву планов. Государствам необходимо постоянно наращивать уровень подготовки к кибератакам, проводить расследования и выявлять возможных преступников, от этого зависит стабильность всего общества.

Для международного сообщества обеспечение кибербезопасности является одним из приоритетных направлений развития, так как преступления в этой сфере подрывают мирную жизнь граждан, способны вызывать напряжение отношений между разными странами, войну и нанести катастрофический урон миру.

Восемь ведущих государств мира, включая Россию, приняли Окинавскую хартию глобального информационного общества от 22 июля 2000 года, по которой в целях развития глобального информационного общества предлагается предпринять «согласованные действия по созданию безопасного и свободного от преступности киберпространства» [2]. Страны, считающие себя передовыми, должны разработать принципы и план по развитию

кибербезопасности. Пока будет происходить разобщенность, мировые державы буду терпеть поражение. Для комплексной защиты государства должны обеспечить развитие безопасности на всех уровнях, в том числе региональных и городских.

Предупреждение кибертерроризма невероятно сложная задача. Для того чтобы обеспечить информационную безопасность РФ, 15 января 2013 года Указом Президента РФ № 31-с на ФСБ РФ были возложены полномочия по созданию государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ [3, с.54]. От установления причин киберпреступлений и совершенствования законодательной базы зависит точность проведения политики по обеспечению безопасности. Из-за того, что кибертерроризм сравним по масштабам угрозы с обычным террористическим актом, введение уголовной ответственности является необходимой и первостепенной задачей.

Одним из важных аспектов защиты населения от кибертеррора является формирование гражданского общества и развитие правовой культуры населения. В России проводятся профилактические мероприятия в школах и ВУЗах по минимизации террористических настроений и проявлений в общественной среде. Также необходима поддержка легитимизации политической оппозиции и свободное выражение различных точек зрения на политический строй. Обеспечение правовой формы государства играет важную роль, ведь, равенство всех людей перед законом и справедливость наказаний приводит к стабилизации общества и увеличению сторонников действующей власти. Это способствует тому, что люди не будут слепо верить громким лозунгам нелегитимной оппозиции, призывающих к беспорядкам, бунту и революции.

В заключение хочется сказать, что кибертерроризм представляет серьезную угрозу для всего человечества наравне с ядерным и биологическим оружием. Из-за того, что данный вид терроризма является новым, он до конца еще не изучен, благо сегодня используются эффективные меры по организации кибербезопасности во всем мире.

Список литературы:

1. Туронок С. Г. Информационный терроризм: выработка стратегии противодействия [Электронный ресурс] / С. Г. Туронок // Общественные науки и современность. – 2011. - №4. – Режим доступа: http://ecsocman.hse.ru/data/2014/01/16/1251303793/Turonok.pdf

2. Григорьев Николай Террористические действия в виртуальном пространстве опасны [Электронный ресурс] / Николай Григорьев, Эдуард Родюков. – Режим доступа: https://nvo.ng.ru/armament/2016-07-22/12_cyber.html

3. Муслимова К. Р. Противодействие международному кибертерроризму в Российской Федерации [Электронный ресурс] / К. Р. Муслимова. - «Южно-Уральский государственный университет (национальный исследовательский университет)» Институт лингвистики и международных

коммуникаций, 2017. – 76 с. – Режим доступа: https://dspace.susu.ru/xmlui/bitstream/handle/0001.74/16863/2017_425_muslimovakr.pdf?sequence=1

Кода Егор Александрович
Институт социальных наук
АлтГУ,
г.Барнаул

Кода Е.А. РАСПРОСТРАНЕНИЕ ЭКСТРЕМИЗМА И ТЕРРОРИЗМА В КИБЕРПРОСТРАНСТВЕ КАК СОЦИАЛЬНАЯ ПРОБЛЕМА

В настоящее время, в условиях пандемии COVID – 19 и переходом многих учреждений на дистанционный режим работы, активизировались различные криминальные интернет- структуры, которые угрожают безопасности не только того предприятия, которое они атакуют, но и всего общества в целом. Интернет стал площадкой формирования радикально настроенной молодежи через социальные сети, прививая им экстремистские взгляды, которые, в свою очередь, наказываются по статье 282 УК РФ. Не единичны случаи вербовки людей в террористические организации через сеть Интернет, что приводит к распространению террористической идеологии на территории Российской федерации, а также угрожает безопасности и жизнедеятельности Российского общества в целом. Исходя из вышеприведенных рассуждений, можно говорить о том, что проблема распространения экстремизма и терроризма в сети Интернет, чрезвычайно актуальна и требует немедленных корректировок как со стороны властей, так и со стороны каждого сознательного гражданина, посредством фильтрации той информации, которую он получает посредством взаимодействия с киберпространством. (Далее распространение экстремизма и терроризма заменяется на кибертерроризм и киберэкстремизм).

Конец 90-х годов прошлого столетия и начало нынешнего столетия ознаменовало совершенно новый способ распространения и передачи информации- Интернет. Но практически с самых первых дней Интернет стал использоваться не только в благих целях простыми гражданами, но и представителями криминального мира. На сегодня киберпространство прочно вошло в жизнь каждого человека, ведь доступ в Интернет возможен практически с любого устройства. Отсюда и быстрое, массовое распространение информации через сеть. Более того, социальные сети выступают катализатором передачи информации, ведь ничто так не «раскачивает» новость, как народное обсуждение этого вопроса. А мессенджеры представители криминального мира используют для связи с теми, кто соглашается вступать с ними в коммуникацию. Примером могут послужить анонимные чаты Telegram.

Сеть Интернет и киберпространство в целом, являются крайне привлекательными для ведения экстремисткой и террористической деятельности, как по функциональному назначению, так и по ряду параметров.

Юджин Спаффорд считал, что Интернет – всемирный виртуальный тренировочный лагерь террористов, в этом с ним нельзя не согласиться[1].

Основные параметры, которые определяют киберпространство, как место распространения экстремисткой и террористической идеологии следующие:

- Слабый контроль со стороны федеральных властей и закона за деятельностью, которая реализуется в сети Интернет.

-Отсутствие должного уровня цензуры информации в массовых сетях

- Минимальный набор технического оборудования для выхода в сеть Интернет, а также минимальная стоимость этого оборудования

-Доступность информации. Даже то, что запрещено в обычном Интернете, крайне легко найти в «даркнете», имея при этом минимальный набор компьютерных знаний.

-Анонимность общения: никто из субъектов достоверно не знает, кто сидит на том конце провода за монитором.

-Крайне быстрая передача информации, а также огромная аудитория для воздействия информацией и т.д

Если посмотреть на проблему с криминологической точки зрения, то становится очевидно, что по мотиву содержательный потенциал киберугроз из корыстного постепенно преобразуется в насильственный, нацеленный на значительные разрушение социальных общностей и материальных инфраструктур. Отсюда следует и большая опасность киберпреступлений для человечества в целом [2, с 378-379].

Интерес к данной проблеме ученые проявляют еще с начала 21 века, в частности- по вопросам нейтрализации, предупреждения и искоренения деятельности экстремистских и террористических киберорганизаций. Но в международном праве до сих пор нет точного определения «киберэкстремизма» и «кибертерроризма». Все предложенные определения, в том числе и О.А. Голика, гласящее, что это «использование персонального компьютера как средства достижения политических целей…» являются достаточно дискуссионными, так как не только с персонального компьютера можно осуществлять такую деятельность, да и в целом непонятно, что конкретно определяется этим понятием, как деятельность. Не хватает конкретики в подобных определениях. Другие ученые определяют кибертерроризм как деятельность в виртуальном мире, осуществимая только в виртуальном мире, но это определение также не выдерживает критики, так как из виртуального мира влияние этой девиации распространяется на реальный мир, нанося вред социальным группам, обществу и государству.

Обращаясь к опросам, которые проводились разными компаниями в разные периоды времени, (автор ведет речь об опросах Компаниями Касперский, Eset, Norton и тд.) выясняется, что в большей степени, лица от 34 до 50 лет чаще всего попадают под кибератаки и получают вирусную программу на свой персональный компьютер, а основным видом киберпреступлений люди видят похищение данных банковских карт и других личных данных путем заражения ПК пользователя вирусной программой – 55%

опрошенных, 28% опрошенных заявили о мошенничестве в интернете, как важной проблеме киберпреступности в целом, 6% выделили основным вариантом киберпреступленийлже-казино и лже- букмекерские конторы, которые не выплачивают деньги, о проблеме кибертерроризмане сказал никто из опрошенных, что свидетельствует о слабой работе средств сообщения о подобных организациях, но в тоже время, выпущено множество социальных роликов о том, как не поддаваться вербовке в такие организации, и что делать, если попал под влияние экстремистской кибер-группировки.

Следует отметить, что органы Роскомнадзора отлично отрабатывают появление различных террористических и экстремистских организаций в социальных сетях. Группы с призывами к межнациональной розни-«Россия для русских», с романтизацией криминального мира, по типу «АУЕ», группы с информацией о радикальном Исламе, призывающим к террористическим актам регулярно блокируются, что свидетельствует о том, что государственные органы занимаются данным вопросом достаточно активно.

Совсем другую картину демонстрирует опрос, проведенный на базе Ленинградского государственного университета имени А.С. Пушкина. Все опрошенные молодые люди (от 18 до 25 лет) признали существование кибертерроризма. 97% опрошенных отметили явную опасность кибертерроризма для общества, что свидетельствует об осведомленности молодых людей по поводу случае кибертерроризма и последствий данного явления. Но многие молодые люди оценили работу органов РФ по предотвращению кибертерроризма и киберэкстремиза недостаточно эффективной, а именно 51,5 % опрошенных отметили, что государство не соблюдает все возможные меры по предотвращению таких преступлений в сети Интернет, и только 31,5 % отметили, что органы РФ делают всё возможное, чтобы избавиться от этих преступлений. Столь высокий процент отметивших, что государство не делает всё возможное может объясняться недостаточной информированностью о деятельности государственных структур по решению данной проблемы. В тоже время, на вопрос «Чувствуете ли вы себя в безопасности в киберпространстве?» 66% ответили утвердительно да, и только треть опрошенных не чувствует себя в безопасности. Это свидетельствует об эффективной политике государства в борьбе за безопасное Интернет-пространство. Что касается понятий разновидности киберпреступлений, то наиболее знакомое понятие респондентам оказалось хакерство, а кибертерроризм знакомменее всего -только1% опрошенных отметил, что знает, что это такое. Киберэкстремизм никто из опрошенных охарактеризоватьне смог.[3]. Когда опрошенным предложили предоставить пути решения проблем интернет преступлений, то 70% затруднились ответить, и не смогли назвать никаких конкретных путей решения данной проблемы.

Вышеизложенные материалы подтверждают сложность и многогранность проблемы киберпреступлений в целом, а в частности кибертерроризма и киберэкстремизма. Особенно опасно распространение экстремистских идей и идей терроризма в социальных сетях среди молодежи, так как молодежь всегда

в оппозиции власти, а такой контент будет подогревать этот оппозиционный интерес, соответственно, и вербовка молодых людей может проводиться крайне легко в террористические или экстремистские организации. Опасность подобных организаций подтверждается опытом прошлых лет: «Синий Кит», «Сова никогда не спит», «АУЕ», и прочие группировки нанесли огромный вред социализации многих молодых людей.

Диффузия терроризма и экстремизма в киберпространство действительно затрагивает и национальные интересы нашей Родины, и систему коллективной безопасности Российской федерации [4]. Оперативные меры по пресечению деятельности таких организаций должны объединяться с превентивными мерами деятельности таких организаций в виде бесед в школах, университетах, публичных лекциях и занятиях по соответствующим темам, а также- развитая система социальной рекламы о том, что за терроризм и экстремизм в киберпространстве грозит не меньшая ответственность, чем за эти же действия в реальной жизни. Аналогично с превентивными мерами распространения и употребления наркотиков среди молодежи, или противоборству с пьяными водителями на дорогах.

В заключение, хочется отметить, что большинство террористических и экстремистских организаций используют в своей деятельности новейшие достижения научно-технического прогресса, в том числе сеть Интернет, ультрасовременные коммуникационные технологии, а старые методы для них отходят на второй план, так как становятся малоэффективными. Так как скорость применения различных видов коммуникационных средств в преступной среде крайне высока, закон не успевает среагировать на все выпады преступного мира в киберпространстве, следовательно, законодательство не успевает регулировать данные вопросы на должном уровне. Поэтому, необходимо проводить постоянную профилактическую работу с населением, касаемо безопасности в сети Интернет. Это форма как бесед и публичных лекций в образовательных учреждениях, так и социальные ролики в социальных сетях, которые распространятся достаточно быстро. Кроме того, необходимо регулярно проводить социологические опросы населения по поводу осведомленности о способах терроризма, экстремизма и иных преступлений в киберпространстве, о том, как с ними бороться и уже на основании этих опросов строить коррекционные меры по работе с населением. Особое внимание стоит уделить подрастающему поколению, так как информация, распространяемая экстремистскими организациями и террористами в Интернете, может нанести непоправимый вред их моральному развитию и социализации, а также старшему поколению, для предупреждения их попадания науловки мошенников и террористов в киберпространстве. Таким образом получится решить столь сложную и многогранную проблему.

Список литературы:

1. Голяндин Н.П., Горячев А.В. Мотивации вербовки в экстремистские и террористические организации // Вестник Краснодарского университета МВД России. 2013. N 2.

2. Лебедев С.Я. Криминологическая оценка и перспективы антикриминогенной превенции террористического потенциала киберпространства // Противодействие экстремизму и терроризму в Крымском федеральном округе: проблемы теории и практики: материалы Всерос. науч.-практ. конф. Симферополь,2015

3. Демида Жанна Леонидовна, Кошечкина Елена Александровна ОТНОШЕНИЕ К ТЕРРОРИЗМУ И КИБЕРТЕРРОРИЗМУ В МОЛОДЕЖНОЙ СРЕДЕ РЕГИОНАЛЬНОГО ВУЗА // TheNewmaninForeignpolicy. 2020. №52 (96). URL: https://cyberleninka.ru/article/n/otnoshenie-k-terrorizmu-i-kiberterrorizmu-v-molodezhnoy-srede-regionalnogo-vuza (дата обращения: 22.11.2020).

4. Пестрецов М.А. Профилактика как важный инструмент противодействия религиозному и политическому экстремизму в Российской Федерации // Вестн. Краснодар.ун-таМВД России. 2016. № 3(33).

Бузаканов Виктор Бакытович
Юридический институт АлтГУ, г. Барнаул
Научный руководитель: Мазуров Валерий Анатольевич,
кандидат юридических наук,
доцент кафедры уголовного права и криминологии АлтГУ

Бузаканов В. Б. ПОПУЛЯРИЗАЦИЯ ИДЕОЛОГИИ ТЕРРОРИЗМА И ЭКСТРЕМИЗМА В КИБЕРПРОСТРАНСТВЕ: ПРОБЛЕМЫ И ПУТИ ИХ РЕШЕНИЯ

Начало XXI в. правомерно называют «информационной революцией», поскольку компьютеры, всемирная сеть Интернета, виртуальные социальные сети, киберпространство в целом не только окружают человека, но и прочно вошливо все сферы повседневной жизни современного общества, включая связанные с противоправным поведением его отдельных представителей.

По своему функциональному назначению киберпространство, в том числе информационно-телекоммуникационная сеть Интернет, сегодня по многим параметрам является наиболее привлекательным средством для экстремистско-террористической деятельности. Если перефразировать слова английского ученого Юджина Спаффорда, то Интернет сегодня — это «всемирный виртуальный тренировочный лагерь» террористов [4].

Привлекательность Интернета для экстремистских и террористических организаций обусловлена следующим:

1. легкой доступностью;
2. незначительным или полным отсутствием национального контроля в форме законодательных норм ограничения или цензуры;
3. неисчерпаемой аудиторией во всем мире;
4. анонимностью общения;
5. быстротой передачи информации;
6. недорогой установкой, содержанием и техническим обслуживанием средств передачи информации;
7. достаточно простым программным обеспечением интерактивной среды в сфере мультимедиа, позволяющим загружать и объединять информацию в различных форматах;
8. применением традиционных средств массовой информации, использующих ресурсы Интернета как источники тем для публикаций.

В настоящее время из 26 террористических организаций, запрещенных на территории России, подавляющее большинство имеет свои интернет-ресурсы, в том числе медиа-агентства и центры. Только за период с 2011 по 2016 г. террористической организацией «Исламское Государство» (запрещена в РФ) созданы медиа-агентства «Аль-Фуркан», «Итисаам», медиа-фонд «Айнад» и

медиа-центр «Аль-Хайят», предоставляющие информацию и вещающие на различных языках мира: арабском, английском, французском, немецком и др. В 2015 г. ИГИЛ запустило в Интернете новый сайт под названием «Халифат. Исламское государство. Информационный сайт» исключительно для русскоязычной аудитории [7, 12].

Мониторинг киберпространства показал, что более 100 тыс. владельцев аккаунтов в «Twitter» либо согласны с идеологией ИГИЛ, либо проявляют интерес к ее деятельности.Если принять во внимание, что подписаться на один из аккаунтов этой социальной сети может от 2 до 50 тыс. человек, то не трудно представить себе объем информационного массива, постоянно вовлекающего в сферу распространения экстремистских и террористических взглядов, а также новостных фэйков этой террористической организации все новых потребителей этих сведений. Для большего охвата аудитории владельцев смартфонови мобильных устройств по заданию ИГ в 2015 г. создано специальное приложение в многозадачной операционной системе Android под наименованием «Рассвет радостных вестей» (TheDawnofGladTidings). Основная задача приложения — в автоматическом режиме осуществлять массовое размножение и рассылку сообщений от имени пользователя в интересах ИГИЛ всем установленным связям [8].

Анализируяроссийские и зарубежные исследования по дилеммам информационного противоборства в глобальной сети [3, 7, 11],можно выделить колоссальный круг направлений деятельности экстремистских и террористических организаций в киберпространстве:

1. совершение информационно-психологических атак на интернет-сообщество;
2. пропаганда экстремистских концепций для оправдания своего насилия в достижении целей организации;
3. создание виртуальной всемирной преступной сети;
4. планирование и координация деятельности участников по совершению конкретных террористических актов и экстремистских акций;
5. сбор информации об объектах планируемых акций и актов;
6. хакерские атаки на государственные сайты и международные интернет-ресурсы [9];
7. предоставление доступной информации о приемах и методах ведения экстремистско-террористической деятельности, вплоть до опубликования рекомендаций по изготовлению средств массового уничтожения населения;
8. формирование различных форм финансирования и привлечения дополнительных средств для обеспечения деятельности организации;
9. выявление сочувствующих и вербовка (рекрутирование) новых членов в организацию [6].

Рассмотрение каждого из вышеназванных направлений может стать предметом самостоятельного исследования. Но учитывая заявленную тему,

обозначим только их множественность и проблемность для обеспечения безопасности общества.

Анализ содержания экстремистских и террористических сайтов показывает, что на них, размещаются сообщения об истории создания организации и ее современном состоянии с обязательным красочным описанием биографий основателей, лидеров или совершенных ими значимых событий — «подвигов», дается подробный обзор ее политических и идеологических целей, прослеживаются социальные и политические связи с известными и публичными личностями, публикуются новостные сообщения об успехах организации иее членах, а также осуществляется бескомпромиссная критика противников и врагов.

Исключительную тревогу у правоохранительных органов вызывает использование экстремистскими группами интерактивных возможностей социальных сетей, предоставляющие их пользователям услуги по загрузке своей информации (контент) и обмену ее в режиме реального времени (онлайн) с другими пользователями.

Согласно данным компании «BrandAnalytics» в Российской Федерации количество активных («говорящих») авторов, которые пользуются социальными медиа, составляет почти 30 млн человек. Ими только в октябре 2020 г. создано около 3 млрд сообщений. Основная часть пользователей предпочитает социальные сети, ими сгенерировано более 80,3 % всех сообщений от совокупного объема упоминаний в социальных медиа. Самой активной из них признается социальная сеть ВКонтакте, объединяющая более 28,5млн авторов, или около 13 % от всего населения России. Второе место занимает микроблогTwitter — 21,7 % от общей статистики авторов. Третье место — за видео-хостингами youtube.com [10] и vimeo.com — 5 %, соответственно.

Половозрастная характеристика социальных сетей свидетельствует о том, что женская аудитория превалирует во всех основных социальных сетях, причем в Instagram она составляет почти 80 % от общей аудитории. Самой возрастной считается социальная сеть Мой Мир, где 78 % пользователей старше 35 лет, а самой молодой — ВКонтакте — 84 % авторов младше 35 лет [1].

Именно последняя самая привлекательная для ведения пропагандисткой работы экстремистских групп и рекрутирования ими в свои ряды новых членов. Из-заогромного объема информации, требующего ежесекундного мониторинга, принимаемые правоохранительными органами меры по выявлению и блокированию экстремистского контента сегодня не позволяют существенно повлиять на складывающуюся ситуацию в медиапространстве. Без глобальных усилий в социальных сетяхвозможно найти отдельных пользователей, группы по интересам, сообщества и даже целые сайты, ведущиекак завуалированную пропаганду, так и призывающие к изменению государственного строя и убийству людей иных взглядов и веры. Такое обстоятельство вызывается еще и тем, что множествоинтернет-ресурсов экстремистских и террористических

организаций находятся вне законодательного поля Российской Федерации. Например, сайт террористической организации «Кавказ-Центр», вещающий для русскоязычных пользователей, многие годы располагается на хостинге литовской компании ELNETA.

Регулярные обращения Российской Федерации на дипломатическом уровне о закрытии данного сайта остаются без реагирования со стороны литовского руководства.

Практика правоохранительных органов зарубежных государствнеоспоримо демонстрирует тот факт, что информационное противодействие экстремизму в сети Интернет в настоящий момент времени требует качественно новых подходов.

По этой причине довольномногообещающими являются методики информационного противодействия экстремизму, разработанные и используемые в США, Китае, Израиле и иныхгосударствах.

К примеру, Бюро расследований штата Джорджии (GeorgiaBureauofIntelligence, GBI) в октябре 2012 г. опубликовало стратегические наработки по организации присутствия сотрудников специальных служб в социальных сетях. В соответствии с этим сотрудникам Бюро предоставлено право применения разнообразных тактических приемов использования своего статуса в сети: открытого, не привлечения внимания (зашифрованного) и тайного (негласного) присутствия. Офицеры и аналитики также вправе действовать на разных уровнях в случае визуального наблюдения и сбора информации из социальных сетей. Первый уровень — очевидный, или открытый статус, который используется тогда, когда сотрудник не скрывает своей принадлежности к ведомству и рассматривает открытые источники информации. В частности, наблюдающийв целях получения необходимой информациимеет правотолько ознакомиться с открытой страницей в Facebook, профилем в LinkedIn или страницей в Twitter.

На втором уровне — статусе непривлечения внимания — явные признаки правоохранительного органа не афишируются в связи с тем, что усилия по сбору информации могут быть затруднены, если станет известно, какое именно ведомство интересуется той или иной информацией (например, в случае проявления интереса к соответствующему блогу или странице в Facebook аналитика из разведывательной службы, работающего по делу о сексуальной эксплуатации детей).

Отдельные криминогенно активные лица могут располагать возможностями по контролю за адресами интернет-протоколов (IP). Следовательно, в определённых случаях аналитику нужен механизм, с помощью которого возможно скрыть принадлежность соответствующего IP-адреса правоохранительному органу. Однако политика ведомства обязана гарантировать надзорное одобрение и контроль за подобными действиями.

Заключительный уровень — тайный — имеет место тогда, когда усилия сотрудника правоохранительного ведомства направлены на то, чтобы его личность осталась неизвестной. В частности, у него имеется тайный профиль

илисекретное имя, для взаимодействия с лицом, покупающим и продающим фотографии с детской порнографией. В связи с тем, чтоданный уровень предполагает активное взаимодействие сотрудника правоохранительногооргана и подозреваемого, политика ведомства должна определять, кто может выполнять эту роль, а также устанавливать надзорные полномочия, необходимые для того, чтобы одобрить использование такого уровня. Также сотруднику нужно учитывать действия, предпринимаемые на местном и федеральном уровнях, а также на уровне штата (напомним, что речь идет о штате Джорджии в США), чтобы избежать дублирования или вмешательства других правоохранительных служб, расследующих это же дело.

Политика Бюро расследований штата Джорджии требует наличия письменного запроса для использования механизмов контроля за социальными сетями. В конкретном запросе обязательно нужно указать цель, временные рамки проведения мероприятия, тип механизма контроля, перечень веб-сайтов, мониторинг которых будет осуществляться, и предположительный срок хранения полученных сведений [5].

Соответствующий продукт успешно апробирован и активно используется в деятельности российских правоохранительных органов семи регионов нашего государства.

Одновременно с этим в сегменте Интернета Россииэнергично функционируют более десятка сайтов, ориентированных на антипропагандистскую работу в сфере противодействия экстремистской идеологии и формирования в российском обществе нравственно-ценностных приоритетов.

Если проанализировать деятельность оперативных подразделений МВД России, ФСБ России по борьбе с экстремизмом и терроризмом, то, несмотря на значительные успехи, к сожалению, естьопределённое отставание в организационно-управленческом и организационно-тактическом плане от современных требований в сфере информационного противодействия экстремистской и террористической деятельности.

В плане дальнейшего развития информационных технологий нашемугосударствунужно ориентироваться на собственные силы и уходить от той иностранной зависимости в области создания аппаратно-программных средств, которая наблюдается в настоящий момент.

Важно уделять больше внимания профессиональной подготовке специалистов в сфере реализации информационных технологий и защиты сведений, шире практиковать наступательные действия в области пропаганды и контрпропаганды на каждом уровне противодействия преступности.

Такие выводы определяют актуальность научных исследований, направленных на решение практических проблем правоохранительных органов, при этом, современные инновационные реалии обусловливают необходимость комплексного подхода к информационному противодействию в сети Интернет, который бы предусматривал следующее:

1. функционирование в системе правоохранительных органов специальныхподразделений постоянного мониторинга киберпространства и своевременного принятия нормативно-технических мер по пресечению пропаганды политического и религиозного экстремизма, а также планируемых акций участников радикальных, экстремистских и террористических групп;

2. обеспечение надлежащей профессиональной подготовки сотрудников таких специализированных служб с привлечением к образовательному процессу специалистов в сфере психологии, теологии, медиа-пространства, а также должностных лиц органов исполнительной, законодательной и судебной власти;

3. объединение усилий общественных, негосударственных, некоммерческих, религиозных, научных интернет-сообществ по созданию агитационно-пропагандистского продукта противодействия идеологии экстремизма и терроризма с последующим его размещением на различных информационных ресурсах всемирной сети, а также организации эффективного правового воспитания пользователей Интернета;

4. изучение и внедрение в правовое пространство национального законодательства положительного опыта зарубежных стран в борьбе с кибертерроризмом и информационным экстремизмом [2], а также создание условий для действенного сотрудничества и формирования правового механизма по обеспечению взаимодействия правоохранительных органов различных государств.

Список литературы:

1. BrandAnalytics. Статистика социальных сетей [Электронный ресурс]. URL: https://br-analytics.ru/statistics/author (дата обращения: 16.11.2020).

2. Баранов В. В. Совершенствование правового обеспечения деятельности органов внутренних дел по противодействию проявлениям экстремизма в глобальной компьютерной сети // Труды Академии управления МВД России. 2016. № 4 (40).

3. Вейманн Г. Как современные террористы используют Интернет [Электронный ресурс]. Специальный доклад № 116. URL: http:// scienceport.ru/library/liball/5170-spetsialnyiy-doklad-№-116-kak-sovremennyie-terroristyi-ispolzuyut-internet/ (датаобращения: 16.11.2020).

4. Голяндин Н. П., Горячев А. В. Мотивации вербовки в экстремистские и террористические организации // Вестник Краснодарского университета МВД России. 2013. № 2.

5. Завьялов С. Зарубежный опыт в области борьбы с пропагандой терроризма в Интернете // Зарубежное военное обозрение. 2014. № 4.

6. Захватов И. Ю, Карулин В. Ю. Вопросы межведомственного взаимодействия по вопросам противодействия терроризму и экстремизму // Труды Академии управления МВД России. 2015. № 2 (34).

7. Мюрид Э. ИГИЛ. «Исламское государство» и Россия. Столкновение неизбежно? М., 2016.

8. Платов В. Информационные ресурсы ИГИЛ [Электронный ресурс]//Новое Восточное Обозрение: интернет-журнал. URL: http:// ru.journal-neo.org/2015/06/08/informatsionny-e-resursy-igil/ (датаобращения: 16.11.2020).

9. Рясов А. В., Лапунова Ю. А. Способы противодействия вовлечению лиц в совершение преступлений террористического характера в информационно-телекоммуникационных сетях // Вестник СевКавГТИ. 2016. № 2 (25).

10. Самошин А. В., Горовой В. В. Особенности предупреждения распространения экстремистских материалов в молодежной среде по глобальной сети Интернет // Труды Академии управления МВД России. 2016. № 3 (39).

11. Сундиев И. Ю. Введение в оперативно-розыскнуютеррологию. М., 2019.

12. Сундиев И. Ю, Смирнов А. А., Костин В. Н. Новое качество террористической пропаганды: медиа-империя ИГИЛ // Информационные войны. 2015. № 1.

Оглоблина Анастасия Юрьевна,
магистрант, юридический институт АлтГУ,
г. Барнаул

Оглоблина А.Ю. ИССЛЕДОВАНИЕ КИБЕРТЕРРОРИЗМА В ПЕРИОД ПАНДЕМИИ, СВЯЗАННОЙ С РАСПРОСТРАНЕНИЕМ НОВОЙ КОРОНАВИРУСНОЙ ИНФЕКЦИИ

За основу исследования была взята статистика компании «Positive Technologies» опубликованная на их сайте «Актуальные киберугрозы: I квартал 2020 года». Positive Technologies – международная компания, специализирующаяся на разработке программного обеспечения в области информационной безопасности, специализирующаяся на комплексном аудите безопасности, организации мониторинга и расследования инцидентов.

Приступим к рассмотрению данного документа, по итогам I квартала 2020 года компания отметила:

- Количество киберинцидентов стремительно растет: выявлено на 22,5% больше атак, чем в IV квартале 2019 года.
- Доля целенаправленных атак осталась на уровне IV квартала прошлого года (67%).
- В течение квартала высокую активность проявляли 23 APT группировки, атаки которых были направлены преимущественно на государственные учреждения, промышленные предприятия, финансовую отрасль и медицинские организации.
- Около 13% всех фишинговых рассылок в I квартале были связаны с темой COVID-19. Около половины из них (44%) пришлись на частных лиц, а каждая пятая рассылка была направлена на государственные организации.
- Более трети (34%) всех атак на юридические лица с использованием ВПО — это атаки троянов-шифровальщиков. Наибольшую активность проявляли Sodinokibi, Maze и DoppelPaymer. Операторы этих и некоторых других шифровальщиков создали собственные сайты, на которых публикуют похищенную у жертв информацию в случае отказа платить выкуп.
- Доля атак, направленных на частных лиц, составила 14%. Половина всех украденных данных — логины и пароли. Это связано с высокой долей шпионского ПО (56%) во вредоносных кампаниях против частных лиц.

Основываясь на рассмотренной статистики, компания считает, что в связи с массовым переходом на удаленную работу в ближайшее время компании могут столкнуться с ростом попыток взлома корпоративных учетных записей и с эксплуатацией уязвимостей в системах удаленного доступа. Угрозы крайне актуальны для компаний, в которых нет строгой парольной политики и регулярного обновления ПО.

Нужно отметить, что вредоносные кампании, нацеленные на организации, в восьми из десяти случаев начинались с рассылки электронных писем с вложениями. Для частных лиц высок риск заразить компьютер не только через электронную почту, но и в результате посещения сайтов и загрузки программ с сомнительных веб-ресурсов. Например, в I квартале злоумышленники скомпрометировали ряд сайтов на базе WordPress и перенаправляли их посетителей на фишинговые страницы, где под видом обновления браузера Chrome распространялся бэкдор. Вредоносное ПО было загружено более 2000 раз.

Поговорим об актуальной проблеме в период пандемии – это фишинговые рассылки на тему COVID-19. Злоумышленники быстро подхватили тему всеобщего беспокойства по поводу коронавирусной инфекции и стали использовать ее для фишинговых писем. По подсчётам компании получилось, что в I квартале около 13% атак, в которых киберпреступники задействовали методы социальной инженерии, были связаны с коронавирусом.

На рисунке, представленном ниже, наглядно продемонстрированы категории жертв фишинговых рассылок, связанных с COVID-19, в 44 % жертвами таких рассылок становились частные лица, а наименьший процент 10 % – промышленность.

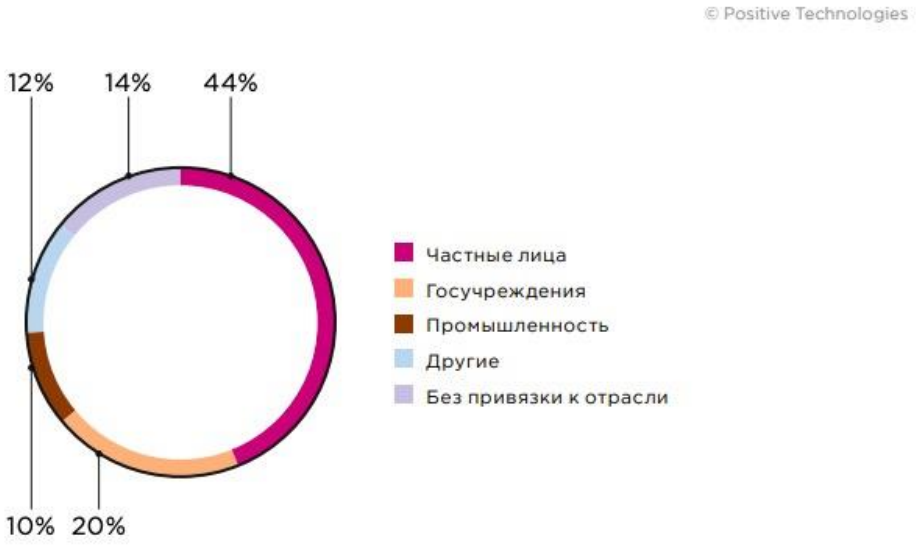

Рис. 1. Категории жертв фишинговых рассылок на тему COVID-19

Рисунок 2. Методы атак (доля атак)

Как отмечает компания, рост числа фишинговых рассылок, посвященных COVID-19,начался со второй половины января. Эпидемией пользовались как для проведения массовых вредоносных кампаний, так и для сложных целенаправленных атак (APT-атак). Под видом официальной информации о статистике заражений, о вакцине и мерах профилактики, рассылаемой якобы от имени государственных органов и медицинских учреждений, в I квартале распространялись трояны Emotet, Remcos, AZORult, Agent Tesla, LokiBot, TrickBot и множество других.

В связи со сложной эпидемиологической обстановкой правительства многих стран, в том числе и Россия, отправили школьников и студентов на дистанционное обучение, а работодателей обязали по возможности перевести сотрудников на удаленную работу и «вся жизнь» была перенесена в платформу для видеосвязи Zoom. Когда начался рост числа пользователей Zoom интерес к ней возрос и со стороны злоумышленников. Так, в течение I квартала было зарегистрировано более 1700 фишинговых доменов, связанных с названием популярной платформы. Активное использование Zoom выявило в приложении ряд уязвимостей. Специалисты компании Check Point обнаружили в платформе

брешь, позволявшую злоумышленникам без приглашения присоединяться к чужим видеоконференциям. Инциденты, связанные с несанкционированным вторжением в онлайн-конференции через Zoom, получили название Zoom-bombing. По заявлению ФБР, в США регистрируется большое число подобных инцидентов. Записи тысяч видеозвонков оказались размещены на YouTube и Vimeo. В свободный доступ попали частные видеозвонки, записи бизнес-собраний, сеансы у врачей, занятия в учебных заведениях. Кроме того, в конце квартала стало известно об уязвимости типа UNC path injection, которая позволяет злоумышленникам похищать через Zoom учетные данные Windows.

Таким образом, были обозначены актуальные угрозы информационной безопасности, основанные на экспертизе компании Positive Technologies, результатах многочисленных расследований, а также на данных авторитетных источников.

Подводя итог, нужно отметить, чтоорганизациям и обычным гражданам, стоит обратить внимание на актуальное состояние информационной безопасности и на наиболее актуальные методы и мотивы кибератак, и киберугроз, что предостережёт интернет-пользователей не стать объектами атак.

В исследовании используются следующие термины:

Кибертерроризм – преднамеренная атака на информацию, обрабатываемую компьютером, на компьютерную систему или сеть, — атака, которая создает опасность для жизни и здоровья людей или наступление других тяжких последствий, если такие действия были совершены в целях нарушения общественной безопасности, запугивания населения или провокации военного конфликта

Кибератака — несанкционированное воздействие на информационные системы и пользователей информационных систем со стороны киберпреступников с использованием технических средств и программного обеспечения в целях получения доступа к информационным ресурсам, нарушения нормальной работы или доступности систем, кражи, искажения или удаления информации.

Массовая атака — кибератака, которая направлена на широкий круг организаций и частных лиц. При проведении массовой атаки злоумышленники могут не ограничиваться одной отраслью экономики или вовсе не учитывать отраслевую принадлежность компаний, их задачей является компрометация максимального числа жертв.

Целевая атака — кибератака, которая направлена на конкретную компанию, отрасль экономики или на ограниченный круг частных лиц. В рамках целевой атаки злоумышленники, как правило, проводят предварительную разведку с целью собрать информацию о выбранной жертве.

Объект атаки — объект несанкционированного воздействия со стороны киберпреступников, например веб-ресурс, компьютер, сервер, сетевое оборудование, мобильное устройство. Объектом атаки может быть и человек, если атака проводится с помощью методов социальной инженерии.

Метод атаки — совокупность приемов, которые используются киберпреступниками для достижения цели.

Список литературы:

1. Актуальные киберугрозы: I квартал 2020 года. [Электронный ресурс]: Positive Technologies. – Режим доступа: [https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020-q1/#id1], свободный (дата обращения: 22.11.2020).

2. Буткевич Сергей Анатольевич Экстремизм и терроризм в киберпространстве: выявление, нейтрализация и предупреждение // Вестник КРУ МВД России. 2018. №1 (39). URL: https://cyberleninka.ru/article/n/ekstremizm-i-terrorizm-v-kiberprostranstve-vyyavlenie-neytralizatsiya-i-preduprezhdenie

3. Гаврилов, Л. П. Электронная коммерция : учебник и практикум для бакалавриата и магистратуры / Л. П. Гаврилов. — Москва : Издательство Юрайт, 2018. — 363 с. — (Высшее образование). — ISBN 978-5-534-01174-6. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/413630

4. Голубев В.А. Кибертерроризм - угроза национальной безопасности [Электронный ресурс]. – Режим доступа: [www.crive-research.ru], свободный– (дата обращения: 22.11.2020).

5. Касьянов, В. В. Социология Интернета : учебник для академического бакалавриата / В. В. Касьянов, В. Н. Нечипуренко. — Москва :Издательство Юрайт, 2017. — 424 с. — (Бакалавр.Академический курс). — ISBN 978-5-534-04944-2. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/408265

6. Рассолов, И. М. Информационное право : учебник и практикум для вузов / И. М. Рассолов. — 5-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2020. — 347 с. — (Высшее образование). — ISBN 978-5-534-04348-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/449839

Бородина Арина Константиновна,
магистрант, юридический институт АлтГУ,
г. Барнаул
Научный руководитель: Казанцев Дмитрий Александрович,
кандидат юридических наук,
доцент кафедры уголовного права и криминологии АлтГУ

Бородина А.К. ЭКСТРЕМИСТСКАЯ ДЕЯТЕЛЬНОСТЬ И ПРОБЛЕМЫ МОТИВА НАЦИОНАЛЬНОЙ, РАСОВОЙ, РЕЛИГИОЗНОЙ НЕНАВИСТИ ИЛИ ВРАЖДЫ

Правовой основой противодействия экстремизму и терроризму являются Федеральные законы от 25.07.2002 № 114-ФЗ «О противодействии экстремистской деятельности», № 35-ФЗ от 06.03.2006 «О противодействии терроризму».

В России антиэкстремистское законодательство существует с 2002 года. В настоящий момент оно продолжает расширяться. Осужденных за экстремистскую деятельность в стране становится все больше и больше. Многие россияне в связи с этим даже считают, что привлечь по этому закону могут любого и за что угодно. Но, конечно же, эта точка зрения неверна — не любого и не за что угодно.

Кэкстремистским в России сегодня могут быть приравнены самые разные виды деятельности. Подробный их список очень широк. Экстремизм в России - это и ложные обвинения лиц, занимающих государственные посты, нарушение прав граждан в зависимости от их национальной, религиозной и т. д. принадлежности, воспрепятствование осуществлению избирательных прав и пр.

Чаще всего граждане РФ подвергаются уголовному преследованию, согласно этому закону, за:

-возбуждение ненависти и розни;

-призывы к экстремистской деятельности;

-оправдание терроризма;

-реабилитацию нацизма;

-оскорбление чувств верующих;

-демонстрацию запрещенной символики;

-распространение экстремистских материалов.

Борьба с экстремизмом: возбуждение ненависти и розни. Привлечь к уголовной ответственности по этому пункту россиянина могут за высказывания в отношении групп людей:

-определенных по признакам этничности;

-религии.

В УК указываются и другие объединяющие признаки, но на практике они используются редко. Возбуждаться вражда в любом случае должна именно к людям, а не к организациям.

Людям, не желающим подвергнуться уголовному преследованию, не стоит делать, прежде всего, публичных намеков на желательность:

-переворота;

-терроризма или сепаратизма;

-дискриминации каких-либо групп;

-создания силовых помех органам власти и т. д.

В данном случае речь в законе идет не об оправдании в педагогическом или моральном плане самих террористов. Наказать могут только непосредственно за утверждение правильности и желательности такого вида давления на общество и государство.

Также следует избегать:

-оправдания массовых преступлений, совершенных нацистами в годы Мировой войны;

-распространения ложной информации о деятельности СССР в годы ВОВ;

-осквернения символов, связанных с российской военной историей, либо памятных дат.

Быть вежливым, к примеру, в той же сети интернет, неплохо. А в данном случае еще и безопасно.

Религиозный экстремизм — именно этот пункт вызывает в российском обществе наибольшее неприятие. Дело в том, что само понятие «чувства верующих» в законодательстве определено расплывчато. То есть решать, что относится именно к религиозным, а что к нерелигиозным чувствам верующих, должны, по сути, сами судьи. Что, конечно же, на практике означает полный произвол и хаос.

Однако бояться привлечения к ответственности за оскорбление чувств верующих слишком сильно все же не стоит. Экстремизм в России в данном случае — это в первую очередь лишь грубые высказывания в отношении веры собеседника или религиозной группы.

Демонстрация запрещенной символики - наказать могут даже просто за выставленную публично картинку или фото (в том числе и при отсутствии какого-либо «экстремистского» намерения). Так что не стоит выкладывать, к примеру, в соцсетях символы:

-нацистские;

-сходные с нацистскими (чем-то похожие на свастику);

-запрещенных на территории РФ террористических или экстремистских организаций;

-организаций, сотрудничавших с нацистами в годы Мировой войны.

Список таких материалов официально публикуется на сайте Минюста, а также центра «Сова». Содержит он более 3 тыс. пунктов и запомнить их все, конечно, невозможно. К тому же и поиск в интернете не всегда помогает узнать о том, запрещен материал или нет. Но, тем не менее, от ответственности за распространение это граждан не освобождает.

Поэтому, чтобы не попасть под действие закона, следует соблюдать такие меры предосторожности:

-избегать распространения материалов уже запрещенных на территории РФ организаций;

-не выкладывать в сеть материалы, вызывающие какие-либо сомнения у пользователя лично, без тщательной проверки на предмет запрещенности.

Некоторые пользователи Сети считают, что, если они не будут выкладывать публично экстремистских картинок или делать подобных высказываний, наказать их не смогут. Однако в интернете в этом плане есть несколько подводных камней, о которых стоит знать.

Проявления экстремизма, с точки зрения российского законодательства, это, помимо всего прочего, и:

-репосты экстремистских материалов, несмотря даже на то, что высказывание в данном случае принадлежит третьему лицу;

-лайки (к примеру, под запрещенным видео).

Публичным же считается любое высказывание или картинка, не защищенные паролем. Также пользователя интернета могут наказать за материал, размещенный в Сети уже давно. Конечно, обратной силы закон не имеет. Но разного рода материалы, выложенные в сеть до признания их экстремистскими, должны быть пользователем удалены.

Список литературы:

1. Европейская конвенция о пресечении терроризма (1977) // СПС «КонсультантПлюс».

2. Дикаев С.У., Диваева И.Р. Уголовная ответственность за преступления террористического характера: Учебное пособие. Уфа, 2001.

3. Зуев А. Средства массовой информации и проблемы межэтнических взаимоотношений. Саратов, 2006.

4. Криминология / Под ред. Дж. Ф. Шели. СПб., 2003.

Стародубцева Мария Александровна,
ассистент кафедры уголовного
права и криминологии
юридического института АлтГУ, г. Барнаул
Рохманов Антон Сергеевич,
Юридический институт АлтГУ, г. Барнаул

Стародубцева М.А., Рохманов А.С. НЕКОТОРЫЕ ПРОБЕЛЫ В ПРАВОВОМ РЕГУЛИРОВАНИИ ЭКСТРЕМИСТСКОЙ ДЕЯТЕЛЬНОСТИ И ЭКСПЕРТИЗЫ ЭКСТРЕМИСТСКИХ МАТЕРИАЛОВ

Экстремизм в научной литературе трактуется как приверженность крайним взглядам и *деструктивным, агрессивным мерам* разрешения конфликтных ситуаций [1]. Это в частности соответствует взгляду Уве Бакеса, рассматривающего экстремизм как этические и правовые границы модели социально-политической, конституционной системы [2, 3]. Одним из вариантов этого широкого спектра экстремистских флуктуаций выступает религиозно-идеологический протест в виде фундаменталистской модели религиозно организованного государства, центрированного вокруг категорий священного и Божественного закона. Другой вариант, сам состоящий из множества частных разновидностей, – ультранационализм. В качестве еще одного примера можно привести неоязыческую субкультурную традицию, фундированную на протестной расово-этнической идентичности. С.И. Чудинов не в полной мере соглашается с позицией Бакеса, согласно которой экстремизм противопоставляется «умеренному ценностно-идеологическому фундаменту». Действительно, это может быть справедливо в европейской либерально ориентированной науке, однако неудачно для перенесения в любую, особенно российскую, реальность, для которой как раз никакой «умеренности» не существует априори. Европейский суд по правам человека отмечал, что область экстремизма, экстремистской деятельности «сложна для формулирования законов с абсолютной точности, допустима определенная степень гибкости, чтобы позволить российским судам оценивать, следует ли конкретное действие расценивать как разжигающее ненависть и вражду по признакам, перечисленным в указанной статье (ст.282 УК РФ)» [4].

В ст.1 ФЗ «О противодействии экстремистской деятельности» [5] (далее – Федеральный закон) дается определение экстремистской деятельности. Однако, если мы в него углубимся, то увидим, что в настоящем Федеральном законе отсутствует само понятие, дан лишь перечень деяний, которые судам следует считать экстремистскими. Следует также отметить, с 2007 года список деяний

расширялся, но, по нашему мнению, это способствовало конкретизации определения экстремистской деятельности. Рост же уголовных дел с 2009 по 2017 (статистика административных дел не ведется) связан с иными, политическими и правовыми, причинами.

Федеральный закон является основным регулирующим актом. Санкции установлены в УК РФ и КоАП РФ. Помимо нормативно-правовых актов важнейшими документами являются Постановление Пленума Верховного Суда РФ от 28.06.2011 N 11 «О судебной практике по уголовным делам о преступлениях экстремистской направленности» [6] (далее – Постановление Пленума) и Стратегия противодействия экстремизму в РФ до 2025 года [7] (далее – Стратегия).

Постановление Пленума до редакции 2018 года было недоработанным и порождало серьезную правовую путаницу. Вот несколько пробелов законодательства, существовавших на то время (с изменениями от 2018 года в скобках):

- Достаточность лишь формального подвода для возбуждения уголовного дела – например, факт размещения в интернете «экстремистского» контента (теперь же необходимы веские основания для возбуждения, которые указывали бы на общественную опасность и мотив совершения преступления).
- Прямой умысел без осознания направленности деяния на цели экстремизма (сейчас же лицо должно понимать направленность деяния на нарушение основ конституционного строя, а также иметь целью возбудить ненависть или вражду либо унизить достоинство человека или группы лиц по признакам пола, расы, национальности, языка, происхождения, отношения к религии либо принадлежности к какой-либо социальной группе).
- Редко учитывался контекст (теперь при определении умысла на возбуждение ненависти суд должен рассматривать совокупность обстоятельств и учитывать: форму и содержание размещенной информации, её контекст; наличие и содержание личных комментариев пользователя; факт личного создания либо заимствования контента; содержание всей страницы пользователя и характеристику его личности; объём «экстремистской» информации, частоту и продолжительность ее размещения, интенсивность обновлений).
- Неясность процедуры и технологии гуманитарной экспертизы на экстремизм – очень часто эксперты буквально давали *правовую* оценку, заключение эксперта превалировало над другими доказательствами (теперь при оценке заключения эксперта по «экстремистским» делам суды должны помнить, что оно не имеет заранее установленной силы, не обладает преимуществом перед другими доказательствами и оценивается по общим правилам в совокупности с другими доказательствами).

Представляется, на Верховный Суд РФ всё же оказало некоторое правовое влияние ранее упомянутое Постановление ЕСПЧ «Дмитриевский против России».

П.101 Постановления ЕСПЧ указывает на важность рассмотрения каждого дела с точки зрения контекста и оценки потенциальной и непосредственной вредоносности. П.112-114 указывают на ошибки в гуманитарной экспертизе на экстремизм высказывания, текста, на чем бы хотелось остановиться подробнее чуть позже.

Необходимо также сказать о Стратегии противодействия экстремизму. Она дает очень важные понятия «идеология насилия», «радикализм», «экстремистская идеология», «проявления экстремизма (экстремистские проявления)».

Исходя из определений Стратегии, деяния указанные в Федеральном законе, о которых было сказано ранее, - это экстремистские проявления. В ФЗ это названо экстремисткой деятельностью. Следовательно, согласно логике, мы можем провести знак равенства между экстремисткой деятельностью и проявлениями экстремизма. Терроризм (указан среди экстремистской деятельности в ФЗ) тоже является проявлением экстремизма.

Каким образом мы можем провести границу между «радикализмом» и «экстремизмом»? В научной среде термин «радикализм» первоначально применялся для того, чтобы охарактеризовать стремление дойти до корня социальных проблем, хотя в настоящее время чаще используется для обозначения комплекса политических идей и действий, нацеленных на коренное (радикальное) изменение существующих социальных и политических институтов [8]. Считалось, что именно экстремизм сопряжен с насилием. В Стратегии же понятия путаются. Т.е. радикалы автоматически представляются как сторонники насилия, термин «радикализм» насыщен негативной коннотацией. С.А. Сергеев считает, что термин «радикализм» отражает крайность взглядов, но не сопряжен с насилием [9]. Возникает, по нашему мнению, ситуация подмены понятий.

Основным средством распространения Стратегия называют Интернет. Опять же трудно согласиться с тем, что это просто «средство коммуникации». Как нам кажется, Интернет-экстремизм – это отдельный вид экстремисткой активности. Законодатель не в полной мере осознает воздействие Интернета, его собственную методологию, выраженную в способах воздействия, что никак не вяжется с «коммуникативным средством». К примеру, сообщества «групп смерти», построенных по типу вовлечения в «игру», хотя связи между самоубийствами детей и деятельности данных сообществ до сих пор не установлены. Мы даже до конца не можем сказать, что возникло первым – недостоверная информация СМИ о «группах смерти», или сами группы смерти; связаны ли «кураторы» внутренней организацией, или нет. В том, что Интернет сейчас по-особому влияет на реальность, не возникает никаких сомнений, однако это может быть связано с молодостью явления. Следовательно, необходимо более глубокое изучение данного феномена. Пока же мы видим одинаковый подход к экстремизму в интернете и вне его. [11]

А теперь перейдем к практической стороне вопроса –к экспертизе экстремистских материалов.

В гуманитарной экспертизе речь идет о специальных исследованиях, которые, как правило, требуются в рамках антиэкстремистского законодательства. Законодателю или правоприменителю важно определить, является текст разжигающим ненависть и рознь или нет, и таким образом установить его предположительно экстремистскую направленность [12].

Диагностически значимыми свойствами проверяемого на экстремизм текста являются:

- Целенаправленность деятельности автора по созданию текста, ее произвольность, осмысленность;
- Публичность речевой деятельности;
- Наличие в тексте призывов к деяниям;
- Наличие в тексте пропаганды
- Наличие в тексте оправдания (терроризма) или обоснования экстремисткой деятельности
- Направленность речевых действий (текста) на возбуждение розни, вражды, ненависти унижение достоинства человека по определенным признакам [13].

Таким образом, анализ того, что именно сказано, не должен подменяться общими рассуждениями на тему «Что автор хотел этим сказать». Е. И. Галяшина также замечает, что представители органов власти не являются социальной группой, а критика власти не может быть экстремизмом [14], в особенности когда данная критика происходит СМИ. В обоснование позиции приводится положения ст.3 и 4 Декларации о свободе политической дискуссии в средствах массовой информации [15]. На эту же Декларацию ссылается Верховный Суд РФ в Постановлении Пленума.

Постановление ЕСПЧ указывает в первую очередь на важность принятия судом самостоятельного решения, которое должно быть основано на всех предъявленных доказательствах. Суд не может вынести обвинительный приговор, потому что «так сказала экспертиза», что по факту произошло в деле Дмитриевского и многих других. Экспертиза в свою очередь не может давать правовую оценку «является или не является данное высказывание экстремистским», или «содержит ли оно признаки экстремизма». Этот вопрос ставит суд перед собой, а не перед экспертом. Задача эксперта, по нашему мнению, состоит в расшифровке символики, сложного, специального текстового материала.

В качестве итога хотелось бы поразмышлять о политическом и социальном в экстремизме. Действительно, в теоретическом плане определение «экстремизма» зависит от того, что в данном государстве, обществе считается нормой, а что – отклонением и девиацией.

Экстремизм так или иначе может ассоциироваться у одних как «борьба за свободу», у других как «экстремизм» и «терроризм». А растяжимость деяний устанавливается на законодательном уровне. Распространением экстремистского материала может стать репост в социальной сети. Возможно, это и правильно, но почему ранее подобное не признавалось экстремизмом, а в

2012 году вдруг стало, пока не вызвало реакцию общества на совсем одиозные случаи в отношении и материала, и способа его распространения, что повлекло, наконец, изменения судебной практики при непосредственном участии Верховного Суда РФ. За 2015 год количество зарегистрированных преступлений экстремистской направленности составило 1521, что приблизительно в 2,5 раза выше, чем в 2010. В Алтайском крае в 2017 году было зарегистрировано 45 преступлений, в 2018 всего 18 преступлений, а в 2019 – одно преступление за весь год и то не было раскрыто [16].

Реально позитивным является снижение числа регистрируемых фактов экстремизма после поправок от 2018 года к Постановлению Пленума, что в свою очередь вызвано реакцией общества и пояснительным решением ЕСПЧ.

Необходимо затрачивать больше ресурсов на просвещение граждан в части объяснения, что есть экстремизм. Экстремизм ассоциируется в общественном сознании в первую очередь с причастностью к террористической деятельности, проповедованием нетерпимости в отношении представителей других национальностей или рас, поддержкой идей фашизма и насильственных методов борьбы. [17]

Список литературы:

1. «Конституция Российской Федерации» (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) // Сайт «Консультант Плюс» [Электронный ресурс]

2. «Конвенция о защите прав человека и основных свобод» (Заключена в г. Риме 04.11.1950) (с изм. от 13.05.2004) (вместе с «Протоколом [N 1]» (Подписан в г. Париже 20.03.1952), «Протоколом N 4 об обеспечении некоторых прав и свобод помимо тех, которые уже включены в Конвенцию и первый Протокол к ней» (Подписан в г. Страсбурге 16.09.1963), «Протоколом N 7» (Подписан в г. Страсбурге22.11.1984)) // Сайт «Консультант Плюс» [Электронный ресурс]

3. Декларация о свободе политической дискуссии в средствах массовой информации (принята Комитетом Министров Совета Европы 12 февраля 2004 г. на 872-м заседании Комитета Министров на уровне постоянных представителей) // Сайт «Консультант Плюс» [Электронный ресурс]

4. Федеральный закон от 25.07.2002 N 114-ФЗ (ред. от 31.07.2020) «О противодействии экстремистской деятельности» // Сайт «Консультант Плюс» [Электронный ресурс]

5. Указ Президента РФ от 29.05.2020 N 344 «Об утверждении Стратегии противодействия экстремизму в Российской Федерации до 2025 года» // Сайт «Консультант Плюс» [Электронный ресурс]

6. Постановление Пленума Верховного Суда РФ от 28.06.2011 N 11 (ред. от 20.09.2018) «О судебной практике по уголовным делам о преступлениях экстремистской направленности» // Сайт «Консультант Плюс» [Электронный ресурс]

7. Галяшина Е.И. «Лингвистика vs экстремизма: В помощь судьям, следователям, экспертам» / под ред. проф. М.В. Горбаневского. М.: Юридический мир, 2006. Стр.9-10

8. Галяшина Е.И. «Экспертиза экстремистских материалов: проблемы методического и информационного обеспечения» // Журнал «Вестник университета имени О.Е. Кутафина (МГЮА)» 07.2018. Стр.26-41.

9. Сергеев С. А. Исследования экстремизма и радикализма в зарубежных и отечественных социальных науках [Электронный ресурс], URL:http://kpfu.ru/docs/F110664239/Statya.Ekstremizm.radikalizm.sokr.bibliograf.pdf.

10. Чудинов С.И. «Экстремизм и научный образ экстремизма: столкновение мировоззренческих парадигм»// Журнал «Теория и практика общественного развития» 2014 г., №18, стр.159-161

11. Backes U. Meaning and Forms of Political Extremism in Past and Present // Central European Political Studies Review. 2007. Autumn.Vol. IX. Part 4. P. 242–262

Соколов Александр Сергеевич, старший преподаватель кафедры уголовного процесса и криминалистики юридического института АлтГУ, г. Барнаул
Федосова Анастасия Сергеевна
Юридический институт, АлтГУ, г. Барнаул

Соколов А.С., Федосова А.С. ЭКСТРЕМИЗМ В СЕТИ «ИНТЕРНЕТ»

Большинство экстремистских преступлений в России совершается в Интернете, в 2019 году они составили порядка 80% от общего числа подобных преступлений. В Алтайском крае с начала 2020 г. выявлено уже более 190 случаев «экстремизма» в Интернете. Так, например, в Алтайском крае А. была привлечена к уголовной ответственности по ст. 282 УК РФ за сохранение видео экстремистского содержания, выражающее ненависть и вражду, а также унижение достоинства группы лиц по признаку мусульманской народности. Ленинский районный суд признал её виновной и назначил наказание в виде штрафа.

Стоит отметить, что экстремистские проявления распространены в большей степени в молодежной среде, это связано с тем, что такой социально-возрастной группе свойственна психология максимализма и подражания. Молодежный экстремизм как массовое явление выражается в пренебрежении к действующим в обществе правилам и нормам поведения.

Основная цель экстремизма - навязывание определенных убеждений населению и привлечение как можно больше единомышленников в свои организации. Возникает вопрос, где это можно сделать в современном информационном обществе?

В наши дни информационное пространство сети «Интернет» используют различные экстремистские и террористические организации, радикально настроенные группировки с целью вербовки молодежи для претворения в жизнь идеологии экстремистской направленности. Так, в г. Барнаул, гражданин Б. был привлечён к уголовной ответственности по ст. 282.1 УК РФ за участие в экстремистском сообществе, суд признал, что информация, распространяемая гражданином Б. на Интернет-сайте по сетевому адресу, распространение которой на территории Российской Федерации запрещено.

Распространение молодежного экстремизма в сети «Интернет» является острой проблемой для «мирных» граждан. Увеличивается количество преступлений, поднимается уровень насилия, экстремизм становится более жестоким и профессиональным. Элементы экстремистского поведения молодежи формируются на фоне деформации социальной и культурной жизни общества. В перечень основных причин роста экстремистского поведения

молодежи исследователи склонны включать следующие: социальное неравенство, желание самоутвердиться в мире взрослых, недостаточную социальную зрелость, а также недостаточный профессиональный и жизненный опыт, а, следовательно, и сравнительно невысокий (неопределенный, маргинальный) социальный статус. Проблема занятости молодежи стала одной из самых сложных социальных проблем, так как риск безработицы особенно опасен среди выпускников учреждений профессионального образования, что происходит из-за недостаточной ориентации системы образования на рынок труда, низкого уровня работы по профессиональной ориентации. По статистике основная масса таких тяжких преступлений, как убийство, нанесение тяжких телесных повреждений, разбой, терроризм, совершается лицами до 25 лет.

Сеть «Интернет» является идеальным инструментом пропаганды террористической и экстремистской деятельности, это связано с некоторыми характеристикам, которыми активно пользуются представители банд формирований и поддерживающие их лица [1]. К таким характеристикам относятся: возможность широкого охвата аудитории; анонимное размещение информации; высокая скорость и быстрый характер распространения материалов; возможность без каких-либо финансовых затрат анонимно создавать собственные пропагандирующие Интернет-ресурсы; допустимость использования представителями экстремистских группировок лазеек в несогласованности в законодательствах стран мира в области «компьютерного права» [7].

Все подобные Интернет-ресурсы ведут свою работу из-за рубежа и имеют международные доменные имена, а именно: «.com», «.org», «.info» [6].

Известным примером для Российской Федерации служит сайт чеченских сепаратистов «Кавказ-Центр», который успешно работал на шведских и американских серверах.

Для вербовки и создания привлекательного образа террористических организаций используются практически все популярные социальные сети и ресурсы: ВКонтакте, Одноклассники, Twitter, Youtube, Instagram. Более того, используются все возможности данных социальных сетей, а именно: массовые рассылки, размещение видео- и аудиоматериалов, фотографий, документов [3].

На сегодняшний день серьезную опасность для общества представляют сайты, откровенно проповедующие идеи экстремизма и терроризма. В основном это социальные сети: ВКонтакте и Одноклассники. Например, в сети ВКонтакте было сообщество под названием «Тёмная сторона реальности», описание группы которого призывало в «мир религиозной паранойи», где пропагандируется идея против – масонов, Сатаны, Путина, и «прочей нечисти». Через такие ресурсы международные террористические организации практически беспрепятственно осуществляют пропаганду радикальных течений ислама, проповедующих борьбу с «неверными», «создание всемирного халифата» и т.д.

Необходимы средства для борьбы с проявлением экстремизма в Интернете. В российском законодательстве используются соответствующие нормы в уголовном и административном кодексах [5]. Но для блокирования экстремизма, как уголовного проявления, следует совершенствовать правовую базу, укреплять деятельность специальных служб, а также активизировать идеологическую работу [4].

Выходом из сложившейся ситуации является проведение последовательной работы по следующим направлениям:

- совершенствование нормативно-правовой базы на основе мониторинга зарубежного законодательства. Для примера, можно рассмотреть законодательство Великобритании. Первой особенностью английского законодательства является отсутствие специализированного законодательства в области противодействия экстремизму. Второй отличительной особенностью является полное отождествление экстремизма с терроризмом. В Соединенном Королевстве по этой причине в данной области были приняты и действуют следующие нормативно-правовые акты: Закон «О терроризме» 2000 г.; Закон «О противодействии терроризму, преступности и безопасности» 2001 г.; Закон «О предотвращении терроризма» 2005 г.; Закон «О борьбе с терроризмом» 2006 г. В рамках этих нормативно-правовых актов к террористической деятельности, помимо совершения самих террористических актов, относятся несообщение властям об акциях террористической направленности, укрывательство самих террористов, материальная поддержка террористов;
- разработка эффективных технических средств противодействия распространению идей экстремизма в сети «Интернет»;
- международное сотрудничество и обмен передовым опытом;
- подготовка соответствующих профессиональных кадров, способных противостоять современной преступности.

На уровне государства для решения указанной проблемы была разработана Стратегия противодействия экстремизму в РФ до 2025 года, которая предусматривает ряд направлений в деле противодействия экстремизму в сфере образования и государственной молодежной политики, в числе которых:

- включение в региональные и муниципальные программы по развитию образования и воспитанию учащейся молодежи мероприятий по формированию у подрастающего поколения уважительного отношения ко всем этносам и религиям;
- организация досуга детей, подростков, молодежи, семейного досуга, обеспечение доступности для населения объектов культуры, спорта и отдыха, создание условий для реализации творческого и спортивного потенциала, культурного роста граждан;
- осуществление мер государственной поддержки системы воспитания молодежи на основе традиционных для российской культуры духовных, нравственных и патриотических ценностей.

Таким образом, отдельные проявления экстремизма, сопряженные с использованием сети Интернет, представляют реальную угрозу

информационной безопасности не только общества, но и государства. Экстремистская деятельность в сети «Интернет» может рассматриваться как проблема общегосударственного значения и угроза национальной безопасности страны. Практически во всех странах мира ведется интенсивная борьба против информационного экстремизма, но актуальным остается вопрос об эффективности данной работы.

Список литературы:

1. О противодействии экстремистской деятельности: федеральный закон от 25.07.2002 № 114-ФЗ [Электронный ресурс] // URL:http://www.consultant.ru/document/cons_doc_LAW_37867/ (дата обращения: 21.10.2020).

2. О защите детей от информации, причиняющей вред их здоровью и развитию : федеральный закон от 29.12.2010 № 436-ФЗ [Электронный ресурс] // URL: http://www.consultant.ru/document/cons_doc_LAW_108808/(дата обращения: 22.10.2020).

3. Борисов С.В. Сущность преступлений экстремистской направленности / С.В. Борисов / / Мировой судья. - 2019. - №4. - С. 12 - 15. 4. Валеев, А.Х. Борьба с проявлением экстремизма в сети интернет / А.Х. Валеев // Бизнес в законе.- 2019. - №6. - С. 125.

5. Герасимов Б.М. Проблемы российского информационного законодательства / Б.М. Герасимов // Информационные ресурсы России. - 2018. - № 6. - С. 12.

6. Доника Е.Е. О некоторых проблемах противодействия экстремизму в России на современном этапе / Е.Е. Доника // Труды Академии управления МВД России. - 2020. - №3. - С. 6 - 8.

7. Кубякин Е.О. Основания социологического обоснования феномена экстремизма / Е.О. Кубякин // Экстрем-парантность: монография. - Краснодар, 2019.

Акимова Диана Алексеевна
Юридический институт,
АлтГУ, г. Барнаул.
Научный руководитель: Соколов Александр Сергеевич,
старший преподаватель кафедры уголовного процесса и криминалистики,
Юридический институт АлтГУ, г. Барнаул

Акимова Д.А. СОВРЕМЕННЫЕ КАНАЛЫ ФОРМИРОВАНИЯ И РАСПРОСТРАНЕНИЯ ИДЕЙ ЭКСТРЕМИЗМА И ТЕРРОРИЗМА В МОЛОДЕЖНОЙ СРЕДЕ

В ходе информационной революции Российская Федерация столкнулась с новым вызовом глобальной безопасности - это превращение интернет - ресурсов, социальных сетей, видеохостингов и видеоигр (в том числе версий, предоставленных в форме мобильных приложений) в пропагандистское и вербовочное оружие радикальных группировок.

Актуальность исследуемой темы подтверждается данными Генеральной прокуратуры о состоянии преступности в России (за январь-сентябрь 2020 года), согласно которым больше половины от всех «киберпреступлений» совершается с использованием сети «Интернет», в том числе почти 60 % преступлений экстремистской направленности, при общем увеличении их числа более чем на 40%.

Обращает на себя внимание и увеличение числа преступлений террористического характера (+21,7 %).

На фоне непростой социально-экономической обстановки значительную угрозу представляет собой сетевой экстремизм, подчеркнул заместитель председателя Совета Безопасности Дмитрий Медведев в ходе совещания о тенденциях развития криминогенной обстановки.

Действительно, распространение в обществе радикальных настроений в связи с психологическими последствиями «локдаунов», в том числе депрессией, социальной изоляцией, утратой источников дохода и другими факторами, способствует уходу экстремистов и террористов в онлайн - пространство.

Пандемия ненависти, коронавирусный экстремизм в Интернете – вот, что, по нашему мнению, может послужить причинами массового нарушения общественного порядка и безопасности, именно поэтому необходимо изучить каналы формирования и распространения радикальных идей для организации последующей работы по устранению и предупреждению угроз экстремизма и терроризма в киберпространстве.

Одним из объектов деятельности экстремистской и террористической организации являются сайты, которые имеют, как правило, оригинальный дизайн, простую навигацию и доступный способ поиска информации. Идеологические установки транслируются через информационную ленту, которая преподносит нужную интерпретацию событий в стране и в мире, статьи и аналитические материалы обычно пишутся в таком же ключе. Для того чтобы случайный посетитель ресурса заинтересовался информацией, она ярко оформляется, заголовки новостей имеют провокационный характер. Сайты стараются держать своих читателей в эмоциональном напряжении, так как степень вовлечения в экстремистскую деятельность зависит от того, насколько часто и долго респондент проводит время на этих ресурсах.

Также объектом внимания радикальных организаций являются социальные сети, число пользователей которых по данным Газеты.RU, составляет порядка 90 миллионов человек (73% от всего населения страны).

Загрузка и формирование медиаконтента с целью воздействия на интернет-пользователей и получения от них ответной «нужной» реакции является мощным инструментом, поскольку данный контент психоэмоционально воздействует на личность. Под видом обмена мнениями экстремисты увеличивают количество «сочувствующих», используя в своих целях несформировавшееся сознание молодого поколения. Они также используют социальные сети для мониторинга личной информации, вводимой пользователем при регистрации на сайте, или в различного рода интернет-опросах и анкетах, по которым можно судить о политических установках, отношении респондента к действующему политическому режиму. С пользователями, которые представляют интерес, устанавливается контакт в целях их дальнейшего задействования в антиобщественной деятельности, исходя из степени внушаемости, управляемости, готовности нарушать закон. В социальных сетях создаются закрытые группы, в которых распространяются материалы экстремистской направленности, участникам сообщаются сведения о месте и времени проведения акций и осуществляется координация деятельности экстремистских группировок.

Наиболее уязвимыми для вербовки со стороны экстремистов, как уже было упомянуто ранее, становятся молодые люди, имеющие ряд социальных проблем, склонность к созависимому поведению, испытывающие влияние психологических факторов в силу возраста, таких как обострённое чувство справедливости, поиска смысла и ценности жизни. Крайне просто и лаконично, на доступном языке формулируется основная конфликтная тема, носящая этнический, религиозный или иной характер, создаются слоганы, мемы и демотиваторы, которые эмоционально заряжают молодых людей.

Согласно данным социологических исследований [1, 2, 3] видеохостинг YouTube, популярные социальные сети (Facebook, Twitter, «ВКонтакте», «Одноклассники», Instagram и др.) и мессенджеры (WhatsApp, Telegram и др.), в которых есть возможность по шифрованному каналу связи создавать группы и участвовать в обмене информацией с другими пользователями на различные

темы, являются каналами формирования и распространения идей и материалов экстремистского характера.

Mediascope представила данные об аудитории интернета в России в 2020 году [4], на их основе мы приводим ТОП -5 наиболее популярных социальных сетей в России (Рис.1):

– YouTube. Охват аудитории 82,8 млн. За просмотром видео пользователи проводят 40-50 минут в день.

– ВКонтакте. Платформа ежемесячно охватывает 73 млн. пользователей и каждый из них проводит в соцсети 30-35 минут.

– Instagram. Охват аудитории 59,4 млн. пользователей. В среднем в Instagram россияне проводят 26 минут в день.

– «Одноклассники». Охват аудитории 50,2 млн. россиян. Средняя продолжительность сессии составляет 22 минуты.

– Facebook. Ею ежедневно пользуются порядка 39 млн. россиян, но проводят они на платформе всего 9 минут.

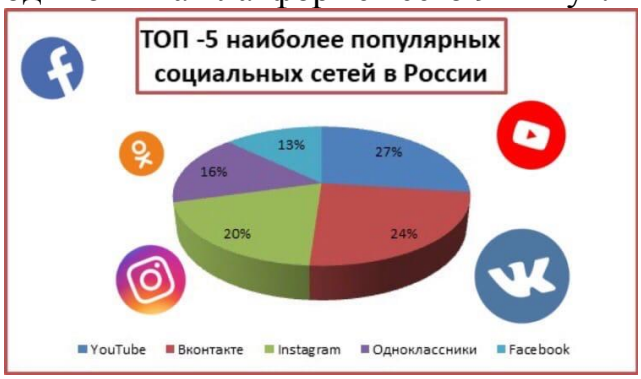

Рис.1

Что касается распространения идей и материалов террористического характера, то оно осуществляется чаще всего в таких мессенджерах, как Telegram, Viber, WhatsApp и Skype, ими пользуются террористические организации, в том числе и запрещённое в России ИГИЛ.Конкретный механизм, как работают вербовщики в данных мессенджерах: на первом этапе они выявляют людей, наиболее склонных к информационной обработке, затем начинают дружеское непринуждённое общение с ними, а потом переводят общение в закрытые группы. Стойкое end-to-end шифрование позволяет членам закрытых групп общаться практически в режиме абсолютной конфиденциальности, поскольку постороннее лицо не может получить информацию о переписке или звонке.

Отметим, что Telegram больше двух лет оставался заблокирован в России - с апреля 2018 года по июнь 2020 года. Несмотря на попытки заблокировать приложение, Telegram продолжал преимущественно стабильно работать в России, а официальное пользование им предоставили только в этом году после того, как основатель Telegramвысказал готовность к противодействию терроризму и экстремизму.

Особое внимание следует уделить новому объекту радикальных организаций - самой быстрорастущей в мире платформе Tik-Tok. Ежемесячный

охват в России составляет 20,2 млн. и сессия в среднем длится не меньше 20 минут (Рис.2).

Рис.2

Приложение позволяет пользователям загружать и просматривать короткие синхронизированные по губам видео с простым в использовании интерфейсом. В то время как многие пользователи стремятся только загружать юмористические и развлекательные мемы, другие используют приложение для распространения идей ненависти. Экстремисты не случайно выбрали эту площадку, ведь дети и подростки – это совсем другая аудитория, из которой вербуют и привлекают тех, кто сможет стать «будущими бойцами», следующим поколением экстремистов. Хотя в условиях предоставления услуг TikTok сказано, что пользователи не могут загружать какой-либо контент, который является подстрекательским, оскорбительным, ненавистническим, дискриминационным, расистским, сексистским, антагонистическим или преступным, приложение ещё не обеспечило соблюдение этих правил [5].

На основе данных «Центра мониторинга молодёжной среды» в социальной сети ВКонтакте ежедневно регистрируется около 5 интернет - формирований, пропагандирующих деструктивную идеологию. И таких сообществ только в социальной сети ВКонтакте более 2,5 тысяч и в них состоят почти 35 млн. активных пользователей.

В качестве мер противодействия экстремизму в социальных сетях и мессенджерах государственными органами и некоммерческими организациями (НЦПТИ, Центр изучения и сетевого мониторинга молодежной среды и другими) осуществляется большая работа по различным направлениям: разработка и совершенствование законодательной базы, направленной против использования интернета в экстремистских и террористических целях; информационное противодействие молодежному экстремизму посредством интернет-мониторинга, позволяющего в режиме реального времени осуществлять компьютерный контент-анализ, лингвистический анализ текстовых потоков, содержащих различные материалы экстремистского характера.

Исходя из высокого уровня опасности, которую представляет социальная сеть ВКонтакте, в рамках проведённого исследования нам удалось принять участие в проекте «Интернет без угроз» (Рис 3).

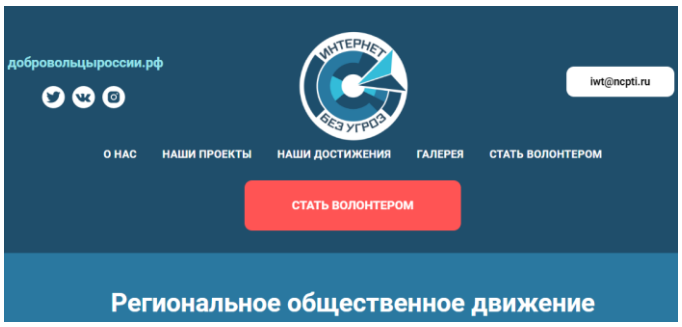

Рис 3.

Сотрудники центра заинтересовались нашим исследованием и предложили подготовить заключение по присланным материалам.

По результатам анализа для передачи в правоохранительные органы с целью последующей блокировки было отобрано 16 ссылок.

Искренне надеемся, что наше плодотворное и взаимовыгодное сотрудничество с Национальным Центром информационного противодействия терроризму и экстремизму в образовательной среде и сети Интернет будет продолжено.

По информации «Новостей ООН», экстремисты также используют видеоигры с целью радикализации и вербовки представителей молодого поколения.

Ниже приводим обновлённый перечень запрещённых на территории России электронных игр и вредоносные идеи, которые при помощи их распространялись [6]:

- «FarCry» — насилие, вандализм;
- «The Masquerade - Bloodlines 2» —насилие;
- «Half-Life 3» — насилие, распространение лженаучных сведений;
- «Counter-strike» — пропаганда терроризма и американского милитаризма;
- «Assassin's Creed: Lineage» — искажение исторической действительности, неверное истолкование принципов российско-китайского партнёрства;
- «Grand Theft Auto V» — романтизация преступности;
- «Red Dead Redemption» — воспевание ценностей американского империализма;
- «Heroes of Might and Magic III» — финансовыйфетишизм, оккультизм;
- «Call of Duty» — извращение внешней политики России, насилие, американский милитаризм.

В России целесообразно ввести ограничения, касающиеся распространения компьютерных игр, заявил в эфире радиостанции "Говорит Москва" председатель общероссийской общественной организации "Право на оружие" Вячеслав Ванеев.

Поводом послужила информация, что 18-летний «стрелок» из Нижегородской области, 12 октября 2020 года, убивший троих человек, увлекался компьютерными играми [7].

По нашему мнению, большинство видеоигр действительно носят деструктивный характер, пропагандируя насилие, экстремизм и терроризм они

отрицательно влияют на ещё только формирующуюся психику молодых людей, и порой степень разрушения бывает настолько высокой, что у молодёжи возникает желание воспроизвести сюжет игры в реальном мире, именно этим и пользуются радикальные группировки и организации. Для того чтобы не допустить этого следует незамедлительно ограничивать доступ к определённому числу видеоигр не только на официальном сайте, но и на сторонних ресурсах.

Итак, механизм формирования идей экстремистской и террористической направленности выглядит следующим образом:

1. Выявление конфликтного потенциала и существующих противоречий между различными социальными группами;
2. Выделение социальных групп, общественнополитических объединений, способных стать стихийным инициатором (проводником) волны протеста. На эту роль могут подходить «легко воспламеняемые» группы (в частности молодежь);
3. Комплексная подготовка выделенных групп к дальнейшим активным действиям, определение основных модераторов;
4. Адаптация реальных целей в соответствии с мерой понимания выбранных групп и их модераторов (возможна подмена понятий, навязывание ложных целей). Внушение им уверенности в практической осуществимости поставленных задач;
5. Обеспечение информационного превосходства навязываемых идей (вбрасывание информации в целевую среду, ее «разгон» и т.д.);
6. Дальнейшее расширение контингента активных участников за счет обострения конфликтной ситуации, дестабилизации обстановки.

Обобщая все выше сказанное, можно сделать вывод о том, что в современном мире установки и ценности, в особенности, молодых людей формируются посредством общения, получения информации в Интернет-ресурсах, времяпровождения за компьютерными играми.

Понимая это, идеологи экстремизма и терроризма активно воздействуют на сознание молодёжи, используя социальные сети, возможности информационной коммуникации в мессенджерах, которые позволяют размещать в свободном доступе экстремистские и террористические материалы и также быстро распространять их через репосты и лайки, что обеспечивает охват относительно большой аудитории за очень короткую продолжительность времени.

Для предотвращения формирования и распространения экстремистского и террористического контента информационным источникам необходимо осуществлять запрет на просмотр деструктивных материалов путем блокирования этих ресурсов, производить сокрытие результатов поиска данного контента по ключевым словам в поисковой системе, вести мониторинг сетей, совершенствовать уже существующие и разрабатывать новые технические и программные средства, позволяющие отслеживать и оценивать информацию, а также определять её источник.

Для успешной борьбы с проявлениями экстремизма и терроризма в сети Интернет необходим комплекс мер, который включает в себя совершенствование существующего законодательства, регулирующего отношения по размещению, хранению и распространению информации в сети Интернет, повышение взаимодействия правоохранительных органов с провайдерами, организаторами и создателями сайтов, групп и блогов, активное взаимодействие с общественностью, в том числе проведение разъяснительной работы с пользователями сети Интернет, привлечение их к участию в поиске противоправного контента, увеличение пропаганды антиэкстремизма и антитерроризма.

Чтобы не стать объектом для манипуляции со стороны экстремистов, мы рекомендуем придерживаться следующих правил:

1. Не публикуйте информацию о себе и своих родственниках: вера, политические взгляды и т. д;
2. Не указывайте свой номер телефона и адрес проживания;
3. Не делитесь важной информацией и событиями, которые происходят в вашей жизни, на всеобщее обозрение;
4. Не вступайте в диалог с незнакомыми людьми;
5. Ограничьте доступ к своим фотографиям, записям и другим материалам и сделайте их доступными лишь для людей, которых хорошо знаете;
6. Не вступайте в группы, которые кажутся подозрительными;
7. Не будьте слишком откровенны в комментариях к темам, обсуждаемым общедоступными группами и сообществами;
8. Используйте опцию «Чёрный список» и возможность отправить жалобу модератору сети или администратору группы;
9. Внимательно относитесь к компьютерным играм, учитывайте их реальную опасность для вашего психического здоровья;
10. Будьте внимательны, когда кто-то проявляет к вам повышенный интерес и помните: первичный отбор «кандидатов» осуществляется по исследованию информации, которую вы сами выкладываете на личных страничках в социальных сетях и других интернет - ресурсах.

Список литературы:

1. ВЦИОМ: Социальные сети: кто туда ходит и зачем? [Электронный ресурс]. URL: https://wciom.ru/index. php?id=236&uid=1457
2. Пользователи соцсетей в России: статистика и портреты аудитории [Электронный ресурс]. URL: https://rusability.ru/internetmarketing/polzovateli-sotssetej-vrossii-statistika-i-portrety-auditorii
3. Тренды русскоязычных соцсетей – 2019 . Исследование. [Электронный ресурс]. URL: https://rusability.ru/news/trendyrusskoyazychnyh-sotssetej-2019-issledovanie
4. ТОП-10 Ресурсов [Электронный ресурс]. URL: https://webindex.mediascope.net/top-resources/projects

5. ТИК-ТОК ИЗОБИЛУЕТ РАСИСТСКИМ, АНТИСЕМИТСКИМ КОНТЕНТОМ, НАПРАВЛЕННЫМ НА ДЕТЕЙ [Электронный ресурс]. URL: https://center-profilaktika.ru/2020/06/19/тик-ток-изобилует-расистским-антисем/

6. Представлен обновлённый список запрещённых в России игр [Электронный ресурс]. URL: https://4pda.ru/2019/03/31/356708/

7. Правозащитники предложили запретить некоторые компьютерные игры в России [Электронный ресурс]. URL: https://ria.ru/20201013/igry-1579617613.html

Высоцкая Кристина Владимировна
Юридический институт, АлтГУ,
г. Барнаул
Научный руководитель: Соколов Александр Сергеевич,
старший преподаватель кафедры уголовного процесса и криминалистики,
Юридический институт АлтГУ, г. Барнаул

Высоцкая К.В. ПРОФИЛАКТИКА ЭКСТРЕМИЗМА И ТЕРРОРИЗМА В МОЛОДЕЖНОЙ СРЕДЕ

В современном мире проблема борьбы с экстремизмом и его крайним проявлением – терроризмом признается как в России, так и за рубежом, особенно значимой и актуальной. Прежде всего, это связано с модернизацией общественной жизни, изменением системы ценностей и активным протеканием процессов глобализации, которые приводят к усложнению структурных связей отдельных групп населения и всего общества в целом. Эти, и другие факторы приводят к усилению межнациональной напряженности и, как следствие, появлению оппозиционных групп, которые пытаются добиться желаемых для них результатов через экстремизм и терроризм.

Чаще всего данному негативному явлению подвержена молодежь, т. к. именно в этой социально-демографической группе, не имеющей прочных идеологических установок, эффективнее приживаются радикальные взгляды и убеждения. Экстремистские и террористические организации активно используют ее в своих интересах, что свидетельствует о недостаточной социальной адаптации молодежи, развитии асоциальных установок в ее сознании, вызывающих противозаконные образцы поведения.

Как показывает мировой и российский опыт борьба с распространением молодежного экстремизма, при отсутствии четкой программы профилактики этого явления не дает необходимого эффекта [1]. В настоящее время необходимость предупреждения распространения экстремистских настроений в молодежной среде является заботой не только государства, но и всего общества в целом.

Для успешной разработки методов профилактики экстремизма и терроризма в молодежной среде необходимо понимать сущность данных явлений.

Экстремизм (от лат. extremum – крайнее) – это теория и практика достижения социально-политических, религиозных, национальных целей посредством «крайних», запрещенных способов [2, с. 7]. Среди молодого поколения он проявляется в деформации сознания, увлеченности радикальным взглядам, нетрадиционными (новыми) религиозными доктринами и, как

следствие, совершении противоправных действий в соответствии со своими убеждениями.

Среди причин возникновения этого явления в молодежной среде можно выделить такие, как снижение жизненного уровня большей части населения и изменение нравственных ценностей, усиление подростковой агрессии, вызванной неэффективной воспитательной системой, и отсутствие действенной социальной профилактики экстремизма. Росту экстремизма способствует и такой фактор, как распространение в СМИ экстремистских материалов (в особенности в сети Интернет, в которой в настоящее время активно пропагандируется идеология экстремизма, призывы к совершению преступлений против людей другой национальности, вероисповедования и т. д.). К причинам проста экстремистского поведения среди молодежи можно отнести: «недостаточную социальную зрелость; желание самоутвердиться; недостаточный профессиональный и жизненный опыт; невысокий социальный статус» [3]. Обострение данных факторов актуализирует проблему профилактики молодежного экстремизма.

Поскольку терроризм как наиболее опасная форма организованной преступной деятельности является видом экстремизма можно предположить, что причины возникновения данных явлений идентичны. К ним также можно отнести отсутствие положительных идеалов у молодежи, неверие в свои силы, чувство безысходности в случае неудовлетворительного стечения обстоятельств, озлобленность и направленность действий исключительно на личное благополучие.

Выявить конкретные причины или мотив, по которым лицо становится на террористическо-экстремистский путь, вряд ли возможно, однако можно обнаружить определенные закономерности. Так, членами неформальных организаций (группировок) экстремистской направленностью обычно становятся люди в возрасте от 14 до 30 лет, т. е. молодежь. Как уже отмечалось выше, именно этот возраст является наиболее подверженным воздействию радикальных взглядов и убеждений. Участие в данной деятельности в основном принимают лица мужского пола, но при этом девушки не являются исключением (на практике они нередко становятся лидерами). Также следует отметить, что участниками неформальных организаций (группировок) являются люди «… с хорошим образованием, знанием законов, умением конспирироваться, стрелять, заботиться о собственном здоровье» [2, с. 129].

Согласно статистике Министерства внутренних дел Российской Федерации (МВД РФ) за 2020 г. (с января по сентябрь) правоохранительными органами было зарегистрировано 1851 преступление террористического характера, что на 33,9% больше, чем год назад, и 651 преступление экстремистской направленности (+43,4%) [4]. Увеличение их количества говорит о необходимости разработки средств, приемов и методов раскрытия, расследования и предупреждения данных преступлений. При этом профилактика молодежного экстремизма становится главным методом борьбы

с распространением идеологии экстремизма, ведь именно верные воспитательные меры способны дать качественные результаты.

В этой связи основные мероприятия по снижению проявлений экстремизма и терроризма в молодежной среде должны быть направлены на улучшение социальной среды, в которой находятся молодые люди, посредством увеличения культурных благ и созданием массовых общественных молодежных организаций, которые бы воспитывали подрастающее поколение на положительных образцах. В том числе, необходимо оживить работу центров организованного досуга несовершеннолетних, способствующих патриотическому, духовно-нравственному, семейному и правовому воспитанию. При этом следует учитывать, что правовое воспитание – один из самых эффективных способов профилактики экстремизма и терроризма в молодежной среде. Способствовать его правильному формированию возможно благодаря, например, встречам и беседам подростков с представителями Министерства внутренних дел РФ, Прокуратуры РФ, Следственного комитета РФ и т. д. Такие мероприятия помогут сформировать устойчивое негативное отношение к преступной деятельности, включая экстремистские деяния.

Не менее важным является привлечение молодежи к участию в добровольческих (волонтерских) организациях, что позволит им реализовать себя как личность среди сверстников, воплотить жизненный потенциал. Также имеет большое значение разработка федеральных программ в области укрепления института семьи, работы с молодежью, распределение бюджетных средств в пользу данного направления (в настоящее время в Российской Федерации действуют такие программы, как «Дети России», «Молодая семья» и т. д.). Для предупреждения распространения экстремизма и терроризма необходимо ввести практику государственного регулирования трансляции телепередач, содержащих сцены насилия, нарушающих нормы морали и нравственности. В том числе, представляет особую важность профилактика в сети «Интернет». В этой связи могут быть предприняты такие меры, как 1) создание площадок (сайтов) для обсуждения проблем, связанных с экстремизмом и терроризмом в режиме «онлайн»; 2) контртеррористическая пропаганда на популярных сайтах (в особенности, в социальных сетях, активно используемых молодежью), опирающаяся на правдивые материалы и факты и предлагающая альтернативные варианты поведения; 3) совершенствование законодательной базы государства, которая опережала бы возможные противоправные действия в сети «Интернет» и т. д.

Изучение международной практики противодействия экстремизму и терроризму крайне важно для совершенствования методов и форм борьбы с данными явлениями.

Одной из характерных особенностей противодействия экстремизму в европейских странах является усиление мер ответственности за совершение преступлений экстремистской направленности и применение рекомпенсивных норм, способствующих привлечению к сотрудничеству лиц так или иначе причастных к преступной деятельности [5]. Большое внимание борьбе с

политическим экстремизмом уделяется в Германии, где проводятся различные превентивные мероприятия, применяются разнообразные методы борьбы с экстремистскими проявлениями при взаимодействии органов государственной власти с органами местного самоуправления и общественными организациями. В том числе в крупных городах США применяется метод интеграции в неформальные организации (группировки) социальных работников, которые пытаются переориентировать деятельность их членов с делинквентной основы на конструктивную. Но при этом стоит учитывать, что работа с такими объединениями требует специальной профессиональной подготовки.

Анализ зарубежной практики противодействия экстремизму и терроризму подтверждает тот факт, что борьба с данными явлениями – это задача не только государства, но и всего общества в целом. Лишь в случае взаимодействия государственных органов с институтами гражданского общества профилактика способна дать наилучший результат. Следует отметить, что опыт иностранных государств может быть полезен России для совершенствования правовых и социальных методов противодействия экстремизму и терроризму. Кроме того, необходимо активизировать международное сотрудничество в целях борьбы с данной проблемой посредством создания международных антиэкстремистских организаций и т. д.

На том же пути, что и зарубежные страны, находится Россия. В настоящее время разработана Стратегия противодействию экстремизму в Российской Федерации до 2025 г. в целях конкретизации положений Федерального закона от 25 июля 2002 г. № 114-ФЗ "О противодействии экстремистской деятельности", согласно которой противодействие предусматривается осуществлять в три этапа, один из которых, а именно второй (2016-2024 гг.), реализуется в данный момент. На этом этапе планируется: а) разработка и принятие законодательных и иных нормативных правовых актов РФ, субъектов РФ, направленных на решение задач в сфере противодействия экстремизму; б) выполнение мероприятий в соответствии с планом реализации Стратегии; в) мониторинг результатов; г) прогнозирование развития ситуации в области межнациональных и межконфессиональных отношений в РФ и возможных экстремистских угроз; д) обеспечение вовлечения институтов гражданского общества в деятельность, направленную на противодействие экстремизму; е) создание системы дополнительной защиты информационно-телекоммуникационных сетей, включая сеть «Интернет», от проникновения экстремисткой идеологии [6].

Следует отметить, что в Алтайском крае также активно ведется работа по противодействию экстремизму и терроризму. В конце 2019 года была утверждена такая государственная программа, как «Противодействие экстремизму и идеологии терроризма в Алтайском крае». В то же время молодежь со всего региона часто приглашают участвовать в различных научно-практических конференциях и фестивалях, посвященных борьбе с экстремизмом и терроризмом (среди них такие, как «Экстремизм и терроризм в киберпространстве – угрозы безопасности человечества», «Я против

экстремизма и терроризма» и др.). На территории региона нередко проводятся круглые столы, антитеррористические учения и пропаганды среди школьников и студентов, различные заседания и лекции о профилактике экстремизма и терроризма. Кроме того, решением данной проблемы занимает объединение «Кибердружина 22». Подтвердить эффективность данных мер можно благодаря статистике преступлений экстремистской направленности. За 2020 г. (январь-сентябрь) не было зарегистрировано ни одного преступления в данной сфере, за 2019 – всего одно, в то время как в 2018 – 18 и в 2017 – 45 [7].

Таким образом, экстремистское и террористическое движения представляют собой сложный феномен, имеющий тенденцию к увеличению и саморазвитию. Его появление обусловлено целым рядом социально-экономических, политических и социокультурных факторов, тесно связанных между собой. Поэтому в целях профилактики экстремизма и терроризма необходимо выработать системный подход, направленный на минимизацию совокупности данных факторов и содействующий росту влияния молодежных общественных организаций, выражающих интересы молодежи как социально-демографической и социокультурной группы.

Список литературы:

1. Довгяло В. К. Профилактика экстремизма в молодежной среде / В. К. Довгяло // Вестник Пермского государственного гуманитарно-педагогического университета, 2018. – Сер. Гуманитарные и общественные науки. – №1. – С. 21-30.

2. Назаров В. Л. Профилактика экстремизма в молодежной среде: учеб.пособие / Назаров, П. Е. Суслонов // М-во науки и высш. образования Рос. Федерации, Урал.федер. Ун-т. – Екатеринбург: Издательство Урал.ун-та, 2018. – 204 с.

3. Бааль Н. Б. Экстремистские молодежные организации в современной России / Н. Б. Бааль // История государства и права, 2007. – №17. – С. 4-6.

4. Состояние преступности в России за январь-сентябрь 2020 г. – М.: Министерство внутренних дел Российской Федерации ФКУ «Главный информационно-аналитический центр», 2020. – 65 с.

5. Кравцов Д. Ю. Практика противодействия экстремизму в разных странах / Д. Ю. Кравцов // NB: Административное право и практика администрирования, 2019. – №4. – С. 22-28.

6. Стратегия противодействия экстремизму в Российской Федерации до 2025 г. [Электронный ресурс]. – Режим доступа: https://тф.мосу.мвд.рф/document/21100691 , свободный.

7. Генеральная прокуратура Российской Федерации. Портал правовой статистики [Электронный ресурс]. – Режим доступа: http://crimestat.ru/regions_chart_total , свободный.

Богомолова Римма Михайловна
Юридический институт,
АлтГУ, г. Барнаул
Научный руководитель: Соколов Александр Сергеевич,
старший преподаватель кафедры уголовного процесса и криминалистики,
Юридический институт АлтГУ, г. Барнаул

Богомолова Р.М. ПРОТИВОДЕЙСТВИЕ ЭКСТРЕМИЗМУ И ТЕРРОРИЗМУ В ИНТЕРНЕТ-ПРОСТРАНСТВЕ

С каждым годом количество пользователей Интернета неуклонно растет. Так, по данным доклада Международного союза электросвязи (МСЭ) «Измерение цифрового развития: факты и цифры за 2019 год» более 53% населения Земли, что составляет 4,1 млрд. человек, имеют доступ к Интернету [1]. Также следует отметить, что по данным GlobalWebIndex на январь 2020 среднестатистический пользователь Интернета проводит в нем 6 часов 43 минуты в день. В России этот показатель составил 7 часов 17 минут [2]. Справедливо предположить, что с наступлением пандемии и переходе многих людей на дистанционную форму работы и обучения количество проводимых в Интернете часов увеличилось.

Такие особенности Интернета как анонимность коммуникаций, простота доступа, высокая скорость передачи информации, возможность коммуникации с огромной аудиторией, что обеспечивается тем, что большая площадь Земли уже имеет Интернет покрытия (в том же докладе МСЭ указано, что на 2019 год 96% населения Земли находятся в зоне доступа к мобильному цифровому сигналу. Для 93% это сеть 3G или более продвинутая. В Европе, Западном полушарии и Азиатско-Тихоокеанском регионе покрытие составляет 95%, в арабских странах - 91%, на пространстве СНГ - 88%, в Африке - 79%)[1]. Эти факторы способствуют росту количества преступлений совершаемых в информационном пространстве. На данный момент нередки преступления экстремистской и террористической направленности.

Для минимизации преступления экстремистской и террористической направленности в Интернете сейчас многими компаниями и государствами предусматриваются предупредительно-профилактические работы. Для этого проводится отслеживание, блокирование и ликвидация сайтов, видеороликов, пропагандирующих идеологию национализма, расизма, экстремизма, терроризма, призывающих к осуществлению экстремистской и террористической деятельности, а также содержащие инструкции по изготовлению взрывных устройств, используемых для проведения террористических актов [3].

Так, например, с 2017 года крупнейший видеохостинг,YouTube, начал осуществление предупредительно-профилактические работы. В том числе, началась активная блокировка видео, содержащих «подстрекающих религиозный, национальный контент», при переходе пользователя на подобного роды видео, стало появляться предупреждение. Авторы подобных видео больше не могли монетизировать просмотры. К тому же для пресечения вербовки потенциальных террористов начала действовать таргетированная реклама. То есть пользователи, которые по той или иной причине заинтересовались и вышли на данные ролики, перенаправляются на антитеррористические видео, которые возможно помогут осознать потенциальным террористам всю опасность их взглядов [4]. В исследовании проекта Jugendschutz.net, опубликованного в январе-феврале 2017 года, говорилось, что YouTube удаляет противоправный контент, на который поступили жалобы, в 90% случаев, Facebook — в 39%, а Twitter — всего лишь в 1% случаев.

Но по сравнению с YouTube , многими государствами уже давно были приняты меры по борьбе с терроризмом и экстремизмом в Интернете. Так, в Великобритании еще в 1990 году был принят акт, касающийся неправомерного использования компьютерных технологий. Стоит отметить, что правоохранительными органами Великобритании создана и функционирует доктрина противодействия экстремизму и терроризму в глобальной сети. Британское Национальное подразделение по борьбе с терроризмом в сфере Интернета (CTIRU) разместило обращение к населению, в которой попросило сообщать о наличии в Интернете материалов, содержащих информацию экстремистского и террористического характера. Для этого на веб-ресурсах действует красная кнопка под названием «Стоп». При нажатии пользователем данной кнопки, провайдеры перенаправляют его на специальный сайт, где просят ввести адрес веб-страницы, на которой был обнаружен подозрительный материал на условиях анонимности. CTIRU анализирует и проверяет полученную информацию и в течение 36 часов осуществляет удаление материала, в случае, если он признается экстремистским. CTIRU работает в постоянном сотрудничестве с провайдерами, что позволило ему добиться высоких результатов [3].

По данным на 2016 год все детские учреждения или организации, предоставляющие в Великобритании услуги по уходу за детьми или детские услуги, обязаны гарантировать, что их система технологий предотвращает доступ к сайтам, включенным в список CTIRU [5].

Если обратиться к опыту США в противодействии экстремизму и терроризму, то с 2001 года действовал Закон о борьбе с терроризмом (также используется акроним *USA PATRIOT Act*). Он был принят после террористических актов 11 сентября 2001 года и, в частности, расширил права ФБР по подслушиванию и электронной слежке [6]. Был введен новый документ – письмо-требование о раскрытии персональной конфиденциальной информации в целях национальной безопасности. Отличием письма от

судебного ордера являлось то, что оно могло быть написано ФБР или иной службой самостоятельно, без решения судьи [3]. При наличии такого письма, ФБР могло получить доступ к любым данным пользователя и запретить руководству компании сообщать ему об этом. С 2015 года «Патриотический акт» был заменен федеральным законом, получившим название «Акт о свободе» (*USA Freedom Act*). Закон запрещает спецслужбам США вести за американскими гражданами электронную слежку [7]. С одной стороны может показаться, что Акт о свободе стал значительным послаблением в американском законодательстве, ведь был принят после событий разоблачений, сделанных со стороны бывшего сотрудника ЦРУ и АНБ Эдвард Сноудена, который обнародовал сведения, вызвавшие большой скандал и осложнили отношения США со своими союзниками. Но при тщательном рассмотрении Акта обнаруживается, что главными лоббистами Акта выступали ФБР и Агентство национальной безопасности, что свидетельствует о том, что он был призван лишь заретушировать те тотальные полномочия, которые получили американские спецслужбы после 11 сентября 2001 г. К тому же представление ежегодного отчета об исполнении Акта о свободе способствует повышению уровня доверия к спецслужбам, в США присутствует разделение уровней защиты гражданских прав собственных граждан и иностранцев, заподозренных в террористической деятельности [8].

С 2016 года служба таможенной и пограничной службы США (CBP) начала предлагать временно въезжающим в страну гражданам оставлять «информацию, связанную с присутствием в интернете» при заполнении формы электронной системы авторизации путешествий (ESTA). Данные изменения объясняются попыткой США недопустить въезд в страну лиц, связанных с террористическими организациями, в том числе с группировкой «Исламское государство» [3].

В ФРГ с октябре 2017 года в стране вступил в силу закон, согласно которому на социальные сети, например, такие как «Facebook», «Twitter» и «YouTube» , налагаются штрафы на сумму до 50 млн.евро за систематическое несвоевременное удаление публикаций, содержащих материалы или новости, разжигающие ненависть, подстрекающие к преступлениям или одобряющие их [3].

С 2000 г. в Российской Федерации началось развитие правовой базы противодействия киберугрозам терроризма и экстремизма, когда была принята первая Доктрина информационной безопасности РФ [9], с 2016 года действует новая ее редакция [10]. С 2008 г. действует Указ Президента РФ от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» [11]. В 2013 г. были утверждены «Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года» [12]. Указом Президента РФ от 15.01 2013 г. на ФСБ РФ возлагаются полномочия по созданию государственной

системы обнаружения, предупреждения и ликвидации компьютерных атак на информационные ресурсы РФ, информационные системы и информационно-телекоммуникационные сети, находящиеся на территории РФ и в дипломатических представительствах и консульских учреждениях РФ за рубежом [13]. С 2017 года действует Указ Президента РФ «О Стратегии развития информационного общества в Российской Федерации на 2017 – 2030 годы», одной из задач которого является совершенствование механизмов ограничения доступа к информации, распространение которой в Российской Федерации запрещено федеральным законом, и ее удаления[14]. По словам главы Роскомнадзора, Андрея Липова, за 2019 год в сети Интернет было выявлено более 530 тысяч запрещенного в РФ контента, причем на первом месте по количеству (208 тысяч) находился контент экстремистского и террористического характера[15].

Таким образом, многие страны мира, международные организации, социальные сети и др. запустили программы противодействия экстремистской и террористической деятельности. Активно развивается и законодательство в этой сфере. Эффективными оказалось создание наблюдательных советов и «горячих линий», которые имеют право оперативно удалять из сети Интернет материалы, имеющие экстремистскую и террористическую направленность. Все более популярными становятся автоматизированные технологии, которые помогают быстро выявлять и удалять террористический контент, аккаунты, чьи владельцы ведут незаконные действия в социальных сетях: агитацию, вербовку, экстремистскую пропаганду. Но, по словам главы Роскомнадзора, несмотря на автоматизированную систему выявления подобного контента, в работе данной службы остается еще много ручного труда. Перспективами развития отслеживания контента террористического характера является применение нейросетей, что позволит сократить количество ручного труда, увеличить точность работы службы[15]. Для борьбы с терроризмом и экстремизмом в Интернете так же можно использовать искусственный интеллект, который также сократит ручной труд, увеличит скорость обнаружения террористического и экстремистского контента. Причем, по сообщению генерального директора IBM России Андрея Филатова, между IBM и рядом российских компаний идут переговоры по внедрению системы искусственного интеллекта Watson for Cyber Security, нацеленной на борьбу с киберпреступностью[16].

Список литературы:

1. Число пользователей интернета в мире выросло до 4,1 млрд человек [Электронный ресурс] // URL:https://tass.ru/obschestvo/7080150(дата обращения 24.11.2020)

2. Вся статистика интернета на 2020 год – цифры и тренды в мире и в России [Электронный ресурс] // URL:https://www.web-canape.ru/business/internet-2020-globalnaya-statistika-i-trendy/(дата обращения 24.11.2020)

3. Бураева Л.А. Зарубежный опыт противодействия экстремизму и терроризму в Интернет-пространстве //Пробелы в российском законодательстве. 2018.–№ 6.–С.283-285.

4. Google ужесточает борьбу с распространением экстремистских видео на YouTube [Электронный ресурс] // URL: https://tass.ru/obschestvo/4346995(дата обращения 24.11.2020)

5. Counter-Terrorism Internet Referral Unit (CTIRU) // From Wikipedia, the free encyclopedia[Электронныйресурс] // URL: https://en.wikipedia.org/wiki/Counter-Terrorism_Internet_Referral_Unit (датаобращения 25.11.2020)

6. Патриотический акт // Материал из Википедии — свободной энциклопедии [Электронный ресурс] // URL:https://ru.wikipedia.org/wiki/Патриотический_акт(дата обращения 24.11.2020)

7. Акт о свободе США // Материал из Википедии — свободной энциклопедии [Электронный ресурс] // URL:https://ru.wikipedia.org/wiki/Акт_о_свободе_США(дата обращения 24.11.2020)

8. Романовская О.В. Акт о свободе: ограничение прав человека в США в целях противодействия терроризму// Электронный научный журнал «Наука. Общество. Государство» 2017. Т. 5, № 3 (19) [Электронный ресурс] // URL: http://esj.pnzgu.ru(дата обращения 24.11.2020)

9. Бураева Л.А. Мировой опыт противодействия экстремизму и терроризму в глобальном информационном пространстве // Теория и практика общественного развития.2015.-№18.-С.131-134.

10. Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» [Электронный ресурс] // URL: https://www.garant.ru/products/ipo/prime/doc/71456224/(дата обращения 25.11.2020)

11. Указ Президента РФ от 17.03.2008 г. № 351 [Электронный ресурс] // URL: http://www.consultant.ru/document/cons_doc_LAW_75586/(дата обращения 25.11.2020)

12. Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года (утв. Президентом РФ 24.07.2013 N Пр-1753) [Электронный ресурс] // URL: http://www.consultant.ru/document/cons_doc_LAW_178634/(дата обращения 25.11.2020)

13. Указ Президента Российской Федерации от 15.01.2013 г. № 31[Электронный ресурс] // URL: https://base.garant.ru/70299068/(дата обращения 24.11.2020)

14. Указ Президента Российской Федерации от 09.05.2017 г. № 203[Электронный ресурс] // URL:http://www.kremlin.ru/acts/bank/41919/page/1(дата обращения 25.11.2020)

15. Роскомнадзор: Экстремистские материалы лидируют среди запрещенных в Сети»[Электронный ресурс] // URL: https://eadaily.com/ru/news/2020/08/10/roskomnadzor-ekstremistskie-materialy-lidiruyut-sredi-zapreshchennyh-v-seti(дата обращения 25.11.2020)

16. Искусственный интеллект против кибертерроризма [Электронный ресурс] // URL: https://ncpti.su/aricles/4432/ (дата обращения 26.11.2020)

Аверина Валерия Андреевна
Юридический институт, АлтГУ, г. Барнаул
Научный руководитель: Соколов Александр Сергеевич,
старший преподаватель кафедры уголовного процесса и криминалистики,
Юридический институт АлтГУ, г. Барнаул

Аверина В.А. КИБЕРТЕРРОРИЗМ КАК УГРОЗА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В последнее время понятие кибертерроризма широко обсуждается в СМИ. Опасность терроризма оказалась больше, чем ожидалось, а функции кибертерроризма невероятно расширились из-за распространения Всемирной паутины. Компьютерный терроризм стал являться реальной социально-опасной угрозой для человечества, по сравнению даже с ядерным или химическим оружием. Опыт у всемирного сообщества в этой сфере со всей очевидностью свидетельствует о несомненной уязвимости каждого государства, тем более, что кибертерроризм не имеет государственных границ; кибертеррорист способен в равной степени угрожать каждой информационной системе, которая расположена в любой точке Земли. Можно сказать, что кибертерроризм является составной частью информационной безопасности. [2]

Говоря о кибертерроризме, нельзя не отметить и киберпреступность. Киберпреступность – это незаконные действия, которые осуществляются людьми, использующими информационные технологии для преступных целей. Среди основных видов киберпреступности выделяют распространение вредоносных программ, взлом паролей, кражу номеров кредитных карт и других банковских реквизитов, а также распространение противоправной информации через Интернет.[2]

Таким образом, можно сказать, что кибертерроризм – это комплексная акция, выражающаяся в преднамеренной, политически мотивированной атаке на информацию, обрабатываемую компьютером и компьютерными системами, создающей опасность для жизни или здоровья людей либо наступления других тяжких последствий, если такие действия были содеяны с целью нарушения общественной безопасности, запугивания населения, провокации военного конфликта.[2]

Отмечу, что характерной особенностью кибертерроризма и его отличием от киберпреступности есть его открытость, когда условия террориста широко оповещаются.[2]

Угроза информационного терроризма обусловлена целым рядом факторов. В первую очередь научно-техническим прогрессом, появлением глобальной информационной сети (ГИС) - Интернета (октябрь 1969 года, США),

глобальными процессами информатизации, интеграцией стран в международный информационный обмен, возрастанием влияния информации на все сферы жизнедеятельности общественных и государственных структур, повсеместной автоматизацией объектов жизнеобеспечения и инфраструктуры государств. [1]

Начало активного использования Интернета террористическими и экстремистскими организациями в России можно отнести к началу 2000-х годов. В дальнейшем развитие данного процесса шло в геометрической прогрессии. Только в 2005–2006 гг. было зафиксировано более 2 млн. компьютерных нападений на информационные ресурсы органов государственной власти, в том числе свыше 300 тыс. атак на интернет представительство президента РФ.

Отмеченная негативная тенденция продолжает сохраняться и в настоящее время. Она полностью корреспондируется с развитием криминальной составляющей киберпреступности в Российской Федерации.

Так, если 55 % сайтов, противоречащих британских законам, зарегистрированы в США, то 23 % – инициированы из России. [4]

С начала 2000-х гг. Российская Федерация принимает активное участие в разработке международных норм, закрепляющих меры борьбы с кибертерроризмом. Однако проводимые меры по борьбе с кибертерроризмом носят скорее формальный характер, и нередко оказываются неэффективными в практической деятельности. Это подтверждают повторяющиеся с каждым годом факты кибератак на крупнейшие компании и государственные органы, как в России, так и за рубежом. Следует отметить, что общество также оценивает политику России по данному вопросу как не эффективную. По результатам анкетирования, проведенного среди молодежи, лишь 18,42 % опрошенных высказались за эффективность существующих мер по противодействию компьютерному терроризму (опрос проводился в 2016 году в г. Омске среди 97 человек).[4]

В 2013 году Президент РФ Путин В. В. своим Указом от 15.01.2013 № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» возложил на ФСБ РФ полномочия по созданию государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ - информационные системы и информационно-телекоммуникационные сети, находящиеся на территории Российской Федерации и в дипломатических представительствах и консульских учреждениях Российской Федерации за рубежом. [3]

В Российской Федерации пока должного внимания указанной выше проблеме не уделяется. Термин кибертерроризм легально не закреплен ни в одном нормативно-правовом акте. Уголовная ответственность за совершение террористического акт предусмотрена ст. 205 УК РФ, при этом квалифицированного признака, связанного с осуществлением данного акта в

киберпространстве российский Уголовный кодекс не предусматривает.Кибертеррористы, которые специализируются на взломе компьютерных систем, постепенно научились организовать отдельные кибератаки в глобальные, положив тем самым начало истории кибервойн. Последовательность громких кибератак продолжилась уже в начале XXI века.[4]

Сегодня вопросы информационной безопасности все более пересекаются с проблемами глобальной безопасности и, конечно, должны будут во многом решаться в рамках сотрудничества и партнерства. Наиболее важной областью сотрудничества является сфера обеспечения международной и национальной информационной безопасности. Для выработки рациональной политики в сфере обеспечения информационной безопасности прежде всего необходима трезвая оценка сегодняшнего состояния, особенностей и перспектив развития информационного оружия и способов его применения. Такая оценка есть базовая предпосылка выработки внешней и внутренней политики государства, военные и военнотехнические компоненты которой могли бы предотвращать или парировать возникшие угрозы и надежно обеспечивали бы безопасность страны.

В заключение хотелось бы отметить, что отрицать сегодняшнее наличие кибертерроризма в разных его проявлениях, в качестве серьёзнейшей угрозы, которая несет вызов мировому сообществу, является опрометчивым и недальновидным. Перед странами стоит задача не только четкого распознавания проблемы, но и выработки наиболее точных правовых и технических методов борьбы угрозами. Чем больше государства будут сотрудничать в таких вопросах, тем легче будет предотвращать не только мелкие, но и крупные, хорошо организованные кибератаки, несущие хаос из виртуального мира в реальный.

Список литературы:

1. Противодействие угрозе кибертерроризма [Электронный ресурс] https://catu.su/analytics/1530-protivodejstvie-ugroze-kiberterrorizma

2. Политика противодействия кибертерроризму в современной России [Электронный ресурс] http://elar.uspu.ru/bitstream/uspu/5716/1/21Prokopeva.pdf

3. Указ Президента Российской Федерации от 15 января 2013 г. N 31c г. Москва "О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации" [Электронный ресурс] https://rg.ru/2013/01/18/komp-ataki-site-dok.html

4. ИСПОЛЬЗОВАНИЕ ИНТЕРНЕТА В ТЕРРОРИСТИЧЕСКИХ ЦЕЛЯХ [Электронный ресурс] https://www.unodc.org/documents/terrorism/Publications/Use_of_Internet_for_Terrorist_Purposes/Use_of_the_internet_for_terrorist_purposes_Russian.pdf

Варнавская Дарья Николаевна
Юридический институт АлтГУ,
г. Барнаул
Научный руководитель: Мазуров Валерий Анатольевич,
кандидат юридических наук,
доцент кафедры уголовного права и криминологии АлтГУ

Варнавская Д.Н. ИНФОРМАЦИОННЫЕ ВОЙНЫ В СОВРЕМЕННОМ МИРЕ

Понятие «информационная война» становиться всё более популярным. Оно используется не только в научных трудах, но и в художественных фильмах. Появление киноплёнок и выступлений различных общественных деятелей, утверждающих наличие информационных атак и манипуляций сознанием, позволяет констатировать актуальность изучения этого явления.

Готова ли Россия противостоять информационной атаке исходящей от развитых стран? Ответ на этот вопрос лучше всего дать, проанализировав события, происходившие в прошлом 2008 г., который, на мой взгляд, смело можно назвать годом «информационного прессинга».

Одним из основных и самых печальных событий 2008 г. стала война между Южной Осетией и Грузией. Опыт современных локальных конфликтов учит, что любая «обычная» война должна предваряться мощной информационной войной. Чтобы убедиться в этом, приведём несколько примеров. События в Южной Осетии комментировали многие западные СМИ. Так, британский телеканал «Sky News» показал в новостном выпуске 8 августа видеосюжет об обстреле сёл Южной Осетии и столицы республики - Цхинвала грузинской артиллерией в ночь на 8 августа, а на следующий день сопроводил его сообщением, что «Россия ведёт обстрел территории Южной Осетии, входящей в состав Грузии». Долгое время западные телевизионные каналы не вели репортажи непосредственно из Цхинвала, однако почти все сообщали о катастрофических разрушениях города сначала под огнём грузинской артиллерии, затем под огнём артиллерии российской. Все представители западных СМИ базировались в Тбилиси и сообщали о разрушениях в грузинских городах Гори и Поти. В Цхинвале находились только российские телеканалы и один украинский. И только впоследствии Цхинвал посетили более 100 иностранных журналистов. Российский информационный канал «Вести» приводит слова депутата Европарламента Джульетто Кьеза, что

итальянские СМИ «сообщают о том, что Грузия была подвергнута атаке со стороны Южной Осетии, что Россия ведёт войну против Грузии с целью захвата этой страны. Что являлось ложью».

По итогам войны на Кавказе решением Президента России должны были быть созданы специальные организационно-управленческие и аналитические структуры для противодействия информационной агрессии. Цель Информационных войск – создание такого информационного пространства, которое делает международную реальность отвечающей российским интересам. Информационные войска должны решать три основные задачи – стратегический анализ, информационное воздействие, информационное противоборство - и работать одновременно как на внешнюю, так и на внутреннюю аудиторию.

Существуют различные классификации способов воздействия СМИ на человека. Зинорова Н. выделяет следующие методы воздействия:«Наиболее часто используемым способом манипуляции сознания зрителя является - искажение информации».

Прямое искажение информации (современные политики и телевизионные деятели уже давно не используют ложь. Они стараются дозировать правдивую информацию. Не огласив несколько фактов и сделав несколько небольших отклонений, можно получить совершенно другую картину события), сенсационность (концентрируя внимание человека на каких-то фактах, можно не выдавать в эфир информацию о каких-то значимых событиях), узнавание образа (телевидение становится все больше коммерческим, и узнавание личности является одним из рычагов манипулирования сознанием)...

Подобные методы могут быть использованы скорее в том случае, если СМИ подконтрольно стороне, начавшей информационную войну. Однако существуют методы влияния на «свободные» средства массовой информации. Среди основных методов по непосредственному использованию СМИ в информационных войнах находятся война компроматов, утечки информации, дезинформация. Использование этих методов связано с разведывательной деятельностью в информационной войне. В классическом понимании разведки мы имеем сбор информации, оценку ее достоверности и объединение отдельных фактов в аналитическую картину. Информация поступает как от иностранцев, делающих это случайно или специально, так и от технических средств информации (спутниковая фотосъемка, прослушивание и т.д.). В условиях быстрого развития международных открытых сетей типа Интернет и присоединения к ним большинства стран кардинально меняется идеология ведения разведки, в которой основной акцент теперь делается на использовании новейших информационных технологий для добывания конфиденциальной информации.

Также часто используются слухи. Например, в США, Великобритании, Швеции при ответственных организациях за национальную безопасность, функционируют специальные структуры, ответственные за работу со слухами. В этих государствах понимают значимость этого канала коммуникации и

осознают необходимость держать его под контролем, а также искусственно воздействовать на общественное мнение, создавая нужные слухи внутри своей организации.

Часто используются такие методы, как игнорирование, уменьшение значимости темы (перенос акцентов на менее негативные элементы темы, кратком затрагивании и неупоминании темы), превентивная пропаганда и опережение (метод состоит в превентивном использовании пропагандистской темы, которая может быть использована другой стороной, с измененными и смягченными компонентами или элементами для уменьшения доверия к теме), общественное неодобрение, создание иллюзии неодобрения тех или иных действий состороны общественного мнения, неопределенные выражения и намеки, несущие негативную окраску, имитационная дезинформация (внесение изменений в пропаганду другой стороны, которые придают ей другое направление, снижают доверие к ней, создают негативный образ), перенос неодобрения и негативного образа (метод состоит в неодобрении целевой аудиторией персон, действий или идей через демонстрацию тех групп, которые одобряют данные идеи или действия, поддерживают эти персоны, но относятся к числу имеющих низкое доверие. Тех, кого боятся, ненавидят или презирают. Состоит в проекции негативных качеств человека, предмета или моральных ценностей на другого человека или идею, чтобы дискредитировать его), «наклеивание ярлыков» (эксплуатация предрассудков и стереотипов населения через наклеивание ярлыка на объект. Например, во время психологических операций против полевого командира Ахмад Шаха Масуда, вооруженные силы демократической республики Афганистан пытались связать с ним такие понятия, как предатель и убийца мусульман, диверсант, слуга и раб американцев и китайцев), ну и последний метод- псевдологический (логические выводы делаются на основе специально ограниченного массива информации. Часто используется при проведении социологических опросов. Замена источника сообщения).

Также необходимо отметить, что информационная война не является чем-то новым для человечества. Наоборот: если пушки изредка затихали, то словесные баталии между государствами не прекращались никогда. Ещё античные авторы в подробностях рассказывают об изощрённых агитационных компаниях, при помощи которых политики древности пытались ослабить своих противников и деморализовать их.

Фемистокл, например, во время войны с персами приказывал вырезать на камнях призывы к ионянам переходить на сторону афинян - или хотя бы не сражаться с ними слишком усердно. Во время Великой Отечественной войны такого рода призывы уже не вырезались на камнях, а печатались на листовках и разбрасывались над вражескими позициями с самолётов.

Информационная война сегодня. Современная Россия -занимающая одну восьмую суши земного шара и обладающая второй по силе армией в мире - впутана в целый ряд информационных конфликтов с самыми разными странами. Главными противниками являются так называемые «страны Запада»,

из которых следует особо выделить США и Великобританию. Помимо собственных СМИ и прочих специальных организаций, в своей информационной борьбе с Россией эти страны в последние десятилетия активно используют как спонсируемые ими силы внутри России (несистемную оппозицию, русофобские СМИ), так и антироссийски настроенные элиты и СМИ некоторых соседних с Россией стран (Польши, Украины, Эстонии, Латвии, Литвы, Грузии).

Главной целью информационной войны, которая ведётся против России, является дестабилизация ситуации внутри страны, в частности организация «оранжевой революции» и других негативных сценариев в России, а вне страны - развитие антироссийского вектора общественного мнения сопредельных и «натовских» стран. Приоритетом является ослабление России и порча её репутации за рубежом. В частности, Запад навязчиво пытается выставить Россию «тиранической», «отсталой» и «агрессивной»: при этом агитация направлена как на население России, так и на жителей других стран.

Наиболее активно информационное взаимодействие между государствами стало проявляться в XX веке в связи с развитием коммуникационных технологий. После окончания Второй Мировой войны возросшее влияние Советского Союза стало представлять угрозу для Запада. Холодная война во многом стала информационным противостоянием двух сверхдержав. В Советском Союзе велась активная пропаганда о «загнивающем» Западе и упадке капитализма, в США же муссировалась так называемая коммунистическая угроза, что стало причиной обильной информационной пропаганды внутри страны.

Особое обострение в информационно-пропагандистской сфере между США и Россией произошло во время грузино-осетинского конфликта. По официальным данным, Россия принимала участие в этой войне защищая своих граждан и миротворцев, подвергнувшихся нападению со стороны Грузии. В СМИ США это было представлено как агрессия со стороны России. Уже 8 августа американское информационное агентство давало новости подрубрикой«РоссиявторгласьвГрузию».ЭтоттелеканалпоказывалкартинкуизразрушенногоЦхинвала,послеобстреловгрузинскойартиллерии,ивыдавалзауничтоженный российскими войсками грузинский город Гори. При этом в Цхинвале телеоператоров CNN в те дни не было. А вот в Гори американцы были, но там не оказалось разрушений. Позднее телеканал CNN признал, что произошла ошибка, но это было упомянуто вскользь, а «разрушенный» Гори показывался многократно.

Президент Грузии Саакашвили утверждал, что агрессия Россия направлена не только против Грузии, но также на США, ЕС и НАТО.

Вполне можно сказать, что эту войну на информационном поле битвы Россия проиграла.

Причинакроетсявнедостаточномакцентированиивниманиянаинформационную сферу, а также в неподготовленности медиаресурсов.

Во время украинского кризиса (Евромайдан и т.д.) Россия вошла в информационное противостояние с Западом, в частности с США, более подготовленной. Сказались прошлые провалы в этой сфере и повышение значимости информационной безопасности.

После начала военных действий на Юго-Востоке Украины представители госдепа неоднократно заявляли о вводе российских войск на Украину. Так в апреле 2015 года, представитель Госдепартамента США Мари Харф заявила, что она по-прежнему убеждена в присутствии российских военных на Украине, но при этом не обладает данными об их числе, об этом она заявила на регулярном брифинге. Отвечая на вопрос журналиста о масштабе предполагаемого российского присутствия, она сказала: «Я знаю, что число их огромно, ноне знаю, сколько именно. США знают, что российские военные продолжают действовать навостоке Украины».

С начала операции по бомбардировке Россией позиций ИГИЛ в Сирии западные СМИ активно переключились на эту тематику. Россию стали обвинять в том, что авиаудары наносятся не по террористической организации Исламского Государства, а по так называемой Сирийской Свободной Армии, которая получает политическую и финансовую поддержку со стороны западных (США, Франция, Великобритания, и других) и арабских(страны Персидского залива и Турция) государств. Представитель госдепартамента США Джон Кирби обвинил Россию в нанесении ударов по сирийской оппозиции. По словам Кирби, менее 10 % ударов российской авиации в Сирии были направлены против боевиков«Исламского государства» и «Аль-Каиды».Это обвинение прозвучало в ответ на ранее сделанное заявление официального представителя министерства обороны России Игоря Конашенкова: «Американские и другие ВВС уже год наносят удары. Так вот у нас есть основания полагать, что они далеко не всегда, а точнее, очень часто, бьют не по террористическим целям». Например, следует привести инцидент, произошедший в сентябре 2014 года, когда жертвами очередных авиаударов США по Сирии стали пять мирных жителей, в том числе один ребенок. На следующий день после своего заявления, на брифинге для журналистов Дж. Кирби не стал конкретизировать ответ на вопрос представителя СМИ, по каким именно группам Россия наносит удары в Сирии. Он пояснил, что в Сирии много разрозненных группировок, но Россия наносит удары в основном по тем, которые противостоят режиму Асада. Какие группировки конкретно имеются в виду, не уточнялось. Также в начале октября были получены обвинения в уничтожении госпиталя Воздушно-космическими силами России, в котором находились сирийские оппозиционеры. В ответ на это заявление, министерство обороны РФ организовало проверку и выяснилось, что в действительности госпиталь в населенном пункте Сармин по прежнему действует.

Стоит отметить, что результативность российских ударов намного выше, чем у коалиции во главе с США.

Можно предположить, что все эти информационно-пропагандистские обвинения направлены на подрыв результатов действий ВКС России в Сирии в

глазах мирового сообщества. Президент Сирии Башар Асад 22 ноября 2015 года заявил, что военные России за два месяца кампании по борьбе с боевиками «Исламского государства» сделали больше, чем коалиция во главе с США за год. По словам Асада, российские авиаудары вынудили боевиков бежать из Сирии в Турцию и другие страны.

Запад ведет активную борьбу с информационной политикой России. Так, в апреле2015годапоступилаинформация,чтоХельсинкипринялирешениеначатьпр отиводействовать российским СМИ. Для этого в Финляндии была создана специальная рабочая группа, в которую вошли представители различных министерств и госслужб.

Основной задачей нового государственного органа будет противодействие российским СМИ,о чем было сказано руководителем правительственной службы по коммуникациям, экспертом комитета по государственной безопасности Маркку Мантила. По его словам, главным в работе структуры будет обмен информацией, координация усилий и совместное планирование.

Представительфинскихвластейуверен,чтоМосквакобыведет«полномасшта бную информационную войну» против ряда стран, в том числе - Финляндии.

Одним из методов борьбы с «ложной информацией» из России должны стать выступления экспертов в школах и на производстве.В2016финансовомгодуСШАрешилипотратитьнапротиводействие информационной политике Кремля 83 миллиона долларов. Об этом в ходе слушаний
всенатскомкомитетепоиностраннымделамконгрессаСШАсообщилзаместительп омощника госсекретаря по делам Европы и Евразии Бенджамин Зифф. Он особо подчеркнул, что основные средства пойдут не на пропаганду, а на контрпропаганду – борьбу с информационной политикой России.

Необходимо отметить что, в современных условиях обострения информационной конфронтации между Россией и Западом очень важно уделять больше внимания структурам по ведению информационной пропаганды. Следует развивать медиа-структуры, вести дополнительную работу в социальных сетях. Нельзя приуменьшать значимость информационной сферыпотому,чтоЗападтолькоусиливаетинформационно-
пропагандистскуюработупопротиводействию России на информационном поле.

СМИ не всегда и не обязательно являются инициаторами или субъектами изменений в сознании отдельных людей или социальных групп. Сами по себе они не могут быть ни инструментом разрушения, ни инструментом созидания и прогресса. Их позитивная или негативная роль определяется тем, какими именно социальными силами и с какой целью они используются.

Список литературы:

1. Расторгуев С.П. Информационная война. – М: Радио и связь. 1999 г. 416 С.

2. Роменков А.А. Информационнная война против России. 2009г. 38С.

3. Гриняев С. Концепция ведения информационной войны в некоторых странах мира [Электронный ресурс]. – Режим доступа:http://www.soldiering.ru/psychology/conception_psywar.php.

4. Генштаб: США обкатали в Афганистане технологию информационных войн [Электронный ресурс]. – Режим доступа:http://vz.ru/news/2015/10/8/771239.html.

5. Иудин А. А., Рюмин А. М., Шпилёв Д. А. Информационная война в Интернет: западные обыватели о России. – Н. Новгород: НИСОЦ, 2011 – 156 с.

6. Подлог в прямом эфире [Электронный ресурс].– Режим доступа:http://www.rg.ru/2008/09/10/podlog-cnn.html.

7. Саакашвили: «Они хотят всю Грузию» [Электронный ресурс]. – Режим доступа:http://inosmi.ru/world/20080813/243214.html.

8. Госдеп заявил об «огромном числе российских военных на Украине» [Электронный ресурс]. – Режим доступа:http://ria.ru/world/20150417/1059296668.html.

9. Госдеп: 90 процентов ударов России в Сирии – по оппозиции [Электронный ресурс]. –Режим доступа: http://www.bbc.com/russian/news/2015/10/151007_us_russia_syria_targets.

10. Жертвами очередных авиаударов США по Сирии стали пять мирных жителей

[Электронный ресурс]. – Режим доступа:http://wek.ru/zhertvami-ocherednyx-aviaudarov-ssha-po-sirii-stali-pyat-mirnyx-zhitelej.

11. В Госдепе США не стали называть группировки, по которым Россия наносит удары в Сирии [Электронный ресурс].–Режим доступа:https://russian.rt.com/article/122481.

12. Минобороны опубликовало доказательства невиновности в уничтожении госпиталя в Сирии [Электронный ресурс].–Режим доступа:http://www.mk.ru/politics/2015/11/03/minoborony-opublikovalo-dokazatelstva-nevinovnosti-v-unichtozhenii-gospitalya-v-sirii.html.

13. Асад: Россия за два месяца в Сирии сделала больше, чем США за год [Электронный ресурс]–Режим доступа:http://www.gazeta.ru/politics/news/2015/11/22/n_7919639.shtml.

14. СМИ: Финляндия создала специальное ведомство для борьбы с российской пропагандой [Электронный ресурс].–Режим доступа:https://russian.rt.com/article/87992.

Варнавская Елена Владимировна
Юридический институт АлтГУ,
г. Барнаул
Научный руководитель: Мазуров Валерий Анатольевич,
кандидат юридических наук,
доцент кафедры уголовного права и криминологии АлтГУ

Варнавская Е.В. РЕЛИГИОЗНО-НАЦИОНАЛИСТИЧЕСКИЙ ЭКСТРЕМИЗМ В ИНТЕРНЕТЕ КАК УСЛОВИЕ ПРЕСТУПНОСТИ ЭКСТРЕМИСТСКОЙ И ТЕРРОРИСТИЧЕСКОЙ НАПРАВЛЕННОСТИ В МОЛОДЕЖНОЙ СРЕДЕ

Общеизвестно, что в современных условиях реальную угрозу, как для всего мирового сообщества, так и национальной безопасности того или иного государства, его территориальной целостности, конституционных прав и свобод граждан представляет экстремизм в различных формах его проявления[1].

В последние десятилетия возникли десятки агрессивных движений, проповедующих различные варианты экстремистской деятельности, это национализм, религиозный фундаментализм, фашизм и идеи конца света.

Националистический экстремизм – это радикальные идеи и действия в отношении представителей иной народности, национальности, стремление к политическому или физическому устранению определенного населения; агрессия, в крайних формах – терроризм в отношении людей иной этнической группы.

Выделяя такую категорию, как националистический экстремизм, мы говорим о том, что национализм является детерминантой экстремистской деятельности. Следуя логике законодателя, можно определить, что национализм является причиной экстремизма, если он [2]:

– Во-первых, возбуждает национальную рознь;

– Во-вторых, пропагандирует исключительность, превосходство либо неполноценность человека по признаку его национальной принадлежности;

– В-третьих, нарушает права, свободы и законные интересы человека и гражданина в зависимости от его национальной принадлежности.

Религиозный экстремизм, это оборотная сторона любой религии, ее темная, опасная сторона, действующая под видом влечения к религии, зарождая и развивая безнравственные взгляды и принципы, влекущие вред интересам лиц или целого общества, заключающиеся в разрушении общепризнанных норм морали и права, препятствующие становлению и развитию институтов демократии и гражданского общества.

Основная цель религиозного экстремизма – признание своей религии, ведущей и подавление других религиозных конфессий через их принуждение к своей системе религиозной веры.

В последствии происходит переход к практике экстремизма, когда радикальные идеи становятся такими убеждениями, ради которых человек готов на все, даже на преступление. Крайние радикальные формы политического мышления реализуются в крайних формах экстремистского поведения и деятельности: в гражданской войне, нелегитимном насилии, геноциде, этноциде, нарушении прав и свобод граждан, закрепленных в конституциях современных государств и нормах международного права. Наиболее ярые экстремисты ставят своей задачей создание отдельного государства, правовые нормы которого будут заменены нормами общей для всего населения религии. Экстремизм многолик. Он проявляется также в расизме, шовинизме, религиозной нетерпимости, связанной с фундаментализмом, тоталитарными культами и т.д [3].

На современном этапе существования человечества, информационный век принес миру не только повсеместное развитие технологий и компьютеризацию всей жизни, но и привел к появлению такой формы социальной девиации, как кибепреступность, которая в настоящее время получает все более широкое развитие.

Кибертерроризм – это серьезная угроза человечеству. Опыт, который уже имеется у мирового сообщества в этой области, предположительно свидетельствует о несомненной уязвимости любого государства, тем более,что кибертерроризм не имеет государственных границ и возрастных рамок [4].

С одной стороны «всемирная паутина» является мощным импульсом человеческого прогресса. Однако сеть, ставшая сегодня неотъемлемой частью жизни молодежи и связавшая в единую неразрывную систему значительную часть человечества, одновременно несет и негативную сторону. Причем, в первую очередь, негативное влияние сказывается на подрастающем поколении: подростки теряют интерес к чтению книг, живое общение заменяется для них виртуальным в чатах и форумах; наблюдается стремительный рост агрессивности, вызванной чрезмерным, а иногда и болезненным увлечением компьютерными играми [5].

Дети 21 века комфортнее ощущают себя в информационном пространстве по сравнению со взрослыми. Они не испытывают страх или тревогу при освоении новых технологий, легко подхватывают современные тренды и непосредственно сами создают их. Социальные сети (Instagram, Twitter, Facebook, Вконтакте, Google+, TikTok), мессенджеры (WhatsApp, Telegram), видеохостингYouTube, мобильные игры — все эти элементы информационного пространства являются привычными вещами для повседневной жизнедеятельности школьников и подростков.Естественно, систематически и постоянно погружаясь в цифровую среду, несовершеннолетние подвергаются влиянию публикуемого потенциально опасного контента [6].

Нельзя не согласиться, что всемирная сеть Интернет, благодаря своим широким возможностям и доступности, является идеальным полем деятельности для террористических организаций. Ведь к ней всегда свободный доступ, здесь отсутствует цензура, в наличии огромная аудитория, обеспечена анонимность связи и быстрая передача информации, невысокая стоимость трафика и многое другое. Привлекают правонарушителей также низкий риск обнаружения и возможность действия практически в любой точке земного шара.

Большинство молодежи черпают из интернета информацию о религии, не осознавая, что становятся жертвами радикальных религиозных течений. Молодые люди, поддаваясь влиянию террористических и экстремистских организаций, зачастую уверены, что занимаются очисткой страны от проблем, среди которых: безработица, бедность, несправедливость при оплате труда и в карьерном росте, социальная несправедливость, отсутствие правосудия в интересах рядового гражданина, неадекватность государственного регулирования и другие. У молодежи, возникает желание сделать мир гораздо более справедливым, при этом молодые люди не сразу осознают, что такой путь, как экстремизм и терроризм, не является допустимым.

Существует такое понятие как экстремистский героизм, он объединяет особые группы экстремистов, чувствующих себя героями, призванными быть провидениями и спасителями, демиургами, во власти которых находится переустройство жизни людей. У представителей молодежи есть много фактов, иллюстрирующих присутствие «экстремистского героизма». Говорят даже о специфических «героических» молодежных субкультурах. К таким субкультурам относятся:

– скинхеды — это молодежная субкультура расистского толка, политизированные фанатские группировки.

– группировки, подобные молодежным РНЕ (русское национальное единство). В последние годы снизили свою активность.

Деятельность подобных группировок проявляется в массовых беспорядках, серии убийств на расовой и межкультурной почве, появлении граффити, свастик, лозунгов, рисунков, названий группировок на стенах домов и подъездов, использовании языка вражды в СМИ, в том числе и в Интернете [7].

Развитие религиозно-националистического экстремизма среди молодежи представляет особую опасность даже не потому, что уровни детской, подростковой и молодежной преступности заметно возросли, а поскольку это связано с развитием «анормальных» установок в групповом сознании молодого поколения, что влияет на ценности, предпочтительные образы поведения, оценки социального взаимодействия – то естьв широком смысле связано с социальной и политической культурой российского общества в ее проективном состоянии [8].

Глобальная сеть Интернет может использоваться террористами не только в качестве инструмента для публикации экстремистских видео-материалов, но и

для непосредственного контакта с теми, кто наиболее подвержен вербованиюи несовершеннолетние как правило входят в категорию группы риска. Подростки наиболее склонны поддаваться целенаправленному влиянию со стороны профессиональной пропаганды экстремизма и терроризма. Террористические организации используют информационно-коммуникационное пространство в качестве поля действия для подготовки террористов. Реализуя все возможности социальных сетей и видеохостингов, террористические организации распространяют практические навыки в виде интерактивных учебных пособий, аудиои видеоклипов, сообщений [9].

Рассмотрев аспектырелигиозно-националистического экстремизма,можно сделать вывод, что противодействие его проявлениям в молодежной среде требует комплексного подхода, объединяющего силовые, политико дипломатические, экономические и гуманитарные формы и методы действий, в сочетании с эффективными антитеррористическими мерами, как на национальном, так и на международном уровнях.

Не менее важным направлением борьбы является проведение профилактической работы среди молодежи, в том числе: организация и проведение комплексных мероприятий по формированию правовой культуры в молодежной среде; воспитание у подрастающего поколения толерантного мировоззрения, терпимости по отношения ко всем людям, вне зависимости от их национальности, религии, социального, имущественного положения и иных обстоятельств.

Важным направлением в профилактике религиозного экстремизма в России также является повышение квалификации педагогов. Комплекс мер для педагогов возможно систематизировать на основе уже имеющегося теоретического материала научных исследований.

Список литературы:

1. [Электронный ресурс]. – Религиозный экстремизм. Центр содействия государству в противодействии экстремистской деятельности: https://csgped.ru/protivodejstvie/ekstremistskaja-dejatelnost/religioznyi-ekstremizm.html (дата обращения: 11.11.2020).

2. Бабышева, К. А. Национализм как детерминанта экстремистской деятельности / К. А. Бабышева, К. А. Сенькова. — Текст : непосредственный // Молодой ученый. — 2019. — № 51 (289).

3. Антоненко В.И. Экстремизм - угроза национальной безопасности Российской Федерации / В.И. Антоненко // Техническая и социокультурная толерантность в преодолении экстремизма в юношеском возрасте. 2018. – 7 с.

4. Макашова В.Н. Механизмы противодействия кибеэкстремизму и кибертерроризму в системе образования / В.Н. Макашова //Педагогические науки. 2015. – № 10. – С. 2054 – 2055.

5. Бураева Л.Г. Кибертерроризм в молодежной среде / Л.Г. Бураева // Экономико-юридический журнал. 2016. – С. 271.

6. Кузнецова Е. В. Правовые меры обеспечения информационной безопасности несовершеннолетних в сети Интернет: российский и зарубежный опыт: методические рекомендации. 2016. С. 4.

7. [Электронный ресурс]. – Экстремизм и национализм. Studme.org : https://studme.org/155452/psihologiya/ekstremizm_natsionalizm (дата обращения: 11.11.2020).

8. Маздогова З.З. Молодежный религиозный экстремизм в современной России и пути его преодоления / З.З. Маздогова // Теория и практика общественного развития. 2015. - № 13. – С. 13.

9. Макашева М.Н. Кибертерроризм как угроза для несовершеннолетних / М.Н. Макашева // Адъюнкт кафедры криминологи Санкт-Петербургского университета МВД России. 2019. – С. 128.

Голованова Екатерина Константиновна
Юридический институт, АлтГУ, Барнаул
Научный руководитель: Соколов Александр Сергеевич,
старший преподаватель кафедры уголовного процесса и криминалистики,
Юридический институт АлтГУ, г. Барнаул

Голованова Е.К. ОСОБЕННОСТИ ПРОЯВЛЕНИЯ ЭКСТРЕМИЗМА В СЕТИ «ВКОНТАКТЕ»

Многие дела, которые возбуждают из-за записей в социальных сетях, в большинстве случаев в социальной сети «Вконтакте», связаны с экстремизмом. Вопросы уголовной ответственности за экстремизм рассматриваются различными статьями Уголовного кодекса РФ, наибольшую известность из которых имеет статья 282 УК РФ. Однако непосредственно текст данной статьи предусматривает ответственность не за экстремизм в целом, а конкретно за возбуждение ненависти, которое, в свою очередь, является частным случаем экстремизма. В некоторых случаях, действия, связанные с экстремизмом, могут не наказываться в уголовном порядке. Существует ряд правонарушений, не рассматриваемых в качестве общественно опасных, и, соответственно, по отношению к которым могут предприниматься меры административного характера.

Особенности распространения информации во «Вконтакте» определяют их значение, которое трудно переоценить. Информация может распространяться как новостная рассылка от сообщества, в котором состоит пользователь социальной сети, так и непосредственно от пользователя к пользователю, что и обуславливает скорость ее распространения. С психологической точки зрения пользователь воспринимает свою страницу как некое личное пространство, что обусловлено особенностями социальных сетей, такими как самостоятельный выбор пользователем круга общения и фильтрация контента посредством членства в интересных пользователю сообществах. Именно из-за этой персонализации, доверие пользователя социальной сети к получаемой информации априори выше, чем к информации, получаемой из других источников, таких как федеральные СМИ и даже Интернет-СМИ. Естественно, что столь мощный медийный инструмент имеет свою специфику и может быть использован для публикации материалов экстремистской направленности. [1]

Эксперты и правозащитники говорят, что в России с каждым годом увеличивается количество уголовных дел за публикации в такой социальной сети как «Вконтакте». Пользователей судят за картинки, их репосты и даже лайки к ним. Всего за 4,5 года в России возбудили 875 дел за посты, репосты,

комментарии и высказывания в интернете. 500 из которых уголовные и административные дела завели по постам и репостам в социальной сети «ВКонтакте». Свыше трех четвертей составляют преступления, связанные с пропагандой идей национального, религиозного, расового превосходства во "ВКонтакте".

Пропаганда экстремизма в социальных сетях имеет свою специфику. Ввиду того, что во «Вконтакте» часто указывается личная информация, возможно целенаправленное распространение материалов, реклама групп, например, для определенной возрастной группы пользователей для оказания максимального на них влияния. [1] Для религиозного экстремизма в качестве примера можно рассмотреть возрастной состав любой группы, пропагандирующей религиозный фундаментализм. Средний возраст подписчиков невысок, более половины составляет молодежь до 18 лет, что и представляет благодатную почву для продвижения идей религиозного экстремизма из-за внушаемости данной группы лиц.

В последние годы отмечается активизация ряда экстремистских движений, которые вовлекают в свою деятельность молодых людей. Анализ данных за последние пять лет показывает, что возраст четырех из пяти лиц, преступная деятельность которых пресечена, составляет не более 30 лет. [2]

В настоящее время членами неформальных молодежных организаций (группировок) экстремистско-националистической направленности в основном являются молодые люди в возрасте до 30 лет, и нередко, в том числе - несовершеннолетние лица 14-18 лет.

Экстремисты, как правило, являются представителями маргинальных кругов. Они не имеют семьи, детей, стабильной работы и устойчивого источника дохода. Обычно занимаются неквалифицированным трудом, либо являются фрилансерами. Занимаются активным самопиаром, осуществляя социально одобряемые действия и позиционируя себя в соответствии с принципом «мы из народа и для народа».

За призывы к экстремизму в социальных сетях подозреваемых зачастую задерживают и даже арестовывают, поэтому эмоциональный пост во «ВКонтакте» зачастую может повлечь последствия не менее серьезные, чем продуманное выступление на митинге.

В Алтайском крае прекращено уголовное дело в отношении обвиняемого в экстремизме Антона Ангела. По словам адвоката Андрея Миллера, решение вызвано частичной декриминализацией статьи Уголовного кодекса об экстремизме в Сети. При этом Антон Ангел намерен обжаловать постановление, чтобы добиться реабилитации.

На жителя Заринска было заведено уголовное дело о "возбуждении ненависти либо вражды, а равно унижении человеческого достоинства". В материалах дела утверждалось, что двое свидетелей обнаружило на его странице во "ВКонтакте" репосты из группы "Сион". В этих сообщениях экспертиза обнаружила признаки враждебного отношения к евреям.

Дело Ангела стало одним из четырёх уголовных дел за лайки и репосты, которые были заведены в отношении пользователей "ВКонтакте" барнаульским Центром по противодействию экстремизму.

Подобное дело суд рассматривал в Петербурге. Студентку Оксану Борисову арестовали за репост записи о несанкционированном народном сходе в память о погибшем бойце спецназа Дмитрие Сидоренко. Девушку почти сутки продержали в отделе полиции, а потом суд приговорил ее к суткам административного ареста за нарушение законодательства о проведении митингов. [3]

Выявлением экстремистских преступлений занимается центр по противодействию экстремизму ГУ МВД России. Иногда случаи экстремизма обнаруживают в «Одноклассниках», но в основном – во «ВКонтакте». Для этого специалисты работают по специальным методикам, о которых нельзя рассказать подробно, потому что эта информация относится к оперативной. Далее с привлечением понятых собираются необходимые данные, составляется специальный протокол, после чего проводятся лингвистические исследования. После этого решается вопрос о возбуждении уголовного дела.

Чаще всего такие дела направляются в суд, потому что это особая категория преступлений. Прежде чем возбудить уголовное дело, в течение года проводятся оперативные действия по сбору информации о причастности лица к такому преступлению. После того как эти материалы легализуют, следователь дополнительно проводит проверку в течение 30 суток. На момент принятия решения о возбуждении уголовного дела информация как правило избыточна.

Поправки в закон «Об информации, информационных технологиях и о защите информации» [5] сделали возможным блокировку интернет ресурсов за призывы к беспорядкам и экстремизм. Выявлением экстремистских ресурсов занимается Генпрокуратура. За ограничение доступа к сайтам отвечают интернет провайдеры, действующие на основании обращения Роскомнадзора. [4]

«ВКонтакте» подверглась критике со стороны пользователей за целую серию уголовных дел об экстремизме, в которых фигурировали ее пользователи. На участившиеся случаи с возбуждением дел за публикации социальная сеть ответила возможностью сделать профиль полностью приватным, оставив его открытым только для друзей.

Для эффективной борьбы с пропагандой экстремизма как во «Вконтакте», так и в других социальных сетях необходимо наличие действенного механизма по осуществлению непрерывного мониторинга и оперативного блокирования вредоносного контента и принятия мер в рамках законодательства РФ в отношении лиц, распространяющих данный контент. Все это следует проводить строго в соответствии с действующим законодательством РФ для недопущения нарушения прав и свобод граждан страны.

Зачастую требуется незамедлительно ограничить доступ пользователей социальных сетей к контенту, содержащему призывы к экстремистским действиям, однако для этого требуется дождаться окончания официальной

процедуры по признанию его экстремистским, т.е. решения суда и внесения страницы в единый реестр экстремистских сайтов. [1] С другой стороны, блокировка с технической точки зрения должна осуществляться корректно, уже имели место случаи, когда из-за наличия контента, признанногоэкстремистским, блокировались видеохостинг Youtube.com и социальная сеть facebook.com. Имели место факты блокировки некоторых серверов google, что создало неудобства всем российским пользователям почты gmail, так как заблокированный сервер отвечал за вложенные документы в почте.

Несмотря на усилия правоохранительных органов по выявлению и блокировке экстремистского контента, в российских социальных сетях до сих пор не составляет никакого труда отыскать группы и отдельных пользователей, выступающих за нарушение территориальной целостности Российской Федерации, либо сообщества религиозных фундаменталистов, ведущих там открытую пропаганду и призывы к убийствам людей иной веры. Поэтому необходимо развивать взаимодействие на основе действующего законодательства РФ с руководством социальных сетей для блокировки конкретного пользователя, распространяющего экстремистские материалы, блокировки экстремистских групп в рамках социальной сети, так как это не допустит полную блокировку ресурса из-за наличия там вышеуказанных материалов. Для этого и необходимо развивать систему мониторинга социальных сетей.

Для российского Интернет-пространства необходимо наличие структур, которые могут успешно осуществлять мониторинг социальных сетей и своевременно информировать правоохранительные органы о фактах пропаганды политического и религиозного экстремизма. Это позволит существенно повысить эффективность по противодействию экстремизму, не давая заинтересованным лицам вести пропаганду и распространение экстремистских материалов.

Список литературы:

1. Гладышев В., «Социальные сети как инструмент для пропаганды экстремизма» [Электронный ресурс]// http://nac.gov.ru/publikacii/stati-knigi-broshyury/gladyshev-v-socialnye-seti-kak-instrument-dlya.html

2. Центрально Административный Округ города Москвы «Особенности профилактики и борьбы с проявлениями экстремизма и терроризма в молодежной среде» [Электронный ресурс]// https://cao.mos.ru/countering-extremism/features-for-the-prevention-and-suppression-of-manifestations-of-extremism-and-terrorism-in-the-yout/

3. Радио «Свобода», выпуск от 10 апреля 2019 [Электронный ресурс] // https://www.svoboda.org/a/29873361.html

4. Российское новостное интернет-издание «Lenta.ru» от 26 ноября, 22:20 [Электронный ресурс]// https://lenta.ru/news/2019/04/09/vk_extremizm/

5. Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 08.06.2020) "Об информации, информационных технологиях и о защите информации"

Матвеев Даниил Дмитриевич
Юридический институт
АлтГУ, г. Барнаул
Научный руководитель: Соколов Александр Сергеевич
старший преподаватель кафедры уголовного процесса и криминалистики
Юридический институт
АлтГУ, г. Барнаул

Матвеев Д.Д. ПОЯВЛЕНИЕ ЭКСТРЕМИСТСКОГО НАЦИОНАЛИЗМА В РОССИИ

Проблема появление экстремистского национализма в России уходит своими корнями в конец 90-ых, начало 2000-ых годов. Именно тогда, после распада СССР, в Россию массово хлынули представители различных этносоциальных групп, в том числе таджики, грузины, кавказцы, армяне и другие. Однако не все население России расценивали проводимую миграционную политику как приемлемой. Тогда стали зарождаться первые движения скинхедов, и активизировались праворадикальные партии.

Одно из современных новостных изданий проводило исследования связанные с национализмом начала 90-ых годов. В данном исследовании были представлены две основные националистические организации 90-х годов, РНЕ-Русское национальное единство, просуществовавшее до 2000 года, и НБП-национально большевистская партия, просуществовала до 2010 года. РНЕ был присущ национализм, условно рабочего класса в который входили люди отслужившие, военные, охранники, бывшие милиционеры и люди, которые хотели на них походить. Для которых военные были образцом. А национализм НБП, условно, представлял собой национализм интеллигенции. В ней состояли художники, интеллектуалы, и те, кто хотел на них походить, - в большинстве своём студенты или молодые люди студенческого возраста. При этом и те, и другие признавали себя союзниками. [1]

Готовя материал данной статьи нам вспомнились события 1825 года. Когда в Российской империи, после войны с Францией, образовалось два аппозиционных течения, Северное и Южное общества, которые преследовали единую цель, но контингент входивший в их число и способы свержения монархии были разными.

Однако время шло, и стали появляться более радикальные организации такие как «Боевая организация русских националистов», которая за время

своего существования успела совершить 11 убийств, в число умерщвлённых входили представители восточных национальностей, антифашисты и журналистка Анастасия Бабурова, российская журналистка, активистка антифашистского движения. Была убита в центре Москвы вместе с адвокатом С. Ю. Маркеловым по политическим мотивам.

К середине 2000-ых годов, полиция была серьёзно озабочена появлением нового радикального движения - скинхедов, первую волну которого удалось свести на нет.

Так, например в Москве, если видели школьника в одежде характерной для представителя данной субкультуры, которая представляла из себя джинсы, ботинки Dr.Martins, тонкие подтяжки, белую шнуровку и рубашку, то его задерживали, ставили на учёт в детскую комнату милиции, а также проводили разъяснительные беседы. Главной отличительной чертой выступала наголо бритая голова, свидетельствующая о причастность к продолжателям фашисткой идеологии.

В результате активных мероприятий, направленных на подавление распространения праворадикальной субкультуры среди школьников, были достигнуты результаты по снижению распространения идеологии, однако подавить полностью не удалось.

Движение праворадикальных субкультур переродилось после событий 2000-ых годов, таких как теракт на Дубровке в 2002 году, когда был захвачен театр в центре Москвы боевиками в ответ на военные действия на Кавказе, а также теракт в школе Беслана и взрывы многоэтажных домов в Москве, которые привели к огромным жертвам среди мирного населения, и в результате которых, националистические движения вновь активизировались.

Одним из идеологических лидеров выступил Марцинкевич М.С., более известный как (Тесак). В 2009 году против него было возбужденно уголовное дело по 282 статье УК РФ, о разжигании межрасовой ненависти. Уголовное дело было возбужденно в результате анализа его видеороликов, выложенных в сети Интернет, в которых он не лестно отзывался о мигрантах и миграционной политики России.

Марцинкевич М.С., считал, что гастарбайтеры забирают работу у граждан России, призывал к депортации указанных граждан и применение по отношению к ним самосуда. В период с 2007 по 2013 год, Марцинкевич М.С. был трижды привлечен к уголовной ответственности по статье 282 УК РФ (разжигание межнациональной ненависти). Марцинкевич М.С. был не единственным привлеченным лицом в России кого задерживали по статье 282 УКРФ. Так, «26 марта 2015 года, в квартирах четырех московских националистов прошли обыски в рамках уголовного дела, возбужденного Главным следственным управлением (ГСУ) Следственного комитета (СК) по городу Москве еще месяц назад, 27 февраля. Фигурантами обысков стали Дмитрий Демушкин — глава этнополитического объединения «Русские», Владимир Ермолаев и Денис Тюкин — члены руководства той же организации,

а также Владилен Кралин (Владимир Тор) — один из лидеров незарегистрированной Национально-демократической партии (НДП).[2] [3]

Данные лица привлекались к уголовному преследованию за организацию так называемых “Русских маршей”.

По данным источников в сети Интернет, первый «Русский марш» состоялся в 2005 году, через год после учреждения Дня народного единства. Националисты успешно воспользовались этим, фактически «монополизировав» событие.

«Русский марш» представляет собой протестный политический ритуал, состоящий из марша со скандированием националистических лозунгов и призывов политического характера. Это одно из немногих подобных событий, повторяющихся ежегодно и позволяющих изучить взаимодействие националистических активистов и государственных властей.

С развитием новых технологий и подключением все большего количества абонентов к сети интернет, экстремизм, как и любое явление в современном мире получил развитие во всемирной сети Интернет.

По официальным данным Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор), в 2017 году на территории Российской Федерации по запросу генпрокуратуры было заблокировано 13,5 тысяч сайтов, а в 2020 году 50 тысяч сайтов, связанных с тематикой экстремизма, призыва к массовым беспорядкам и несанкционированным митингам.[4]

Однако, это не мешает появлению все новых и новых объединений в сети интернет, в частности в популярной социальной сети “Вконтакте”. Данные сообщества пропагандирую не только ненависть к представителям средней Азии, но и открытую Русофобию. Национализм в современном мире имеет под собой не только этническую ненависть, но и конфессиональную неприязнь.

Самым громким из недавних событий, которые произвели резонанс на общественность стали угрозы в адрес журналистки Собчак К.А.. Так 27 октября 2020 года, Собчак К.А. в социальной сети Instagram, опубликовала пост, в поддержку лидера Франции Эммануэля Макрона, который незадолго до этого выступил с речью в память об убитом учителе, показавшем на своем уроке карикатуру на пророка Мухаммеда.

Российским представители ислама были оскорблены тем, что Собчак К.А. поддерживает французского лидера, и в её адрес было направлено множество угроз её жизни и здоровья.

При этом, мир знает и более старые примеры Исламского национализма. Такие как Исламское Государство (запрещенная на территории Российской Федерации организация) «Хизб ут-Тахрир (запрещенная на территории Российской Федерации организация) «международная панисламистская политическая партия, основанная в 1953 году в Восточном Иерусалиме судьёй местного шариатского апелляционного суда Такиюддином ан-Набхани»и иные.

Указанные националистические движения преследуют единую цель - создание во всем мире единого Халифата, представляющего собой исламскую сверхдержаву.

По сведениям различных источников количество задержанных и осужденных лиц в России за преступления в области национальной безопасности, в том числе сторонников Хизб ут-Тахрир (запрещенной на территории Российской Федерации организация) варьируется от 300-600 человек начиная с 2007 года.

Данные организации ведут вербовку в свои ряды по средствам социальных сетей, таких как: Вконтакте, Viber, WhatsApp и Telegram. Основным контингентом на кого направлены действия по вербованию в ряды экстремистких организаций являются молодые люди, женщины в возрасте от 25 до 35 лет.

Высокая численность представителей женского пола в рядах ИГ (Запрешенной на территории Российской Федерации) обусловлена тем, что вербовщики данных экстремистских объединений в совершенстве владеют социальной инженерией и работают как тонкие психологи, входя в доверие к своей жертве и будущей ячейки экстремистка-террористического подразделения.

По данным информационного агентства «Звезда» за период с 2014 по 2016 годы в мире было завербовано в ряды ИГИЛ (запрещенной на территории Российской Федерации организации) от 27 до 31 тыс. человек.[5]

Анализируя указанную информацию, в ходе подготовке настоящего материала, мы пришли к выводу, что в настоящее время, дестабилизировать политическую стабильность в Российской Федерации кроме политических объединений в виде аппозиции, может три вида объединений:

1. Остатки праворадикальных группировок, разбросанных по всей стране, кроме регионов в которых в большинстве своём проживают представители Средней Азии.
2. Этнополитические объединения, такие как «Русские» в число которых входит – создание парламентской партии националистического характера
3. Террористические организации ведущие незаконную деятельность на территории Российской Федерации с целью дестабилизации политическую обстановку на территории России в целом.

Список литературы:

1. Дмитрий Сергеев / Откуда появился ИГИЛ: как террористы смогли добиться могущества на Ближнем Востоке / [Электронный ресурс] информационное агентство “Звезда” / доступ открытый - https://tvzvezda.ru/news/vstrane_i_mire/content/201712191049-w5o1.htm?utm_source=tvzvezda&utm_medium=longpage&utm_campaign=longpage&utm_term=v1

2. "Уголовный кодекс Российской Федерации" от 13.06.1996 N 63-ФЗ (ред. от 27.10.2020) о “ Возбуждение ненависти либо вражды, а равно унижение человеческого достоинства” [Электронный ресурс] // СПС КонсультантПлюс: Законодательство: Версия Публ. – URL: http://www.consultant.ru/document/cons_doc_LAW_10699/d350878ee36f956a74c2c86830d066eafce20149/

3. РИА НОВОСТИ / Роскомнадзор в 2017 году заблокировал 13,5 тысячи экстремистских сайтов / [Электронный ресурс] / Информационное агентство РИА НОВОСТИ / доступ открытый - https://ria.ru/20180220/1514993958.html

4. ТАСС / В 2020 году заблокировали 30 тыс. интернет-ресурсов с негативным контентом / [Электронный ресурс] / Информационное агентство ТАСС / доступ открытый - https://tass.ru/obschestvo/9283355

5. Виктория Взятышева /Каким был национализм 90-х? Социологи рассказывают о скинхедах и нападениях на мигрантов в России/ [Электронный ресурс] Информационное агентство Бумага / доступ открытый - https://paperpaper.ru/photos/kakim-byl-nacionalizm-v-90-e-otkuda-v-ros/

Ходакова Анастасия Евгеньевна,
Юридический институт АлтГУ, г. Барнаул
Научный руководитель: Мазуров Валерий Анатольевич,
кандидат юридических наук,
доцент кафедры уголовного права и криминологии АлтГУ

Ходакова А.Е. ОСОБЕННОСТИ ПРОФИЛАКТИКИ И БОРЬБЫ С ПРОЯВЛЕНИЯМИ ЭКСТРЕМИЗМА В СОЦИАЛЬНЫХ СЕТЯХ

На сегодняшний день социальные сети являются неотъемлемой частью жизни большинства жителей нашей планеты. В широком смысле «социальная сеть» представляет собой онлайн-платформу, которая используется для общения, знакомств, создания социальных отношений между людьми, которые имеют схожие интересы, также для развлечения (музыка, фильмы) и работы.

Но в последнее время участились случаи, когда социальные сети используются во вред своему прямому назначению, а именно как площадка для пропаганды экстремистских идей, вербовки в террористические организации, призывов к антиправительственным митингам, вступления в неофашисткие сообщества и т. д. Это связано с тем, что сфера социальных сетей не имеет законодательного регулирования, интернет, в частности социальные сети, не имеют территориальных границ, всебольше пользователей социальных сетей стали использовать фальшивые аккаунты с вымышленными именами и фамилиями, все это в совокупности дает зеленый свет радикально настроенным против существующих общепризнанных общественных норм и правил в государстве гражданам использовать социальные сети как инструмент достижения своих экстремистских идейи выражения своего собственного мнения не боясь наступления негативных последствий.

В данном случае сущность экстремизма проявляется в достижении социально-политических, религиозных, национальных целей путем демонстрировании крайних взглядов и методов действия, радикальном отрицании существующих общественных норм и правил в государстве со стороны отдельных лиц или групп посредством использования социальных сетей. Это может проявляться в размещении фото/видео/аудио материалов,побуждающих ненависть либо вражду, а также унижающих достоинства человека либо группы лиц по признакам пола, расы, национальности, языка, происхождения, отношения к религии, а равно принадлежности к какой-либо социальной группе и т.п.

Поэтому возникшая проблема с проявлением экстремизма в социальных сетях является актуальной, и соответственно требует современных способов и методов ее разрешения.

В связи с этим необходимо в первую очередь проводить профилактические мероприятия. Так, например, привитие устойчивых нравственных принципов как: уважение прав и свобод граждан, запрет на дискриминацию по признаку пола, расы национальности, вероисповедания, религии и.тд, должно происходить в детском и подростковом возрасте, а также просвещение со стороны учителей и родителей о правилах поведения в сети интернет. Так как воспитание в семье, формирование правосознания и нравственного мировоззрения человека имеют важное значение в криминологической характеристике личности экстремиста.

В настоящее время среди приоритетных задач в рамках противодействия экстремизму выделяют информационно-психологическое противодействие распространению идеологии терроризма и экстремизма в молодежной среде. На территории Российской Федерации созданы центры противодействия экстремизму и терроризму в интернете и центры мониторинга, такие как Центр изучения и сетевого мониторинга молодежной среды, Национальный центр информационного противодействия терроризму и экстремизму в образовательной среде и сети Интернет (НЦПТИ) и многие другие, активно сотрудничающие с Роскомнадзором, Министерством науки и высшего образования Российской Федерации, Министерством просвещения Российской Федерации, силовыми ведомствами.

Так, Центр изучения и сетевого мониторинга молодежной среды выявляет информацию, касающуюся детского суицида, кибербуллинга, распространения криминальной субкультуры и других деструктивных тенденций в молодёжной среде.

Национальный центр информационного противодействия терроризму и экстремизму в образовательной среде и сети Интернет (НЦПТИ) осуществляет активное противодействие распространению идеологии терроризма и экстремизма, совершенствование работы по информационно-пропагандистскому обеспечению антитеррористических мероприятий в сети Интернет, привлечению молодежи и студентов к разработке теоретических и методологических основ противодействия идеологии терроризма. При поддержке НЦПТИ создано уникальное общественное движение по работе с молодежью — проект «Интернет без угроз», направленный на развитие гражданского самосознания пользователей сети Интернет, на распространение полезного контента и помощи правоохранительным органам в вопросах, связанных с поиском противоправного контента.

Обобщая все выше сказанное, можно сделать вывод о том, что современная молодежь формирует свои установки и ценности посредством общения и получения информации в социальных сетях. Понимая это, идеологи экстремистских движений и групп активно воздействуют на сознание молодых граждан, используя социальные сети и возможности информационной

коммуникации в мессенджерах, что подтверждается статистическими данными и анализом материалов средств массовой информации. Социальные сети позволяют размещать материалы разного жанра, а также быстро их распространять методом снежного кома или же цепной реакции, через репост, что обеспечивает охват относительно большой аудитории за очень короткое время.

В рамках мер противодействия экстремизму в социальных сетях и мессенджерах государственными органами и некоммерческими организациями (НЦПТИ, Центр изучения и сетевого мониторинга молодежной среды и другими) осуществляется большая работа по различным направлениям: разработка и совершенствование законодательной базы, направленной против использования интернета в экстремистских и террористических целях; информационное противодействие молодежному экстремизму посредством интернет-мониторинга (региональный проект «Интернет без угроз»), позволяющего в режиме реального времени осуществлять компьютерный контент-анализ, лингвистический аналииз текстовых потоков, содержащих различные материалы экстремистского характера.

Центральное внимание стоит уделить методам борьбы с экстремизмом в социальных сетях.

Одной из основных проблем борьбы с проявлениями экстремизма в социальных сетях являются проблема отсутствия законодательного регулирования отношений, возникающих в связи с использованием социальной сети. При этом, принимая во внимание отсутствие у социальных сетей географических границ, необходимо развивать международное сотрудничество по урегулированию отношений в рассматриваемой области (создавать международные договоры, определяющие как статус международного информационного пространства, так и алгоритмы разрешения споров, вопросы оказания правовой помощи и т.п.).

Для успешной борьбы с проявлениями экстремизма в социальных сетях необходим комплекс мер, который включает в себя в первую очередь совершенствование по использованию информации в сети Интернет, а также ее контролю. В рамках данного направления представляется необходимым развитие и международного сотрудничества.

Как уже отмечалось огромное количество информации в сети Интернет и социальных сетях, делает невозможным ее ручной контроль. Существенно затруднены и технический контроль содержания информации, а анонимность пользователей затрудняет также установление лица, разметившего информацию. В связи с этим вторым направлением является совершенствование существующих и разработка новых технических и программных средств, позволяющих контролировать (оценивать) информацию и устанавливать лиц, ее размещающих.

Третьим направлением является совершенствование взаимодействия правоохранительных органов с провайдерами, организаторами и создателями сайтов и блогов в целях недопущения размещения и своевременного

блокирования информации экстремистского содержания. Также представляется необходимым совершенствование взаимодействия с общественностью. Данное взаимодействие должно предусматривать проведение разъяснительной работы с пользователями сети Интернет, а также получение от них информации о сайтах и информации экстремистского содержания.

Следующим направлением должно явиться разработка единых критериев и методик исследования информации по выявлению признаков экстремизма.

Только комплексный подход позволит повысить эффективность противодействия распространению экстремизма в социальных сетях и сети Интернет в целом.

Также хотелось отметить, что мной было проведено собственное исследование в виде проведения онлайн-опроса среди студентов юридического института АлтГУ в социальной сети «ВКонтакте» и выявлено их отношение к проявлению экстремизма в социальных сетях. Всего в опросе было задействовано 27 человек, среди них 59,3 % представителей женского пола и 40,7 % мужского пола. Возрастной диапазон составил от 17 до 22 лет.

Большинство респондентов чаще всего используют такие социальные сети как: ВКонтакте, InstagramиYouTube. Подавляющая часть опрошенных уделяют по 4-5 часов в день социальным сетям, при этом только 18,5% отвечающих часто сталкиваются с экстремистским контентом в сети и 70,4 % сталкиваются, но редко.

Как показало исследование, сегодняшнее молодое поколение предпочитает никак не реагировать на проявление экстремизма в социальных сетях, 59,3 % опрошенных увидев картинку, унижающую чувства верующих или человеческое достоинство либо дискриминацию по признаку пола, расы или национальности предпочтут ничего не делать. 33,7 и 7,4 % опрошенных отправляют такой материал в спам (рассылка без согласия получателя) и отправляют жалобу администрации аккаунта или сообщества как материал, содержащий экстремизм или враждебное высказывание.

Больше половины респондентов считают обоснованным привлечение к уголовной ответственности за размещение, а равно за распространение фото/видео/аудио материалов с экстремистским содержанием, 37% опрошенных воздержались от квалификации деяния и ответили «не знаю».

В завершение можно сказать, что профилактика идеологии экстремизма среди молодежи в социальных сетях является очень важной задачей для современного общества. При этом решение данной задачи требует принятия следующих мер:

- ведение постоянного мониторинга Интернет-пространства с целью выявления и блокирования материалов экстремистской направленности;
- предоставление возможности подключения к процессу выявления противоправного контента бдительных Интернет-пользователей;
- разработка и актуализация методического обеспечения процесса информационного противодействия экстремизму;

- ведение разъяснительной работы с целью описания сущности экстремизма, а также формирование стойкого неприятия обществом идеологии насилия;

- привлечение молодежи к участию в противодействии терроризму, экстремизму, национализму и религиозному фундаментализму в образовательной среде.

Список литературы:

1. Распоряжение Правительства РФ от 29.11.2014 N 2403-р «Об утверждении Основ государственной молодежной политики Российской Федерации на период до 2025 года». [Электронный документ]. URL: http://www.consultant.ru/ document/cons_doc_LAW_171835/ (датаобращения: 25.10.2020).

2. Болдырев Евгений Вячеславович, Гонтаренко Надежда Николаевна - Молодежный экстремизм в социальных сетях: анализ основных трендов и мер противодействия

3. Грибанов Е. В. Экстремизм в молодежной среде в контексте этнокультурной коммуникации // Актуальные вопросы противодействия экстремизму и терроризму: сб. матер.межвуз. круглого стола. Воронеж, 2015.

Курепина Любовь Константиновна
Юридический институт, АлтГУ, г. Барнаул

Курепина Л.К. ПРОТИВОДЕЙСТВИЕ ИДЕОЛОГИИ ТЕРРОРИЗМА, РАСПРОСТРАНЯЕМОЙ СРЕДИ ПОДРОСТКОВ В СЕТИ «ИНТЕРНЕТ»

В настоящее время в сети «Интернет» очень обширно распространяется и пропагандируется идеология терроризма. Особому влиянию террористической идеологии подвержены подростки. Сложившаяся ситуация требует отдельного внимания со стороны правоохранительных органов, потому что у несовершеннолетних граждан имеются отдельные особенности психики, а отсюда и поведения.

Существуют различные способы распространения идеологии терроризма: семинары по вербовке лиц, печатные брошюры, книги, статьи и т.д. В их число на сегодняшний день входят и социальные сети. Роль социальных сетей принимает все большее значение в жизни человека. Используя социальную сеть, можно с легкостью общаться с людьми на другой половине земного шара, можно быстро узнать необходимую информацию. Так же несложно найти интересующего человека, причем это займет считанные секунды, так как довольно часто социальные сети (например, Одноклассники, ВКонтакте, Instagram, Телеграмм) в качестве регистрации предлагают людям указывать о себе многое: размещать фотографии и видео, указывать интересы, излюбленные места посещения, информацию о работе, об образовании, делиться с личными мыслями, участвовать в опросах, по которым можно определить отношение человека к той или иной проблеме, и другое. По таким данным можно легко воссоздать полный (в том числе и психологический) портрет конкретного пользователя, а кроме того – подбирать потенциальную аудиторию вербовщикам террористических организаций.

Практически все крупные международные террористические структуры широко используют в информационно-пропагандистских акциях, ориентированных на подростков, сеть «Интернет», учитывая ее доступность и популярность в подростковой среде. Согласно проведенного специалистами аппарата НАК анализа использования террористическими и экстремистскими организациями ресурсов сети «Интернет», в 1998 году террористические структуры поддерживали в развивающейся на тот момент «всемирной паутине» всего 12 сайтов. Уже к 2005 году их насчитывалось около 4800, а в настоящее время, по оценкам экспертов, – около 10 тысяч. Кроме того, в сети функционирует большое количество новостных агентств и сайтов напрямую не аффилированных с террористическими организациями, но разделяющих их идеологию и оказывающих террористам поддержку в различных формах. Многие сайты специально постоянно меняют свой адрес, а в структуры

экстремистских и террористических объединений все чаще входят специалисты, как правило, из числа молодых программистов, владеющие навыками компьютерного взлома и т.п. В сети «Интернет» в настоящее время работают около 200 только русскоязычных сайтов, поддерживающих идеи терроризма и экстремизма.

Стратегия национальной безопасности Российской Федерации до 2020 года к числу основных источников угроз национальной безопасности в сфере государственной и общественной безопасности относит деятельность террористических организаций, группировок и отдельных лиц, направленную на насильственное изменение основ конституционного строя Российской Федерации, дезорганизацию нормального функционирования органов государственной власти, а также экстремистскую деятельность националистических, религиозных, этнических и иных организаций и структур, направленную на нарушение единства и территориальной целостности Российской Федерации, дестабилизацию внутриполитической и социальной ситуации в стране.

В ряде регионов России накоплен немалый положительный опыт работы в сети. Так, в 2009 году по инициативе активистов студенческих организаций и молодых ученых столичных вузов с целью информационного противодействия экстремизму и терроризму в сети «Интернет», были созданы следующие интернет-ресурсы: портал «Наука и образование против террора», сайт «Молодежь за Чистый Интернет», сайт «Молодежь за Честный Интернет». На указанных информационных ресурсах, блогах и форумах освещаются и обсуждаются темы: о деятельности идеологов и руководителей террористического бандподполья, их сообщников, а также иных структур, работающих в интересах организаций экстремистского и террористического толка; о неприятии идеологии терроризма и религиозно-политического экстремизма; об уважительном отношении к традиционным религиям; высказывания духовных лидеров основных конфессий, в том числе авторитетных исламских богословов Саудовской Аравии и Египта, осуждающих терроризм; размещаются материалы деятельности федеральных органов исполнительной власти, НАК в сфере противодействия терроризму, информация о научно-теоретических, информационно-пропагандистских мероприятиях антитеррористической направленности в России и за рубежом. Успех контртеррористической работы в сети «Интернет» в значительной мере зависит от того, насколько она ведется регулярно, наступательно и профессионально. Это направление противодействия идеологии экстремизма и терроризма имеет особое значение для профилактики указанных крайне опасных социальных явлений в подростковой среде.

Я считаю, что помимо всех проводимых мер, необходимо также обязать каждую школу в городе иметь профессионального психолога, в обязанности которого должно входить проведение различных мероприятий, направленных на противодействие распространению террористической идеологии. Также необходимо распространять информации об ужасных и необратимых

последствиях террористических актов в сети «Интернет», то есть на таких порталах, как «Вконтакте», «Инстаграм», «Ютуб» и др. для лучшего восприятия несовершеннолетней аудиторией. В таком формате можно как писать различные агитационные статьи, так и снимать познавательные видеоролики.

Список литературы:

1. Статья «Противодействие идеологии терроризма в социальных сетях» [Электронный ресурс]. Режим доступа http://www.eduportal44.ru/npo/Pl

2. Статья «Противодействие идеологии терроризма в социальных сетях» [Электронный ресурс]. Режим доступа http://www.honestnet.ru/terrorizm/protivodeystvie-ideologii-terrorizma-v-sotsialnyh-setyah.html

3. Статья « Противодействие идеологии терроризма в сети "Интернет"» [Электронный ресурс]. Режим доступа https://marfino.mos.ru/antiferro/recommendations-on-rules-of-personal-safety/countering-the-ideology-of-terrorism-in-the-internet.php

Кондрахина Эльвира Владиславовна
Юридический институт, АлтГУ, г. Барнаул
Научный руководитель: Соколов Александр Сергеевич,
старший преподаватель кафедры уголовного процесса и криминалистики,
Юридический институт АлтГУ, г. Барнаул

Кондрахина Э.В. БОРЬБА С ЭКСТРЕМИЗМОМ И ТЕРРОРИЗМОМ В КИБЕРПРОСТРАНСТВЕ

Экстремизм, острая проблема современности, чаще проявляется в политической, экономической, религиозной и др. сфер общественной жизни. Существуют разные точки зрения о появлении экстремизма в России, одни считают, что зародилось данное явление когда появилось социальное неравенство, разделение общества на классы позволило одним «возвыситься» над другими. В следствии этого угнетённая масса населения стала совершать действия и поступки для получения заветных благ. Другие считают, что данное явление появилось в XIX веке, при Александре II и продолжило развиваться. http://ivo.garant.ru/ - /document-relations/12127578/1/0/10111Экстремизм - (лат. extremus - крайний) - ориентация в политике на крайне радикальные идеи и цели, достижение которых осуществляется в основном силовыми, а также нелегитимными и противоправными методами и средствами [1].

Экстремизм в киберпространстве - один из многих видов киберугроз, которые вызывают всеобщую озабоченность. Имея пространственные характеристики, оно с уверенностью повторяет характерные черты реальной социальности. Явления по типу экстремизма находят там свои проявления, проблемы зависимости, киберпреступности, экстремизма в киберпространстве и крайней его форме – терроризме. Интернет привлекает своей лёгкой доступностью, возможность анонимного общения, быстрой передачи информации и др. Выделяют различные формы интернет-экстремизма. К ним относятся: троллинг, буллинг, астротурфинг и др. Троллинг часто проявляется среди пользователей социальных сетей и многопользовательских онлайн игр. Его можно определить как попытку манипулирования объектом-жертвой путём передачи провокационных сообщений через канал связи между пользователями, которые вызывают разногласия с принятыми этическими нормами общения, психические расстройства и импортирование полученных моральных проблем в реальный мир.

Астротурфинг использует многоступенчатую систему воздействия на жертву в интернете (навязчивая реклама, опасные ссылки, вирусы, боты) с целью политического, социального, духовного негативного воздействия, в том числе социально опасного, экстремистского (пропаганда идей расовой

неприязни, насилия, употребления и распространения запрещённых веществ и т.д.).

Кибербуллинг - агрессивное умышленное воздействие психо-социального характера на жертву в интернете, со стороны одного лица или группы лиц [2].

Серьезную роль в противодействии экстремизму и терроризму играют правоохранительные органы, прежде всего, органы внутренних дел. В Федеральном законе от 7 февраля 2011 г. N 3-ФЗ «О полиции» в числе важнейших обязанностей полиции определены предупреждение, выявление и пресечение экстремистской деятельности общественных объединений, религиозных и иных организаций, граждан; участие в мероприятиях по противодействию терроризму и в обеспечении правового режима контртеррористической операции, а также в обеспечении защиты потенциальных объектов террористических посягательств и мест массового пребывания граждан, в проведении экспертной оценки состояния антитеррористической защищенности и безопасности объектов. По данным специализированных служб ГУ МВД России по Северо-Кавказскому федеральному округу в ходе информационно-технического мониторинга осуществляется контроль над содержанием более 100 информационных ресурсов сети Интернет этно-националистического и псевдорелигиозного характера. В их числе: около 20 русскоязычных экстремистских интернет-сайтов, пропагандирующих радикальную псевдоисламскую идеологию, и более 30 сайтов – материалы этно-националистического толка [3].

Так же разработана стратегия в целях обеспечения дальнейшей реализации государственной политики в сфере противодействия экстремизму в Российской Федерации, а также в целях конкретизации положений Федерального закона от 25 июля 2002 г. № 114-ФЗ "О противодействии экстремистской деятельности" и Указа Президента Российской Федерации от 31 декабря 2015 г. № 683 "О Стратегии национальной безопасности Российской Федерации". Данная стратегия реализуется в два этапа. На первом этапе реализации настоящей Стратегии планируется осуществить следующие мероприятия:

а) разработка и принятие законодательных и иных нормативных правовых актов Российской Федерации, субъектов Российской Федерации, направленных на противодействие экстремизму;

б) выполнение мероприятий, предусмотренных планом мероприятий по реализации настоящей Стратегии;

в) проведение мониторинга результатов, достигнутых при реализации настоящей Стратегии;

г) прогнозирование развития ситуации в области межнациональных (межэтнических) и межконфессиональных отношений в Российской Федерации и возникновения экстремистских угроз;

д) обеспечение вовлечения институтов гражданского общества в деятельность, направленную на противодействие экстремизму;

е) создание системы дополнительной защиты информационно-телекоммуникационных сетей, включая сеть "Интернет", от проникновения экстремистской идеологии.

На втором этапе реализации настоящей Стратегии планируется обобщить результаты ее реализации и при необходимости подготовить предложения по разработке новых документов стратегического планирования в сфере противодействия экстремизму [4].

Актуальная проблема в борьбе с кибер-экстремизмом заключается в стремительном росте преступности, вызванной развитием технологий, и сложность в расследование дел связанных с данным правонарушением. Так в Алтайском крае с 2010 по 2017 годы регистрировали от 40 до 48 тыс. преступлений за год. До 2012 года включительно их число составляло 5−8 преступлений. Резкий взлёт зарегистрированных случаев экстремизма случился в 2013 году — 21 за год. В следующие три года этот показатель колебался в пределах 25−29 преступлений.

В 2016 году в крае на 10% снизилось число экстремистских преступлений. В 2017 году произошёл новый взлёт: правоохранители зарегистрировали 45 случаев, рост составил 73,1%.

В 2018 году правоохранительными органами края выявлено 17 преступлений экстремистской направленности, совершенных с использованием сети Интернет, из указанного числа 14 уголовно наказуемых деяний задокументировано сотрудниками полиции. За 2018 год сотрудниками органов внутренних дел края задокументировано 62 административных правонарушения экстремистской направленности (2017 год – 98), в том числе предусмотренных ст. 20.2 КоАП РФ (Нарушение установленного порядка организации либо проведения собрания, митинга, демонстрации, шествия или пикетирования) – 2; ст. 20.3 КоАП РФ (Пропаганда либо публичное демонстрирование нацистской атрибутики) – 28; ст. 20.29 КоАП РФ (Производство и распространение экстремистских материалов) – 32. Из указанного числа выявленных административных правонарушений экстремистской направленности 56 совершены с использованием сети Интернет, из них 25 касалось демонстрации и пропаганды нацистской символики (ст. 20.3 КоАП РФ) и 31 – распространения экстремистских материалов (ст. 20.29 КоАП РФ).На данный момент число таких преступлений растёт [5]. В течение 2019 года сотрудниками ОВД края задокументировано 80 административных правонарушений экстремистской направленности (2018 год – 62), в том числе предусмотренных ст. 20.2 КоАП РФ (Нарушение установленного порядка организации либо проведения собрания, митинга, демонстрации, шествия или пикетирования) – 2, ст. 20.3 КоАП РФ (Пропаганда либо публичное демонстрирование нацистской атрибутики) – 10, ст. 20.3.1 КоАП РФ (Возбуждение ненависти либо вражды, а равно унижение человеческого достоинства) – 3, ст. 20.29 КоАП РФ (Производство и распространение экстремистских материалов) – 65. Все выявленные административные правонарушения экстремистской направленности, за

исключением противоправного деяния, ответственность за которое предусмотрено ст. 20.2 КоАП РФ, совершены с использованием сети Интернет.

Решением данной проблемы, будет создание программного обеспечения для сбора информации по экстремизму и терроризму. Такая информационно-поисковая (или информационно-разведывательная) форма противодействия экстремизму, будет эффективной. В задачу граждан должно входить: 1) повышенная бдительность и сообщения о подозрениях в правоохранительные органы; 2) активная гражданская позиция, проявляющаяся в антиэкстремистских выступлениях граждан в средствах массовой информации; 3) сотрудничество с правоохранительными органами. Осведомитель сможет передавать веб-ссылки на источники, содержащие сведения экстремистской и террористкой направленности и подтверждающую фотофиксацию представителям органов правопорядка, получая за это вознаграждение. За каждого найденное правонарушение, имеющие экстремистской или террористической направленности, дают баллы, эти баллы можно будет тратить, например, на посещение культурных мероприятий. С другой стороны, сотрудники правоохранительных органов смогут быстро получать актуальную информация о правонарушении, эффективность их работы увеличится.

Затраты на данную деятельность минимальные, так как образуются только из разработки, внедрения и поддержки необходимого программного обеспечения.

Задача программного обеспечения выходит не только на уровень субъектов или отдельно взятой странны, а на мировой. При создании данного программного обеспечения, можно сократить число правонарушений в интернет пространстве, привлекая внимание общественности к данной проблеме.

Список литературы:

1. Соснов Н. Экстремизм: история и современность. - [Электронный ресурс]. - Режим доступа: http://vestnikburi.com/ekstremizm-istoriya-i-sovremennost/

2. А. М. Кустов. Труды Академии управления МВД России. 2017. №3 (43).профессор кафедры управления органами расследования преступлений, доктор юридических наук, профессор (Академия управления МВД России).

3. С.Н. Миронова. Деятельность правоохранительных органов по противодействию экстремизму и терроризму: материалы всероссийского круглого стола (г. Казань, 30 ноября 2017 г.) / под.ред. – Казань: КЮИ МВД России, 2017 – 160 с.

4. Указ Президента Российской Федерации от 29.05.2020г. №344 «Об утверждении Стратегии противодействия экстремизму в Российской Федерации до 2025 года» // СПС КонсультантПлюс

Куликова Анна Владимировна
Юридический институт АлтГУ, , г. Барнаул
Научный руководитель: Мазуров Валерий Анатольевич,
кандидат юридических наук,
доцент кафедры уголовного права и криминологии АлтГУ

Куликова А.В. ПРОПАГАНДА ТЕРРОРИСТИЧЕСКОЙ ИДЕОЛОГИИ В СЕТИ «ИНТЕРНЕТ»

Тема терроризма в современном мире и его информационном поле является одной из самых актуальных. Она представляет из себя серьезную проблему в настоящее время и значительную угрозу в будущем. Терроризм является одним из наиболее негативных факторов, влияющих на всю жизнь общества.

Киберпространство по своему функциональному назначению, в том числе информационно-телекоммуникационная сеть Интернет, сегодня по многим параметрам является наиболее привлекательным средством для экстремистско - террористической деятельности. Сразу хочется озадачить себя вопросом - а почему? Дело в том, что интернет до сих пор остается неподвластным пространством, где каждый так или иначе волен творить и делать, что он хочет. При лучшем раскладе - в рамках закона, а при худшем - использовать его как для пропаганды своих взглядов, так и для непосредственной подготовки террористических актов. Наибольшую опасность пропаганды идеологии терроризма состоит в том, что основным адресатом указанных материалов является молодежь, как подрастающее поколение с еще не сформировавшимся мироощущением.

В прошлом было не легко организовать и исполнить террористические акты из-за расстояния между «исполнителями» и координации их действий. Сейчас же обе эти проблемы легко решаемы, ведь у всех есть доступ к Интернету, а также к СМИ, через которые можно просочить «свою пропаганду».

Любой теракт – это информационно- пропагандистская акция, призванная привлечь внимание как можно большего количества людей.

По мнению директора Национального центра информационного противодействия терроризму и экстремизму в образовательной среде и сети Интернет Чурилова С.А., причинами того, что Интернет в современном мире стал идеальным инструментом пропаганды террористической деятельности, являются: возможность широкого охвата аудитории; высокая скорость и лавинообразный характер распространения информации через интернет -

ресурсы, социальные сети и блоги, возможность для анонимного ведения противоправной деятельности.

Терроризм относится к числу самых тяжких преступлений по законам Российской Федерации. Существует огромное количество определений терроризма, но предлагаем обратиться к легальному, закрепленному в статье 3 Федеральный закон от 06.03.2006 N 35-ФЗ"О противодействии терроризму». Под понятием терроризма понимают идеологию насилия и практику воздействия на принятие решения органами государственной власти, органами местного самоуправления или международными организациями, связанные с устрашением населения и (или) иными формами противоправных насильственных действий.

Деятельность террористов в Интернете можно классифицировать следующим образом:

Активизм — это «легитимное» использование интернета для пропаганды своих идей, а именно для заработка и увеличения численности;

Хакерство — это хакерские атаки, проводимые с целью выведения из строя отдельных компьютерных сетей либо интернет-сайтов, для получения доступа к секретной информации и т. д.;

Кибертерроризм — это компьютерные атаки, спланированные с целью нанесения максимального ущерба жизненно важным объектам информационной инфраструктуры.

Терроризм в сети опасен тем, что террористы могут атаковать или проникнуть внутрь компьютерных систем и от этого могут пострадать военные, разведывательные службы.

Предлагаем разобраться с тем, какие же цели выдвигают перед собой террористы в сети Интернет. Так или иначе нельзя выделить основную, поскольку все они будут «работать» только в совокупности.

Начнем с пропаганды террористической идеологии. Осуществляется она посредством распространения справочных и агитационных материалов. Для многих террористических группировок глобальная сеть стала средством подготовки новых активистов и исполнителей терактов.

Реклама террористической и экстремистской деятельности, в основном проявляется, как скрытая, ведь руководители группировок на деле те еще психологи, которые мастерски могут проникнуть в сознание людей. Исходя из статистики: индивидуальные террористические действия совершают психически нездоровые люди, идущие на преступление под влиянием только им понятных мотивов.

Запугивание, дезинформация, разрушение эмоциональных и поведенческих установок индивида будут являться еще одной целью террористов. Можно ли считать террористический акт оружием психологического воздействия? Или же люди, которые в силу тех или иных причин, поддались на провокации и пропаганду, просто оказались не в то время и не в том месте?

Говоря о террористических актах, сразу всплывает в памяти «стокгольмский синдром», под которым обычно подразумевается психическое состояние, когда подвергшийся насилию или похищению человек начинает проявлять сочувствие по отношению к обидчику вместо более уместных страха и ненависти. Автором термина выступил швед Нильс Бейерут. В тот период криминалист анализировал нестандартную ситуацию, наблюдавшуюся в ходе захвата заложников при ограблении банка и поразившую весь мир. Как раз данный синдром будет выступать одним из негативных последний, носящих долговременный характер.

Поддержание взаимодействия и связи внутри террористической организации и террористических сообществ между собой - для этой цели широко используются социальные сети. Посредством них поддерживается связь между руководителями и исполнителями, в том числе поддерживается координация действий, а также для отправки тайных сообщений.

Еще одна цель - противодействие пропаганде противника.

У террористической пропаганды есть свой «слушатель». Она нацелена на определенные типы аудитории, а именно - противники, которых нужно запугать; международная общественность, у которой необходимо сформировать соответствующее мнение о деятельности террористических и антитеррористических организаций.; сочувствующие - главная задача работы с ними – агитация, вербовка, подготовка новых активистов; активные члены, с которыми посредством интернета осуществляется связь.

Статья 205.1. УК РФ занимает ведущее положение в криминализации преступлений террористической направленности, диспозиция которой содержит перечень составов преступлений (ст. ст. 205, 205.2, 205.3, 205.4, 205.5, 206, 208, 211, 220, 221, 277, 278, 279, 360 и 361 УК РФ). При этом перечень преступлений, закрепленный в примечании 1 к ст. 205.1 УК РФ отличается от перечня преступлений, содержащихся в ч. 1 ст. 205.1 УК РФ.

Давайте раскроем состав преступления. Объектом будет выступать общественная опасность. Объективная сторона характеризуется альтернативно любым из следующих действий:

склонение лица к совершению хотя бы одного из преступлений, предусмотренных ст. 205, 206, 208, 211, 277, 278, 279 и 360 УК РФ;

вербовка лица для совершения хотя бы одного из вышеперечисленных преступлений;

иное вовлечение лица в свершение любого из перечисленных деяний;

подготовка лица к совершению хотя бы одного из указанных преступлений;

финансирование терроризма;

Субъективная сторона: характеризуется прямым умыслом. Лицо осознает общественную опасность совершаемых действий и желает их совершить. Обязательным субъективным признаком склонения, вербовки, иного вовлечения, вооружения и подготовки является специальная цель совершения

хотя бы одного из преступлений, предусмотренных ст. 205, 206, 208, 211, 277, 278, 279 и 360 УК РФ.

С момента своего появления ст. 205.1 УК РФ стала предметом активных дискуссий среди представителей юридической науки. За непродолжительный срок существования нормы в УК РФ в нее вносились многочисленные изменения (в 2009, 2010, 2014 и 2016 гг.), которые усложнили ее понимание и в результате лишь усилили критику со стороны теоретиков права.

С введением ст. 205.1 в УК РФ основное направление критики законодателя связано с тем, что новая норма, по мнению исследователей, нарушила систему взаимодействия положений Общей и Особенной частей уголовного закона. Утвердилась позиция, согласно которой в ст. 205.1 УК РФ предусмотрена ответственность традиционно понимаемого подстрекателя, регламентируемая в ч. 4 ст. 33 УК РФ, но уже в качестве исполнителя содействия террористической деятельности по ст. 205.1 УК РФ, что в результате привело к деструктуризации УК. На этом основании в научной литературе широкое распространение получили предложения полностью вывести ст. 205.1 из УК РФ или исключить из нее признаки, дублирующие положения ст. 33 УК.

Пленум Верховного Суда РФ также не делает различий между склонением, вербовкой и вовлечением, давая единое толкование всем трем терминам в Постановлении «О некоторых вопросах судебной практики по уголовным делам о преступлениях террористической направленности» от 9 февр. 2012 г. No 1 (ред. от 3 нояб. 2016 г. No 41).

Решение включить ст. 205.1 в УК РФ было обусловлено необходимостью криминализировать не вербовку как таковую, а связанные с ней деяния.

Далее необходимо откатиться к статье 205.2 УК РФ, которая предусматривает ответственность также за публичные призывы к осуществлению террористической деятельности.

Криминализация публичных призывов имеет социальные предпосылки, которые обусловлены общественной опасностью деяния. Как уже ранее говорилось, призывы, как мы считаем, будут являться именно способом достижения поставленных террористом целей. Нельзя недооценивать призывы, подготавливаю таким образом почву, террорист «выращивает» своих союзников, подталкивает к совершению преступления. Следствие этого - дестабилизация обстановки в стране.

Совершение публичных призывов посягает на общественную безопасность. Само понятие достаточно размыто, но можно сказать, что призывы определенно вызывают воздействие на сознание, волю и поведение людей с какой-то определенной целью.

В объективной стороне остава преступления ст. 205.2 УК РФ просматриваются два альтернативных действия

1. призывами к осуществлению террористической деятельности
2. оправданием терроризма.

Конвенция Совета Европы «О предупреждении терроризма» не содержит обязательств для стран-частниц по криминализации оправдания терроризма. Включение в диспозицию ст. 205.2 УК РФ публичного оправдания терроризма, наряду с публичными призывами к осуществлению террористической деятельности, не связано с имплементацией конвенционных положений и является инициативой законодателя. Оправдание терроризма признается преступлением не всеми странами - участницами названного договора, а только конкретным государством.

Призывы - это обращение, воздействующее на сознание и волю людей в целях возбуждения у них желания вести себя определенным образом, в данном случае —-осуществлять террористическую деятельность. Разъяснением этого термина, дано в п. 18 Постановления Пленума Верховного Суда РФ «О некоторых вопросах судебной практики по уголовным делам о преступлениях террористической направленности». Призывы должны выражаться в глаголах повелительного наклонения, которые указывают на желание обращающегося склонить аудиторию к определенному поведению. Призывы могут осуществляться в любой форме: устной, письменной, содержаться в аудио- или видеообращении.

Такие призывы, как правило, будут получать огласку в открытом доступе в сети Интернет. Согласно диспозиции ст. 205.2 УК РФ, виновный призывает к осуществлению террористической деятельности. Понятие террористической деятельности раскрывается в ст. 3 Федерального закона «О противодействии терроризму»путем перечисления действий, составляющих его содержание.

Согласно ст. 1 Федерального закона «О противодействии экстремистской деятельности», террористическая деятельность является разновидностью экстремизма. В УК РФ есть самостоятельная норма, посвященная ответственности за публичные призывы - ст. 280.

В соответствии с примечанием к ст. 282.1 УК под преступлениями экстремистской направленности понимаются преступления, совершенные по мотивам политической, идеологической, расовой, национальной или религиозной ненависти или вражды в отношении какой-либо социальной группы. Примерами могут служить осуществление массовых беспорядков, хулиганских действий и актов вандализма по мотивам идеологической, политической, расовой, национальной или религиозной ненависти либо вражды в отношении какой-либо социальной группы, а также пропаганда и публичное демонстрирование нацистской атрибутики или символики, финансирование экстремистской деятельности либо иное содействование ее осуществлению.

Для более подробного раскрытия понятия экстремизма предлагаем обратиться к ФЗ «О противодействии экстремистской деятельности» (в ред. от 25.12.2012) , в соответствии с которым экстремистская деятельность (экстремизм) — это деятельность общественных и религиозных объединений, либо иных организаций, либо СМИ, либо физических лиц по планированию, организации, подготовке и совершению деяний, направленных на насильственное изменение основ конституционного строя и нарушение

целостности РФ; на подрыв безопасности РФ; на захват или присвоение властных полномочий; на создание НВФ, на осуществление террористической деятельности, на возбуждение расовой, национальной или религиозной розни, а также социальной вражды, связанной с насилием или призывами к насилию; на унижение национального достоинства.

Под призывами целесообразно понимать действия с целью побуждения осуществлению такой деятельности.

Ст. 205.2 УК РФ в части публичных призывов к осуществлению террористической деятельности предусматривает ответственность за разновидность преступного поведения, предусмотренного ст. 282 УК РФ. Ст.205.2 УК РФ предусматривает ответственность за призывы к осуществлению террористической деятельности лишь в том случае, если они совершены публично.

Содержание признака публичности также раскрывается в Постановлении Пленума Верховного Суда РФ «О некоторых вопросах судебной практики по уголовным делам о преступлениях террористической направленности». Согласно п. 18 данного акта, публичным может быть обращение к другим лицам, выраженное в любой форме (устной, письменной, с использованием технических средств, информационно-телекоммуникационных сетей).

Использование компьютерных сетей отвечает признакам публичности при осуществлении пропаганды идеологии терроризма. При использовании «закрытых сайтов», просмотр которых возможен только при применении пароля не исключает признаков публичности.

Если же информацию, связанную с пропагандой идеологии терроризма

пользователь обнаруживает в своем почтовом ящике, то публичность будет иметь место лишь в тех случаях когда файлы отправлялись неопределенному кругу лиц.

Можно сделать вывод о том, что публичность не будет означать обращение к конкретным субъектам правоотношений. Их опасность состоит в том, что данное действие, а именно призыв к определенным действиям, предусмотренных диспозицией статей УК РФ, адресуется к неопределенному кругу лиц.

Как ранее говорилось, интернет с его легкодоступностью будет являться хорошим подспорьем для деятельности террористов.

Рассмотрим несколько способов, с помощью которых можно использовать интернет с целью содействия террористическим группам:

1. Террористы могут осуществлять сбор информации о целях, включая местонахождение целей и их характеристики;

2. Осуществление сбора средств для поддержки какого-либо движения.

3. Совершение сборов различных групп людей и дача им указания о времени и месте проведения встречи, формах различных протестов;

4. Осуществление нападений на людей, вымогательство денег;

5. Возможность обращения к большому числу людей, повсеместная реклама в интернете, активность пользователей;

6. Использование для вселения паники в массы, введение в заблуждение;

Следует констатировать, что за последние десять лет экстремистские и террористические организации прочно обосновались во всех сегментах Интернета и используют его в качестве основного инструмента по распространению радикальной идеологии.

Заметим и тот факт, что идеология терроризма, направлена на лиц, чья психика более восприимчива.

Профилактической работы состоит не в том, чтобы устрашить строгой юридической ответственностью за совершение преступлений террористической направленности в рамках, а, в первую очередь, в том, чтобы сформировать убеждение, что совершение террористического акта неприемлемо, прежде всего, с позиции общечеловеческой морали, гуманного отношения к человеку.

Нужно помнить о том, что в нынешних реалиях сложно отследить действия людей в сети, а особенно детей. Несовершеннолетние будут являться группой риска, которым нужно особое внимание и бдительность. Не просто так все проблемы во взрослой жизни порождены и связаны с детством. Если перед ребенком прообраз человека, причиняющего боль, татаркой пример в дальнейшем может послужить толчком к совершению противоправных действий, усилению его агрессии.

Выработка мер, непосредственно направленных на борьбу с каким либо наиболее опасным посягательством процесс сложный и должен охватывать всевозможные способы регулирования общественных отношений.

Первоочередной задачей, по нашему мнению будет выработка определенных механизмов защиты всего информационного пространства от распространения информации, пропагандирующей идеологию терроризма.

Защита граждан от негативного информационного воздействия не может содержать в себе какое-то одно направление. Защита должна проявляться в комплексной системе мер, разработанных и продуманных тщательным образом. В первую очередь, меры должны быть направлены на молодежь, как на наиболее подверженную социальную группу.

Считаем значительным в работе по выявлению и предотвращению указанной идеологии, а также пропаганды в сети Интернет проведение мониторинга ресурсов на предмет содержания информации о такой идеологии. Мониторинг в будущем поможет быстро и качественно блокировать все ресурсы, используемые террористами для достижения своих целей.

Список литературы:

1. "Конституция Российской Федерации" (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020)

2. «Уголовный кодекс Российской Федерации" от 13.06.1996 N 63-ФЗ (ред. от 31.07.2020)

3. Федеральный закон "О противодействии экстремистской деятельности" от 25.07.2002 N 114-ФЗ (последняя редакция)

4. Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ (последняя редакция)

5. Федеральный закон "О свободе совести и о религиозных объединениях" от 26.09.1997 N 125-ФЗ (последняя редакция)

6. Федеральный закон "О противодействии терроризму" от 06.03.2006 N 35-ФЗ (последняя редакция)

7. Постановление Пленума Верховного Суда РФ от 09.02.2012 N 1 (ред. от 03.11.2016) "О некоторых вопросах судебной практики по уголовным делам о преступлениях террористической направленности"

8. Жаворонкова Татьяна Вячеславовна Использование сети Интернет террористическими и экстремистскими организациями // Вестник ОГУ. 2015. №3 (178). URL: https://cyberleninka.ru/article/n/ispolzovanie-seti-internet-terroristicheskimi-i-ekstremistskimi-organizatsiyami (дата обращения: 25.11.2020).

9. Тарбагаев Алексей Николаевич, Москалев Георгий Леонидович Публичные призывы к осуществлению террористической деятельности (ст. 205.2 УК РФ): проблемы уголовно-правовой регламентации и квалификации // Вестник СПбГУ. Серия 14. Право. 2016. №2. URL: https://cyberleninka.ru/article/n/publichnye-prizyvy-k-osuschestvleniyu-terroristicheskoy-deyatelnosti-st-205-2-uk-rf-problemy-ugolovno-pravovoy-reglamentatsii-i (дата обращения: 25.11.2020).

10. Буткевич Сергей Анатольевич Экстремизм и терроризм в киберпространстве: выявление, нейтрализация и предупреждение // Вестник КРУ МВД России. 2018. №1 (39). URL: https://cyberleninka.ru/article/n/ekstremizm-i-terrorizm-v-kiberprostranstve-vyyavlenie-neytralizatsiya-i-preduprezhdenie (дата обращения: 25.11.2020).

11. Мухамбетов, Ж. С. Терроризм в сети / Ж. С. Мухамбетов, А. О. Цымбалий. — Текст : непосредственный // Молодой ученый. — 2018. — № 11 (197). — С. 59-62. — URL: https://moluch.ru/archive/197/48723/ (дата обращения: 15.11.2020).

12. Таова Л.Ю. Экстремизм и терроризм – глобальные проблемы современного общества // ИСОМ. 2016. №5-1. URL: https://cyberleninka.ru/article/n/ekstremizm-i-terrorizm-globalnye-problemy-sovremennogo-obschestva-1 (дата обращения: 25.11.2020).

13. Пинкевич Татьяна Валентиновна, Черных Евгения Евгеньевна Публичные призывы к осуществлению террористической деятельности или публичное оправдание терроризма: проблемы квалификации // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2014. №3 (27). URL: https://cyberleninka.ru/article/n/publichnye-prizyvy-k-osuschestvleniyu-terroristicheskoy-deyatelnosti-ili-publichnoe-opravdanie-terrorizma-problemy-kvalifikatsii (дата обращения: 25.11.2020).

14. Горбунов Константин Георгиевич Противодействие террористической пропаганде в Интернете // ОмГУ. 2016. №2. URL: https://cyberleninka.ru/article/n/protivodeystvie-terroristicheskoy-propagande-v-internete (дата обращения: 25.11.2020).

15. https://news.rambler.ru/other/43616582/?utm_content=news_media&utm_medium=read_more&utm_source=copylink

СЕКЦИЯ «ПРИОРИТЕТНЫЕ НАПРАВЛЕНИЯ ПРОТИВОДЕЙСТВИЯ ЭКСТРЕМИЗМУ И ИДЕОЛОГИИ ТЕРРОРИЗМА В ОБРАЗОВАТЕЛЬНОЙ СФЕРЕ И МОЛОДЕЖНОЙ СРЕДЕ»

Саенко Арина Александровна
Колледж АлтГУ
Стародубцева Мария Александровна,
ассистент кафедры уголовного права и криминологии
юридического института АлтГУ

Саенко А.А., Стародубцева М.А. О ПРОБЛЕМЕ НЕОБХОДИМОСТИ ПОВЫШЕНИЯ ПРАВОВОЙ КУЛЬТУРЫ УЧИТЕЛЕЙ И ПРЕПОДАВАТЕЛЕЙ В ВОПРОСАХ ПРОФИЛАКТИКИ ЭКСТРЕМИЗМА И ИДЕОЛОГИИ ТЕРРОРИЗМА В ОБРАЗОВАТЕЛЬНОЙ СРЕДЕ

В обоснование актуальности нашей темы, отметим, что в 2020 году объявленный в марте локдаун фактически «выключил» многих людей из системы общественных отношений, породил всплеск преступности и значительное ухудшение криминогенной обстановки. Почти на 41% возросло число совершенных преступлений экстремистской направленности. Причем, как указывает статистика, большинство из лиц, совершивших данные деяния, являются несовершеннолетними.

Вынужденная самоизоляция повлекла падение уровня обучения, вырвала молодежь из привычного им мира, привела подростков фактически в маргинальное состояние хрупкого баланса между нормой и патологией [1,2]. Плюсом к этому добавилось массированное психологическое воздействие СМИ и сети «Интернет», где свободно действуют потенциальные вербовщики в экстремистские и террористические объединения.

А, как известно, именно молодежь является «группой воздействия» для подобных лиц, поскольку обладает неустойчивым социально-психологическим фоном и не до конца сформированным мировоззрением [3]. Сюда добавляется и крайняя нестабильность экономической ситуации в стране, рост безработицы и инфляции.

В таких условиях обычный подростковый максимализм приобретает крайние черты, перерастающие в экстремистские настроения. Непредсказуемость действий несовершеннолетнего, его спонтанность и

нередко группой характер действий обуславливает повышенную опасность молодежного экстремизма [4, 5].

Нами было проведено эмпирическое исследование – анонимное анкетирование школьников, студентов и преподавателей по вопросу их правовой осведомленности в отношении экстремизма. Опрошены были 74 человека, разделенных нами на две группы. Из них 45 человек – студенты 1-2 курса СПО (Колледж АлтГУ), ученики 9-11 классов МКОУ «Гилевская СОШ». 29 опрошенных- преподаватели Колледжа ФГБОУ ВО «Алтайский государственный университет», МКОУ «Гилевская СОШ». Возраст респондентов первой группы 15-17 лет, возраст второй группы – 30-50 лет.

Прежде всего, респондентам предлагалось ответить на вопрос, известно ли им, что такое экстремизм. В группе школьников и студентов 97,8% отвечающих сообщили, что знают этот термин, 2,2% ответили отказом. В группе учителей и преподавателей 100% сообщили о знании данного понятия. Можно отметить, что правовая культура нашей выборки находится на достаточно высоком уровне.

Далее респондентам предлагалось ответить на вопрос о причинах экстремизма. Студенты и школьники отметили в качестве основной причины деформацию системы ценностей в обществе (35,6%). Причем, так ответили именно студенты по большей части. 20% считает причиной экстремизма недостаточное правовое просвещение граждан, 15,6% отмечают недостаточную досуговую занятость детей подросткового возраста и взрослого населения. 13,3% указали кризис школьного и семейного воспитания как фактор роста экстремистских проявлений и только 8,9% считают основным условием многонациональность населения. Это косвенно говорит об отсутствии у респондентов склонности к националистическим идеям и установкам.

Группа опрошенных педагогов также основной причиной отметила деформацию общественных ценностей (41,4%). 27,6% назвали причиной экстремизма недостаточную терпимость людей, нехватку толерантности. Здесь, как раз и подразумевалась многонациональность, весьма актуальная для Алтайского края, с его высоким процентом иностранных мигрантов. 17,2% указывают недостаточное правовое просвещение населения.

На вопрос «Какие способы профилактики экстремизма наиболее приемлемы с Вашей точки зрения?» школьники и студенты в 62,8% случаев указали радикальные, допускающие ужесточение уголовной ответственности за экстремизм, недопущение создания и функционирования новых религиозных и национальных объединений, тотальную цензуру. 27,9% респондентов отметили способы, основанные на опыте зарубежных стран в профилактике экстремизма. 9,3% опрошенных признают право на существование либеральных способов противодействия экстремизму. Укажем, что данная картина ярко отражает как раз такой признак молодежи как максимализм, желание «выделиться из толпы». Большинство опрошенных стремятся именно к радикальным мерам разрешения проблемы, не оглядываясь на последствия.

У взрослых респондентов картина совершенно иная. 62,1% опрошенных указывают в качестве профилактики экстремизма способы, основанные на опыте зарубежных стран, придерживаются центристской позиции. 27,6% за радикальные методы, и 10,3% за либеральные рычаги воздействия, позволяющие создание и функционирование новых религиозных и национальных объединений, отсутствие всякой цензуры.

Касательно актуальности темы экстремизма для Алтайского края, обе группы респондентов согласились с тезисом, что тема скорее актуальна, чем не актуальна (42% и 51% соответственно).

26,7% опрошенных школьников и студентов признали, что сталкивались с проявлениями экстремизма. Это признали и 13,7% преподавателей. Мы видим, что тема для участников выборки не столь уж оторвана от непосредственного восприятия. Однако, здесь речь идет, чаще всего, о новостях и публикациях в СМИ.

Непосредственно отдельные факты дискриминации в отношении себя признали 11,1% школьников и 27,6% преподавателей. Здесь картина уже более любопытна. Свою роль, вероятно, играет и трансграничность региона, обилие транспортных потоков, проходящих через него, высокая доля трудовой миграции и, соответственно, довольно большая доля интолерантного поведения.

69% педагогов знают о программах мероприятий по профилактике экстремизма и идеологии терроризма в их образовательных учреждениях. Однако, 31% ответил отказом, что означает невовлеченность в подобные мероприятия практически трети педагогического состава. Это можно объяснить как большой нагрузкой, так и неосведомленностью либо нежеланием учителей тратить время на правовое просвещение. 48,3% респондентов – преподавателей отметили, что не участвуют в подобных мероприятиях, соответственно, не участвуют и их кураторские группы /классы.

Такой высокий процент невовлеченных в воспитательные мероприятия просветительского и гражданско-патриотического профиля вызывает определенные опасения. Отсюда мы можем выделить «группу риска», лиц, не знающих о проявлениях экстремизма и способных подпасть под влияние потенциальных вербовщиков. Также, 41,4% педагогов считают мероприятия по профилактике экстремизма неэффективными.

В определенном смысле данные мероприятия направлены исключительно на повышение правовой культуры студентов и преподавателей, и по отношению к непосредственному воздействию на обучающихся они действительно не приносят мгновенного результата. Плюс стоит отметить, что часто на такие лекции студентов и школьников загоняют «для галочки», чтобы заполнить аудитории и отчитаться о выполнении календарного плана воспитательной работы. Но даже в этом случае, нельзя просто отмахиваться от подобной работы со студентами и школьниками. А именно это мы и наблюдаем, по данным нашего опроса.

Отсюда мы предлагаем сделать упор на вовлеченности в мероприятия по профилактике экстремизма и идеологии терроризма педагогов образовательных учреждений. Мало собрать студентов на лекцию, важно проводить научно-образовательные семинары для преподавателей, повышать их правовую культуру. Необходимо, чтобы у педагогов выработался интерес к таким просветительским и гражданско-патриотическим мероприятиям, и тогда они начнут вовлекать в них студентов. А для этого необходима слаженная работа образовательных учреждений, правоохранительных органов и институтов гражданского общества.

Выдвигаемые нами тезисы было решено проверить на практике. В ходе исследования мы решили доказать, что осведомленность молодежи о мерах профилактики экстремизма и терроризма повысится именно после проведения преподавателями правильно выстроенных тематических классных и кураторских часов. Чтобы доказать это было проведено профилактическое мероприятие «Экстремизм в молодежной среде» среди школьников старших классов МКОУ «Гилевская СОШ» . В связи с условиями пандемии, мероприятие было проведено в дистанционном формате, но это не помешало нам с ребятами рассмотреть все важные аспекты данной темы. В ходе мероприятия были затронуты такие вопросы как:

1. Что такое экстремизм?
2. Чем он опасен?
3. Какой бывает экстремизм?
4. Кто входит в «зону риска» потенциальных вербовщиков?
5. Как не попасться на уловки вербовщиков?
6. Как бороться с экстремизмом?

В ходе беседы ребята проявляли интерес, активно задавали свои вопросы. Ученики были крайне обеспокоены тем, что может произойти в нашем государстве, если не бороться с такой глобальной проблемой 21 века, как экстремизм.

На рис. 1 представлена фотоэкспозиция мероприятия.

Рис. 1 Профилактическое мероприятие «Экстремизм в молодежной среде», проведенное среди школьников старших классов МКОУ «Гилевская СОШ»

Мероприятие показало, что на самом деле наше молодое поколение по - настоящему болеет за мирное будущее, и регулярные мероприятия по профилактике экстремизма действительно будут идти им на пользу. Ребята признались, что впервые за все время обучения, мероприятие было им интересно. Это и говорит о том, насколько важно повысить интерес к подобным мероприятиям прежде всего у преподавателей, которые уже личным примером будут давать ученикам соответствующую нравственно-психологическую установку.

Список литературы:

1. Абрамова Г.С. Практическая психология: учебное пособие. М.: Прометей, 2018.538 с.
2. Адорно Т. Исследование авторитарной личности / Под общей редакцией доктора философских наук В.П. Култыгина. М.: «Серебряные нити», 2001. 416 с.
3. Аминов И. И. Юридическая психология: учебное пособие. М.: Юнити-Дана, 2014. 270 с.
4. Андронникова О. О. Гендерная дифференциация в психологии: учебное пособие. М.: Инфра-М, 2017. 262 с.
5. Арутюнов С. А. Этничность - объективная реальность // Этнографическое обозрение. 1995. N 5. С. 19 - 24.

Виснер Алина Николаевна
Колледж АлтГУ, г. Барнаул
Научный руководитель: Стародубцева Мария Александровна
ассистент кафедры уголовного права и криминологии
юридического института АлтГУ

Виснер А.Н. О НЕКОТОРЫХ ПРОБЛЕМАХ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ В РОССИИ

В настоящее время сложно представить жизньчеловека без использования достижений технического и научного прогресса. На протяжении многихлет люди пытаются улучшить качество своей жизни,усовершенствовать имеющиеся технологии. Так, вповседневной деятельности человека появилиськомпьютер, сеть «Интернет», сотовая связь, мобильныйтелефон и т. п. Всеобщая компьютеризация и информатизация населения позволяют намного быстрее икачественнее решать обыденные задачи и достигатьопределенных целей.

К сожалению, технические новшества используются не только законопослушнымигражданами, но ипреступниками. При этом количество преступлений,совершенных с применением информационных технологий увеличивается стремительными темпами.Исходя из официальной статистики МВД России, за январь – ноябрь 2018 г. с использованием компьютерныхи информационно-телекоммуникационных технологийбыло совершено 156 307 преступлений, а за аналогичный период предыдущего года – 82 440.

Крометого, возросло число преступлений в сфере информационно-телекоммуникационных технологий. Поданным Генеральной прокуратуры Российской Федерации, в 2017 г. их количество увеличилось с 65 949до 90 587. Доля такихпреступлений от числа всехзарегистрированных в России преступных деянийсоставляет 4,4 % – это каждое 20 преступление. Показатели первого полугодия 2018 г. также свидетельствуют о росте указанной категории преступлений(+3,4 %).

Анализируя судебную и следственную практику, можно сделать вывод о том, что самыми распространенными киберпреступлениями являются неправомерный доступ к компьютерной информации(ст. 272 УК РФ), создание, использование и распространение вредоносных компьютерных программ(ст. 273 УК РФ), мошеннические действия, совершенные с использованием электронных средств платежа(ст. 159.3 УК РФ).Количество мошенничеств с использованием платежных карт в 2018 г. выросло в 7 раз.Цифры неутешительные, тем более что раскрываемость преступлений в сфере

информационно-телекоммуникационных технологий ежегодно колеблется от 45 до 53 процентов.

Вышесказанное свидетельствует о необходимости разработки соответствующей методики по организации раскрытия и расследования преступлений в сфере компьютерных и информационно-телекоммуникационных технологий. Вопросы противодействия киберпреступности не просто не перестают быть актуальными, а остаются крайне острыми, требующими особого внимания со стороны правоохранительных органов и государства.

По этому поводу неоднократно высказывается Президент Российской Федерации. Так, в июле 2018 г. на Международном конгрессе по кибербезопасности в Москве В. В. Путин озвучил список мер по киберзащите страны, которые намерено принять правительство. В список вошли международное сотрудничество, создание системы обмена информацией о кибератаках, использование отечественного программного обеспечения и подготовка квалифицированных кадров.

Выступая на расширенном заседании коллегии МВД России 28 февраля 2019 г., Президент РФ вновь обращает свое внимание на угрозы, связанные с кибербезопасностью государства и безопасностью информационного пространства.

Действительно, развитие информационно-телекоммуникационных и компьютерных технологий сопровождается активной деятельностью преступников. Однако проблема заключается не только в увеличении числа киберпреступлений, но и в повсеместном распространении таких преступлений во всех сферах. Новейшие компьютерные и информационные технологии используются в незаконном обороте наркотических средств и психотропных веществ, пропаганде деструктивной идеологии, при совершении различного рода мошеннических действий, незаконных финансовых операций и других преступлений.

Одним из примеров громкого киберпреступления является созданный вирус «Petya», ставший угрозой мирового масштаба. Весной 2017 г. по всему миру были зафиксированы атаки вируса-вымогателя «Petya». Принцип действия заключался в полной блокировке операционной системы с предложениемпоследующего выкупа в размере 300 долларов США в биткоинах (на тот момент курс биткоина составлял 1 BTC = 2367 $). В процессе его деятельности пострадали такие крупные компании, как Роснефть, Башнефть, Сбербанк, Хоумкредит и другие.

Разблокировка потребовала кропотливой работы экспертов-криминалистов в сфере информационных технологий и сети Интернет, специалистов по IT-технологиям и сотрудников лаборатории Касперского. По данным из разных источников известно, что указанная вредоносная программа нанесла ущерб более чем 60 странам на общую сумму около $8 млрд.

По данным Сбербанка, ущерб мировому бизнесу от кибератак в 2018 г. вырос до $1,5 трлн, вдвое выросла продолжительность DDoS-атак. Кроме того,

19 февраля 2019 г., заместитель председателя правления Сбербанка Станислав Кузнецов заявил: «… за последние полгода число преступлений, совершаемых с использованием методов социальной инженерии в отношении клиентов банка, увеличилось на 30–40 %» .

Проанализировав современное состояние информационно-телекоммуникационного пространства, имеющуюся научную литературу, аналитические сведения о состоянии преступности и технической оснащенности правоохранительных органов, можно выделить ряд проблем, которые, определенно, требуют скорейшего решения:

–деятельность по раскрытию и расследованию преступлений основана на принципах, некоторые из которых уже неэффективны. В настоящее времяправоохранительные органы с имеющимся арсеналом технических средств и технологий не всегда могут противопоставить себя «новой преступности» с новыми технологиями и новыми способами совершения преступлений;

–до конца не урегулирована система государственных учреждений, проводящих компьютерно-технические и иные судебные экспертизы по делам о преступлениях, совершаемых с использованием информационно-телекоммуникационных технологий;

–не сформированы предмет, методы, цели и задачи цифровой криминалистики. Это новое перспективное направление, требующее осмысления и развития ввиду необходимости разработки практических рекомендаций по работе с электронными, виртуальными, цифровыми следами, компьютерной техникой, интернет-сервисами, приложениями и программным обеспечением. Современный правоохранитель обязан владеть такими навыками;

– в сфере кибербезопасности отсутствует эффективное взаимодействие органов внутренних дел с государством, обществом и учреждениями.

Меры по противодействию кибер-угрозам остаются на декларативном уровне, не получая усовершенствования и усиления. Так, до настоящего времени нет сформированной системы оперативного обмена информацией с банковскими организациями, финансово-кредитными учреждениями и даже с операторами сотовой связи. Сведения необходимо получать путем длительных процедур согласования, направления запросов, писем в службу безопасности, проведения следственных действий судебного санкционирования. Перечисленное влияет на раскрытие преступлений «по горячим следам», усложняет процесс расследования, позволяя преступниками тщательно скрыть следы противоправных действий.

Хотя справедливо будет отметить, что с 1 июля 2018 г. оператор связи обязан хранить в базах данных на территории Российской Федерации текстовые сообщения пользователей услуг связи, голосовую информацию, изображения, звуки, видео-, иные сообщения пользователей услуг связи – до шести месяцев с момента окончания их приема, передачи, доставки и (или) обработки . Таким образом, от оператора связи можно получить любую информацию, в том числе

переданную посредством приложений-мессенджеров (Whatsapp, Telegram, Viber и т. п.). На данный момент считаем данное нововведение положительным для раскрытия и расследования преступлений, однако никаких сведений о применении новшеств на практике нет. Сложно представить, каким образом будут аккумулироваться и храниться огромные массивы информации. К тому же не ясно, насколько эффективны поправки, внесенные в законодательство о связи и иные правовые акты, ведь налицо вторжение в сферу конституционных прав граждан.

Кроме названных выше проблем стоит указать и на недостаточно совершенное законодательство в области противодействия киберпреступлениям (например, не установлена уголовная ответственность за фишинг (компьютерные преступления, основанные на принципах социального инжиниринга) и рассылку вредоносного спама как за отдельный вид преступлений). К сожалению, оставляет желать лучшего система подготовки юридических и технических кадров. В вузах, осуществляющих подготовку сотрудников органов внутренних дел, необходимо разрабатывать новые темы, разделы, спецкурсы, посвященные расследованию преступлений в сфере информационно-телекоммуникационных технологий, кибербезопасности и информационной безопасности. В качестве общей проблемы отметим невысокий уровень компьютерной грамотности и осведомленности о современных киберугрозах большинства населения, в том числе государственных служащих.

На наш взгляд, проведенный анализ охватывает далеко не все проблемы, связанные с кибербезопасностью общества и государства. Более того, с развитием информационно-телекоммуникационных технологий будут появляться новые способы совершения преступлений и методы противодействия правоохранительным органам. Современные условия жизни заставляют бороться с анонимными и неконтролируемыми сервисами, использованием приложений-мессенджеров в преступных целях, «серыми» SIM-картами. Безусловно, нельзя просто ограничить доступ к тем или иным интернет-сервисам. Без должного правового регулирования проблему решить невозможно, необходимо повышать ответственность за размещение в сети запрещенного контента, формировать правовые и организационно-технические механизмы противодействия противоправной деятельности в данной сфере.

Очевидно, что государство ведет активную политику в рамках противодействия киберпреступности и преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий. Однако в данный момент это меры не профилактические, не предупреждающие и не предотвращающие указанный вид преступных посягательств, а, по большей части, – контрмеры в ответ на уже совершенные преступления или действия, направленные на их пресечение. Как бы это печально ни звучало, современный преступник значительно быстрее осваивает просторы Интернета, активнее изучает, разрабатывает и применяет новейшие технические разработки.

Скачок в росте зарегистрированных киберпреступлений мы можем увидеть на рис. 1.

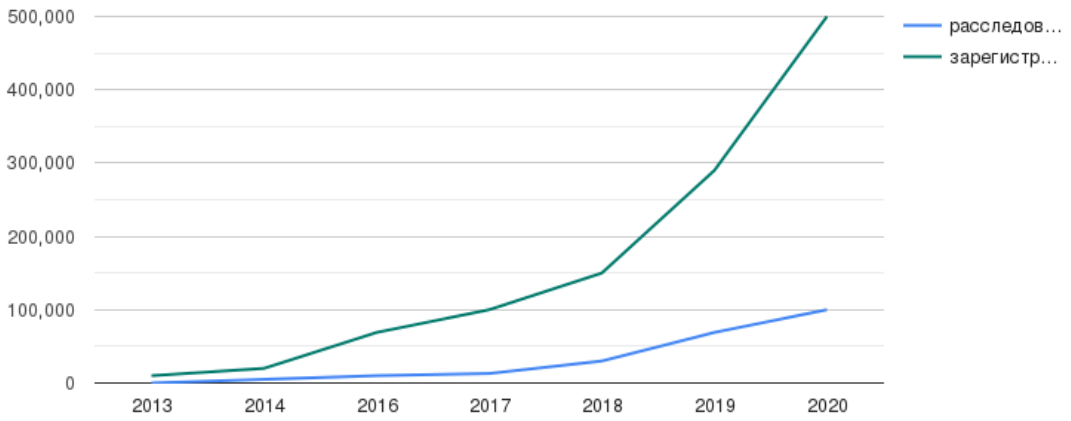

Рис.1 Количество зарегистрированных киберпресуплений в России 2013-2020 гг.

Количество киберпреступлений в первом квартале 2020 года выросло на 83,9%, а удельный вес таких деяний достиг 19,9% от общего числа. В основном из-за этого фактора уровень преступности в стране в целом вырос на 4%.

Прогнозируем к концу 2020 года число зарегистрированных киберпреступлений - около 0,5 млн. Раскрываемость их - не более 23%. Доля в общем числе преступлений по стране - 19%-22%.

Сегодня нам со всей ясностью видно, что российским правоохранительным органам не хватает достаточного числа подготовленных в ИТ сотрудников, отсутствуют методики расследования инновационных преступлений, нет надежных и эффективных информационно-аналитических решений. Отсутствует принципиально новая система криминалистического учета и идентификации в киберпространстве, так необходимая нам сегодня.

Список литературы

1. Гончар В. В. Отдельные вопросы совершенствования подготовки кадров, специализирующихся нарасследовании преступлений, совершаемых с использованием информационных технологий: сборник статей Международной научно-практическойконференции / В. В. Гончар // Криминалистика в условиях развития информационного общества (59-е ежегодные криминалистические чтения). – Москва:Академия управления МВД России, 2018. – С. 73–77.

2. О преступлениях, совершаемых с использованием современных информационнокоммуникационных технологий [Электронный ресурс]. –

URL:https://genproc.gov.ru/smi/news/news-1431104. (дата обращения: 10.11.2020 г.).

3. Официальный сайт Министерства внутреннихдел РФ [Электронный ресурс]. – URL: http://mvd.ru/presscenter/statistics/reports/item/804701 (дата обращения: 20.10.2020 г.).

Дубович Анастасия Андреевна
Колледж АлтГУ, г. Барнаул
Стародубцева Мария Алексндровна,
ассистент кафедры уголовного права и криминологии
юридического института АлтГУ

Дубович А.А., Стародубцева М.А. АНАЛИЗ ДИНАМИКИ ПРЕСТУПНОСТИ ТЕРРОРИСТИЧЕСКОЙ И КИБЕРТЕРРОРИСТИЧЕСКОЙ НАПРАВЛЕННОСТИ В РОССИИ ЗА ПЕРИОД 2016-2019 ГГ.

Криминологический анализ показывает, что в России динамика преступно сти террористической направленности продолжает носить неблагоприятный ха рактер [1]. В частности, указанный тезис подтверждается данными уголовной статистики. Отметим некоторые аспекты преступности данного вида.

В 2017 г. наметилась тенденция к уменьшению числа зарегистрированных преступлений террористического характера на 16 % (1 871) .

Снижение преступлений террористического характера было обусловлено:

решением задач по противодействию распространения радикального ислама;

активизацией деятельности по выявлению и привлечению к уголовной ответственности лидеров и активных членов террористических группировок, осуществляющих вербовку граждан РФ и СНГ для участия в вооруженных конфликтах на стороне международных террористических организаций «исламское государство» и «Джабхат ан-Нусра», а также установлению маршрутов переправки рекрутов;

осуществлением комплекса мер по предупреждению и пресечению террористических проявлений в местах массового пребывания граждан; на предприятиях по производству оружия, боеприпасов и взрывчатых веществ, местах их хранения; на объектах транспортной инфраструктуры, энергетики и связи.

Структура преступлений террористического характера на период 2017 г. включала организацию незаконного вооруженного формирования или участие в нем, ст. 208 УК РФ (39,5 %; 739), организацию деятельности террористической организации и участие в деятельности такой организации, ст. 2055 УК РФ (26,1%; 488), содействие террористической деятельности, ст. 2051 УК РФ (12,3 %; 231), публичные призывы к осуществлению террористической деятельности или публичное оправдание терроризма, ст. 2052 УК РФ (10 %; 187), прохождение обучения в целях осуществления террористической деятельности, ст. 2053 УК РФ (5,5 %; 103), террористический акт, ст. 205 УК РФ (2 %; 37) и иные (4,6 %; 86).

Следует указать, что в 2017 г. выросло число террористических актов (+48 %), а также таких составов, как содействие террористической деятельности (+15,5 %), организация террористического сообщества и участия в нем (ст. 2054 УК РФ) (+300 %).

В 2018 году тенденция к снижению количества террористических преступлений сохранилась.

В январе - декабре 2018 года зарегистрировано 1679 преступлений террористического характера.

Удельный вес преступлений террористического характера от общего числа преступлений за 2018 год составил 0,1 %.

Мы видим ярко выраженную отрицательную динамику преступлений данного вида (- 10,3 %).

Можно сделать вывод о том, что обстановка в Российской Федерации в сфере противодействия терроризму на 2018 год оставалась сложной, но контролируемой правоохранительными органами.

В результате реализации комплекса мер значительно снизилось число совершённых преступлений террористической направленности, сократилось количество терактов.

Как отметил в своем отчете за 2018 год директор ФСБ РФ А.В. Бортников, в ходе контртеррористических операций и отдельных оперативно-боевых мероприятий нейтрализовано 65 боевиков, в том числе 10 главарей бандгрупп; задержано 36 главарей, 236 бандитов и 589 пособников.

В рамках реализации Комплексного плана противодействия идеологии терроризма в Российской Федерации предпринят ряд дополнительных мер по защите информационного пространства от террористических угроз. Роскомнадзором, МВД и ФСБ России во взаимодействии с Генеральной прокуратурой расширено внедрение автоматизированных систем мониторинга средств массовых коммуникаций. Это дало возможность пресечь деятельность по распространению противоправной информации более чем 64 тысяч интернет-ресурсов, из которых свыше 47 тысяч содержали материалы, связанные с деятельностью МТО.

Однако, необходимо отметить, что в 2019 году происходит ухудшение обстановки по указанному виду преступлений. По данным Генеральной Прокуратуры Российской Федерации, за январь-июль 2019 года было зафиксировано 1 108 преступлений террористического характера, что было на 7 единиц или 0,64% больше, чем за аналогичный период предыдущего года. При этом было выявлено 427 лиц, совершивших такие преступления (на 40 человек или 8,57% больше, чем в 2018 году). По 485 террористическим преступлениям было проведено предварительное расследование (на 12 единиц или 2,54 % меньше, чем в предыдущем году), по 347 преступлениям уголовные дела были отправлены в суд. 424 преступления не было раскрыто (на 89 единиц или 26,57% больше, чем в 2018 году). [2]

В итоговом отчете Генеральной прокуратуры РФ за декабрь 2019 г., отмечено, что количество преступлений террористического характера возросло на 7,6 % (с 1 679 до 1 806).

Удельный вес преступности террористического характера за 2019 год составил 0,12 %.

Отмечается положительная динамика данного вида преступлений по сравнению даже с июлем 2019 года.

В 2019 году, по заявлению А.В. Бортникова, в России было предотвращено 50 преступлений террористической направленности и не допущено ни одного теракта.

Всего во время контртеррористических операций и оперативно-боевых мероприятий нейтрализованы 32 бандита, в том числе 9 бандглаварей, 41 главарь банд, 241 боевик и 606 пособников задержаны. Кроме того, в России была пресечена деятельность 78 законспирированных ячеек международных террористических организаций.

Кроме того, на фоне сокращения ресурсной базы боевики ищут новые способы приобретения оружия. Так, в этом году силами МВД, ФСБ и Росгвардии ликвидированы 83 нелегальные мастерские по производству и переделке оружия, нейтрализованы 8 преступных групп, занимавшихся поставками оружия и боеприпасов из зон вооруженных конфликтов.

Приведенная статистика свидетельствует о том, что:

- ежегодно в нашей стране совершается относительно стабильное число преступлений террористического характера около 1000 преступлений в год;
- при этом, в целом, отмечается тенденция к их снижению;
- удельный вес рассматриваемых преступлений составляет около 0,04% в общем количестве всех зарегистрированных преступлений.

Но в этой статистике мы не находим акты кибертерроризма.

Относительно киберпреступности и кибертерроризма стоит отметить, что четкая статистика данных деяний не ведется, и это также можно признать упущением в политике противодействия.

Стоит отметить хронологию случаев наиболее крупных действий кибертеррористов, направленных на приостановку работы российских банков и финансовых организаций за последние три года. В приводимый список не вошли кибертеррористические акты, связанные с похищением средств российских банков.

• 30 сентября 2013 года хакерская группа «Анонимный Кавказ» опубликовала на видеосервисе YouTube видео, в котором объявила о начале операции против российских банков «в отместку за геноцид кавказских народов». По данным «Лаборатории Касперского», 1 октября 2013 года сайт Сбербанка подвергся DDoS-атаке, 2 октября - сайт Альфа-банка, 3 октября - сайты Банка России, Альфа-Банка и Газпромбанка. Целью атаки было ограничение доступа к публичным сайтам банков, но атаки не привели к затруднениям в их работе. В частности, работа сайта ЦБ была прервана всего на семь минут [3].

• 24 марта 2014 года работа сайта Банка России была прервана на период с 09:45 до 11:00 мск в результате DDoS-атаки, мощность которой была более чем в десять раз выше, чем у пропускная способность каналов связи сайта.

• 17 марта 2014 г. российские банки подверглись DDoS-атаке, в результате которой были временно отключены веб-сайт и интернет-сервисы банка ВТБ 24 (атака не затронула работу отделений, банкоматов и пластиковых карт), а также интернет-сервисы. и входит в сеть банкоматов Альфа-Банка. Ответственность за нападение взяла на себя группа "Анонимный Кавказ".

• 2 октября 2015 года «Лаборатория Касперского» объявила, что с 25 сентября она зафиксировала крупнейшую с начала года волну длительных DDoS-атак на веб-сайты и системы онлайн-ссылок восьми крупных российских банков. Половина атакованных кредитных организаций получила сообщения от организаторов этой волны DDoS с требованием заплатить выкуп, чтобы остановить атаки на криптовалюту биткойн. Это обстоятельство позволило экспертам «Лаборатории Касперского» предположить, что за атаками стоит хакерская группа DD4BC, которая ранее в 2015 году также требовала выкуп в биткойнах во время атак на банки и финансовые учреждения в других странах. Инциденты не причинили ущерба российским банкам.

• 10 ноября 2016 года FinCERT (организация Банка России по борьбе с киберпреступлениями) зафиксировала хакерские DDoS-атаки на несколько крупных банков и передала эту информацию правоохранительным органам. Сообщалось, в частности, что 8 ноября 2016 года Сбербанк отразил серию мощных DDoS-атак, организованных из нескольких десятков стран. По данным газеты «Ведомости», аналогичным кибератакам подверглись Альфабанк, Банк Москвы (структура ВТБ) и Московская биржа. СМИ сообщили, что также пострадали банк «Открытие» и Росбанк.

• По данным FinCERT, в атаке участвовали ботнеты с устройств так называемого «Интернета вещей», нарушений доступности банковских сервисов не зафиксировано. По данным «Лаборатории Касперского», киберпреступники атаковали сайты как минимум пяти известных финансовых организаций из ТОП-10. Эта серия атак стала первой крупномасштабной волной DDoS-атак на российские банки в 2016 году.

Стоит также отметить, что огромное количество атак являются не зарегистрированными. Это обуславливаются несколькими причинами, представленными в рисунке 1. (рис.1).

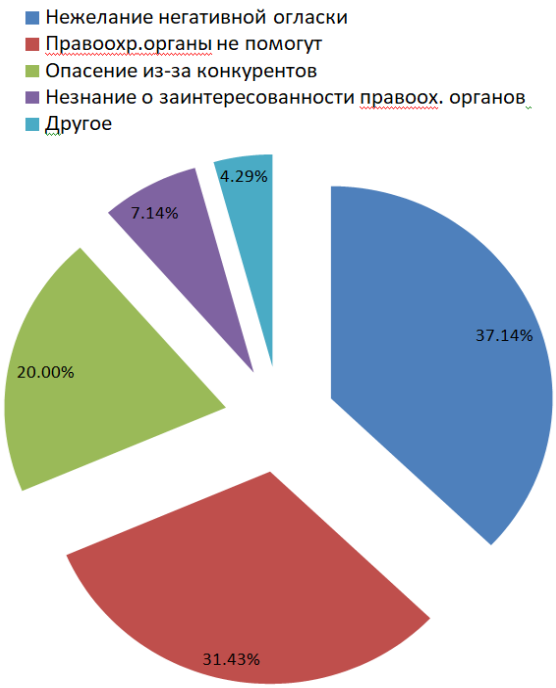

Рис. 1. Причины несообщения организациями о кибератаках

Проанализировав крупнейшие кибератаки в Российской Федерации, можно выделить следующие приемы кибератак [4]:

• получение несанкционированного доступа к личной, коммерческой, банковской информации, составляющей государственную и военную тайну;

• повреждение физических элементов информации, пространства (например, глушение, нарушение сетей питания, использование специальных программ, разрушающих оборудование);

• уничтожение информации, программного обеспечения, технических ресурсов за счет внедрения вирусов, программных ошибок, преодоления систем защиты;

• техническая реализация в телеканалах вещания информации с целью распространения слухов, дезинформации, объявления требований террористической организации;

• разрушение или подавление линий связи, перегрузка узлов связи, меняющих адресацию запросов в Интернете;

• проведение информационно-психологических операций, влияющих на сознание населения и др.

Эти техники постоянно совершенствуются в зависимости от средства защиты, используемые разработчиками компьютерных сетей. Таким образом, киберпреступники могут использовать различные типы атак в сетях, которые позволяют им получить доступ к корпоративной сети, перехватить контроль над ней или заблокировать обмен информацией в сетях.

К средствам проведения таких атак относятся компьютерные вирусы:

• сетевые черви, изменяющие и уничтожающие секретную информацию или блокирующие работу вычислительных систем;

• логические бомбы, срабатывающие при определенных условиях, запланированных преступниками;

• «Троянские кони», которые отправляют своему «владельцу» через сеть «Интернет» различную информация с зараженного компьютера.Далее приведём популярность средств осуществления кибертеррористической угрозы, от общего числа инцидиентов (рис.2.)

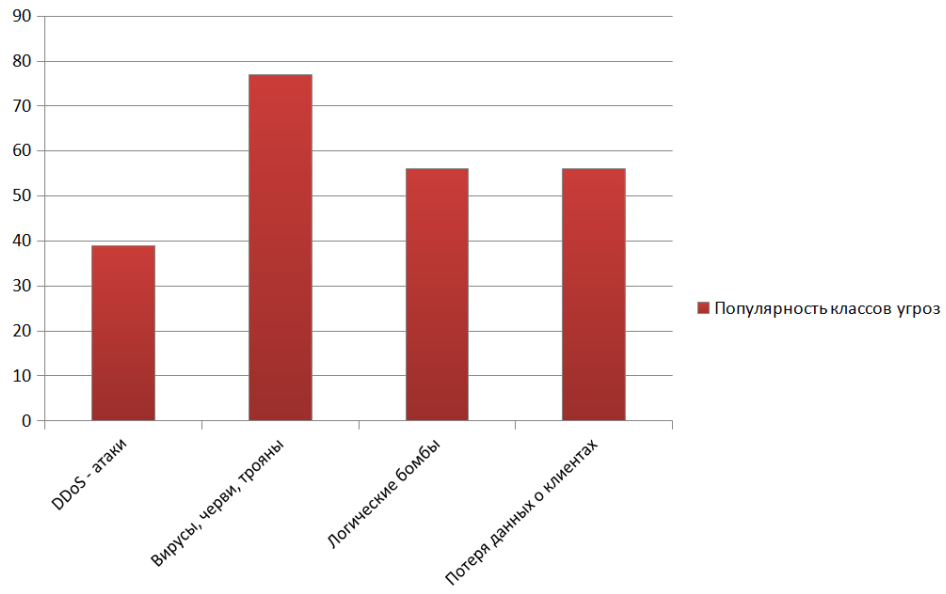

Рис. 2. Популярность классов кибертеррористических угроз, % от общего числа инцидентов, за период с 2013-2016 гг.

Анализ нормативных правовых актов позволяет выделить следующие причины возникновения кибертерроризма - политические, социальные и экономические [5].

Политические причины делятся на внешние и внутренние. К внешним причинам относятся глобализация, углубление разрыва между уровнями благосостояния разных стран, военная агрессия против другого государства и его оккупация, усиление глобального цифрового противостояния и разрыв в уровне информационного развития стран, столкновение политические интересы разных государств. Внутренние причины - политическая нестабильность и обострение политических конфликтов внутри государства, отсутствие механизмов взаимодействия государственной власти и гражданского общества, навязывание правящей элитой социально-политических реформ и иных нововведений, не характерных для данного общества, недовольство граждан страны деятельностью иностранных

правительств; пропаганда кибертерроризма со стороны руководства страны, общественных организаций и СМИ.

Среди социальных причин возникновения кибертерроризма можно выделить усиление социальной дифференциации общества, его разделение на группы с разным экономическим статусом, заметное снижение качества жизни людей и слишком медленный процесс формирования среднего слоя общества.

К экономическим причинам кибертерроризма относятся продолжающийся экономический и энергетический кризис, рост цен, инфляция и безработица.

Правоохранительные органы стремятся повысить безопасность информационного пространства за счет минимизации воздействия кибертеррористов на информационные системы. Однако в настоящее время эта проблема уже вышла из-под контроля правоохранительных органов и переросла в серьезную государственную и международную проблему.

Список литературы:

1. Федеральный закон Российской Федерации от 6 марта 2006 г. N 35-ФЗ «О противодействии терроризму».

2. Генеральная прокуратура Российской Федерации. [Электронный ресурс]. URL: http://www.genproc.gov.ru/. (дата обращения: 19.11.2020).

3. Нормативно-правовое регулирование молодежной политики : учебное пособие / Р.И. Зинурова, Э.Б. Гаязова, А.Р. Тузиков; М-во образ. и науки России, Казан.нац.исслед.технол.ун-т. – Казань : Изд-во КНИТУ, 2013.

4. Мамедов В. А., Деккерт Д.В., Роль органов местного самоуправления в предупреждении экстремизма в контексте охраны общественного порядка и обеспечения общественной безопасности. - [Электронный ресурс] URL: http://www.lib.csu.ru/vch/169/vcsu09_31.pdf.

5. Экстремизм и его причины / под ред. Ю.М. Антоняна. М., 2010. 288 с.

Щедрина Мария Евгеньевна
Колледж АлтГУ, г. Барнаул
Научный руководитель: Мария Александровна Стародубцева,
ассистент кафедры уголовного права и криминологии
юридического института АлтГУ

Щедрина М.Е. ПРЕСТУПЛЕНИЯ ЭКСТРЕМИСТСКОЙ НАПРАВЛЕННОСТИ – 2020: СОСТОЯНИЕ, СТРУКТУРА, ДИНАМИКА

В 2020 году тема экстремизма снова становится более чем актуальной. Локдаун, объявленный в марте 2020 г. фактически вырвал сотни тысяч людей из налаженной системы социальных связей и взаимоотношений [11]. Множество людей потеряли работу либо вынуждены были перейти на так называемую «удаленку». Резко возрос упровень фрустрированности общества, постоянное нагнетаемое СМИ социальное напряжение перешло на новый уровень в связи со вспышкой коронавирусной инфекции. Безработица повлекла фактическую остановку экономики, падение уровня жизни населения, снижение уровня заработной платы и рост цен на продукты первой необходимости.

Не обошел стороной локдаун и систему образования: практически все образовательные учреждения перешли на дистанционный режим работы, что повлекло, в свою очередь, очевидное падение качества получаемых знаний. Молодежь оказалась вырвана из жизни, основным средством общения и взаимодействия стала сеть «Интернет». Ответом на кризис в экономике и социальной сфере стал резкий всплеск экстремистских настроений в обществе, прежде всего, среди молодежи. Только за первый квартал 2020 г. уровень зарегистрированных преступлений экстремистской направленности вырос, по сравнению с 2019 г. на 40,9%. К концу года очевиден еще больший рост. СМИ и сеть «Интернет» пестрят сообщениями и лозунгами о том, что преступность в России перешла в онлайн-формат, и лидируют преступления именно экстремистской и частично террористической направленности [1].

В октябре 2020 года на сайте Судебного департамента Верховного Суда Российской Федерации были опубликованы статистические данные о деятельности российских судов за первое полугодие 2020 г [2].

По данным ведомства, за первые шесть месяцев 2020 года по так называемым «экстремистским составам» осуждено 210 человек против 432 осужденных за весь 2019 год.

Можно сказать, что по статистике приговоров всплеск экстремистских преступлений пока не ощущается, но при анализе статистики мы не берем в

расчет дела, находящиеся в производстве, коих большинство на сегодняшний день. Прежде всего, речь идет о массовых случаях провокаций при проведении онлайн-акции «Бессмертный полк», связанных с размещением на сайте акции фотографий нацистских преступников. Еще не завершено расследование относительно самоубийства в СИЗО одного из ярких деятелей ультраправой оппозиции М. Марцинкевича, известного как «Тесак», и выявление участников протестных акций импровизированного «прощания» с ним, прокатившихся по ряду российских городов. В частности, 28.09.2020 г. такая акция прошла и в Барнауле. 04.11.2020 г. в Барнауле прошла так же акция ультраправой оппозиции «Русский марш», объединившая под своими знаменами 50 человек. Все эти эпизоды мы, повторяем, не берем во внимание при анализе статистики приговоров за первое полугодие 2020 г.

Из осужденных в первой половине 2020 года 132 человека (в 2019 году - 244) были осуждены по статьям о наказании за публичные высказывания разного рода (статьи 282, 280, 280.1, 205.2, 354.1, части 1 и 2 ст. 148 УК РФ), а 78 (на 2019 год - 188) - за создание экстремистских или террористических сообществ и продолжение деятельности организаций, запрещенных как экстремистские или террористические (статьи282.1, 282.2, 205.4, 205.5) [3].

Если в 2019 году по сравнению с 2018 годом увеличилась доля преследований за причастность к запрещенным организациям, а доля преследований за высказывание снизилась в результате частичной декриминализации ст. 282 УК РФ, то в первом полугодии 2020 года по сравнению с 2019 годом доля преследований за причастность к запрещенным организациям несколько снизилась, а доля преследований за высказывание, наоборот, немного увеличилась.

Наибольшее количество уголовных приговоров за пропаганду в первой половине 2020 года было вынесено по ст. 280 УК РФ) и количество приговоров по этой статье продолжает расти: за первые шесть месяцев 2020 года осуждено 80 человек, а за весь 2019 год - 145. Оправдан один человек, против 12 дела были прекращены. Уже сейчас можно сказать, что прогноз, высказанный нами в 2018 г., о том, что после частичной декриминализации ст. 282 УК РФ, ст. 280 станет ее полноценной заменой, вполне оправдывается.

Далее следует ст. 205.2 УК РФ за пропаганду терроризма - 73 осужденных за первое полугодие 2020 года против 126 человек за весь 2019 год, то есть цифры и здесь растут.

Число осужденных по другим агитационным статьям намного меньше: по ст. 280.1 - по призывам к сепаратизму в первой половине 2020 года вынесен один приговор (четыре за весь 2019 год); единственный осужденный по этой статье, как по основному составу, был приговорен к обязательным работам с запретом занимать определенные должности или заниматься какой-либо деятельностью. Три человека были осуждены по ст. 354.1 о реабилитации нацизма (двое осужденных по этой статье в качестве основного оштрафованы), еще двое освобождены от уголовной ответственности; в 2019 году по ст. 354.1 двое были осуждены. Только один человек был осужден по ч. 1 ст. 148 УК РФ

об оскорблении чувств верующих; двое человек освобождены от уголовной ответственности. Практики по ч. 2 ст. 148 УК РФ в 2020 г. мы не обнаружили [4].

Согласно ст. 282 УК РФ: осуждено всего три человека, двое из них - по декриминализованной части первой, то есть повторному эпизоду в течение года, и только один - по более серьезной второй части. Интересно сравнить эти цифры с данными за 2018 год (518 человек) и 2019 год (36 человек): мы видим, что после декриминализации статьи количество осужденных по ней уменьшилось с сотен до единиц.

29 мая 2020 года Президент России Владимир Путин утвердил новую редакцию Стратегии противодействия экстремизму до 2025 года. О ее подготовке стало известно в марте 2020 года, когда МВД вынесло проект поправок на общественное обсуждение (утвержденный текст, однако, несколько отличается от этого проекта) [5].

В предыдущей редакции Стратегии, утвержденной в 2014 году, были определены понятия «идеология экстремизма», «проявления экстремизма», «субъекты противодействия экстремизму», «противодействие экстремизму» и «радикализм». В новой версии эти определения несколько изменены, кроме того, в Стратегию введено понятие «идеология насилия». Оно определяется как совокупность взглядов и идей, которые оправдывают использование насилия для достижения политических, идеологических, религиозных и других целей [6].

Если в старой версии Стратегии понятие «радикализм» определялось как «глубокая приверженность идеологии экстремизма, способствующая совершению действий, направленных на насильственное изменение основ конституционного строя и нарушение целостности государства». Российская Федерация », то в новой редакции дается следующее определение: «бескомпромиссная приверженность идеологии насилия, характеризующаяся стремлением к решительному и радикальному изменению основ конституционного строя, нарушением единства и территориальной целостности. Российской Федерации».

Кроме того, определение понятия «проявление экстремизма», которое относится только к действиям, совершаемым из ненависти и вражды или способствующим обострению межэтнических, межконфессиональных и региональных конфликтов, теперь распространяется на действия, угрожающие конституционному порядку и нарушение территориальной целостности России. В новую редакцию включены мероприятия, направленные на минимизацию и устранение последствий экстремизма как «противодействие экстремизму» [7].

В новой версии Стратегии дано новое описание внешних и внутренних экстремистских угроз. Под внешними угрозами теперь понимается «поддержка и стимулирование рядом государств деструктивной деятельности иностранных или международных неправительственных организаций, направленной на дестабилизацию общественно-политической и социально-экономической ситуации в Российской Федерации, нарушающую единство и территориальная

целостность Российской Федерации, включая разжигание «цветных революций», разрушение традиционных российских духовно-нравственных ценностей, а также содействие деятельности международных экстремистских и террористических организаций, в частности распространению экстремистской идеологии и радикализма вобществе» [8].

Конкретизируется определение внутренних угроз в новой Стратегии. К таким угрозам относятся попытки осуществления экстремистской деятельности со стороны националистических, радикальных общественных, религиозных, этнических и иных организаций и лиц, распространение идеологии насилия, убеждения, вербовки или иного вовлечения граждан России и иностранцев на территории страны в деятельность экстремистских сообществ и другая незаконная деятельность, а также формирование закрытых этнических и религиозных анклавов.

В отдельном абзаце указано, что к внутренним угрозам также относятся угрозы, обусловленные историческими и социально-экономическими особенностями и ведущие к сепаратистским проявлениям межнациональных и территориальных противоречий и конфликтов в отдельных субъектах Российской Федерации [9].

Термины «националистический, религиозный и политический» исключены из списка наиболее опасных видов экстремизма (очевидно, потому что они не определены).

Проведение несогласованных публичных мероприятий, в том числе протестов (в предыдущей редакции использовался менее точный термин «несогласованные действия»), квалифицируется как экстремизм в нескольких пунктах Стратегии [10].

Таким образом, мы можем увидеть достаточно четко обрисованную картину динамики экстремистских преступлений в период 2020 г. и ответ законодателя на определенный рост экстремистских проявлений.

Список литературы:

1. «Конституция Российской Федерации» (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) // Сайт «Консультант Плюс» [Электронный ресурс]

2. «Конвенция о защите прав человека и основных свобод» (Заключена в г. Риме 04.11.1950) (с изм. от 13.05.2004) (вместе с «Протоколом [N 1]» (Подписан в г. Париже 20.03.1952), «Протоколом N 4 об обеспечении некоторых прав и свобод помимо тех, которые уже включены в Конвенцию и первый Протокол к ней» (Подписан в г. Страсбурге 16.09.1963), «Протоколом N 7» (Подписан в г. Страсбурге22.11.1984)) // Сайт «Консультант Плюс» [Электронный ресурс]

3. Декларация о свободе политической дискуссии в средствах массовой информации (принята Комитетом Министров Совета Европы 12 февраля 2004

г. на 872-м заседании Комитета Министров на уровне постоянных представителей) // Сайт «Консультант Плюс» [Электронный ресурс]

4. Федеральный закон от 25.07.2002 N 114-ФЗ (ред. от 31.07.2020) «О противодействии экстремистской деятельности» // Сайт «Консультант Плюс» [Электронный ресурс]

5. Указ Президента РФ от 29.05.2020 N 344 «Об утверждении Стратегии противодействия экстремизму в Российской Федерации до 2025 года» // Сайт «Консультант Плюс» [Электронный ресурс]

6. Постановление Пленума Верховного Суда РФ от 28.06.2011 N 11 (ред. от 20.09.2018) «О судебной практике по уголовным делам о преступлениях экстремистской направленности» // Сайт «Консультант Плюс» [Электронный ресурс]

7. Галяшина Е.И. «Лингвистика vs экстремизма: В помощь судьям, следователям, экспертам» / под ред. проф. М.В. Горбаневского. М.: Юридический мир, 2006. Стр.9-10

8. Галяшина Е.И. «Экспертиза экстремистских материалов: проблемы методического и информационного обеспечения» // Журнал «Вестник университета имени О.Е. Кутафина (МГЮА)» 07.2018. Стр.26-41.

9. Сергеев С. А. Исследования экстремизма и радикализма в зарубежных и отечественных социальных науках [Электронный ресурс], URL:http://kpfu.ru/docs/F110664239/Statya.Ekstremizm.radikalizm.sokr.bibliograf.pdf.

10. Чудинов С.И. «Экстремизм и научный образ экстремизма: столкновение мировоззренческих парадигм»// Журнал «Теория и практика общественного развития» 2014 г., №18, стр.159-161

11. Backes U. Meaning and Forms of Political Extremism in Past and Present // Central European Political Studies Review. 2007. Autumn. Vol. IX. Part 4.P. 242–262

ПечинкинаАлёнаСергеевна
АбасовРзаИнтигамоглы
КолледжАлтГУ, г. Барнаул
Научный руководитель: Мария Александровна Стародубцева,
ассистент кафедры уголовного права и криминологии
юридического института АлтГУ

Печинкина А.С., Абасов Р. БОРЬБА С ТЕРРОРИСТИЧЕСКИМИ АКТАМИ В КИБЕРПРОСТРАНСТВЕ

Мы хотим представить несколько организаций и террористических актов в киберпространстве:

Синий кит.

Игра, ставшая популярной в социальной сети Вконтакте. Это одна из многочисленных групп, публикующих депрессивные и шокирующие материалы: фотографии, видеозаписи, аудио и короткие демотивирующие тексты. Название напрямую связано с печальным природным явлением — массовой гибелью китов, которые самостоятельно выбрасываются на берег.Создатели сообщества проводили связь между этим актом, объяснить который современные ученые не могут, и суицидом подростков. Призыв закончить собственную жизнь звучит в разных формулировках и подается в игровой форме.

Постоянные хештеги в виде "Разбуди меня в 4.20" ," Ня.Пока.","Я в Игре".

Благодаря этим хештегам так называемые кураторы находили своих жертв. Синий кит-якобы помогал людям, которые устали жить, он помогал им скорее умереть.

Сейчас, в настоящий момент данное сообщество заблокировано и администрация ВК очень чётко следит за такими группами!

На рис. 1 мы хотим представить переписки настоящих людей, которые участвовали в данной «игре» и их эмоции

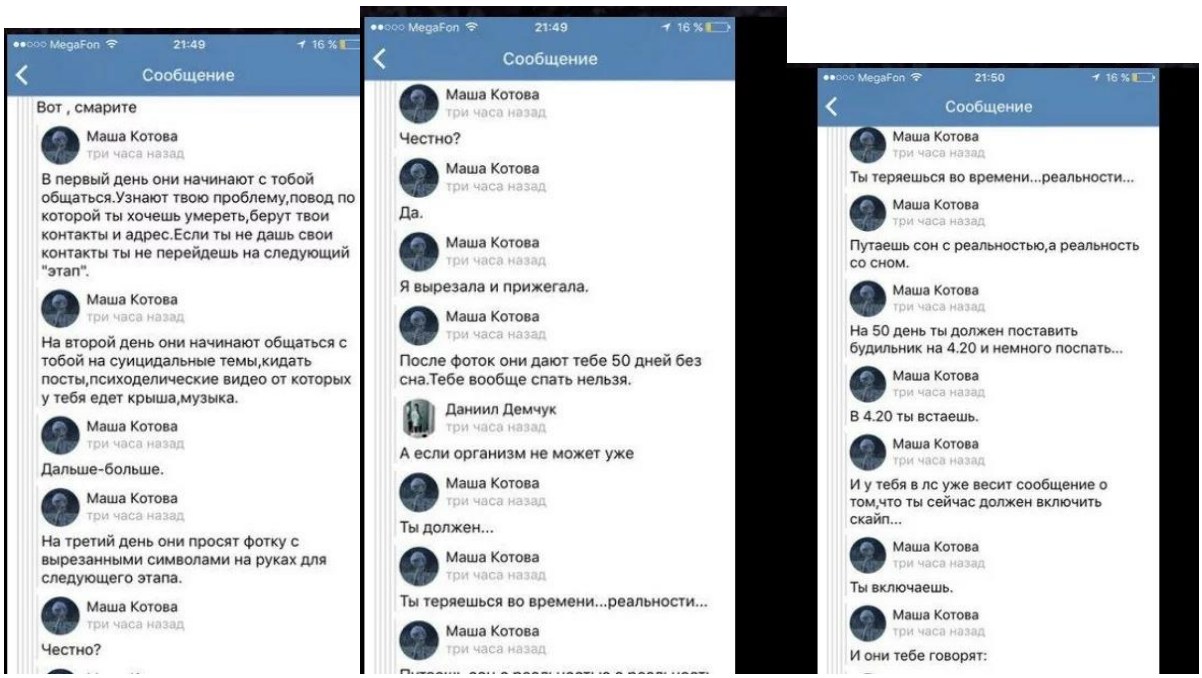

Рис. 1. Скриншоты переписок людей, участвовавших в игре «СИНИЙ КИТ» (материалы сети «Интернет»)

Игра Говорящая Анджела!

В конце января 2014 года по слухам произошел взлом мобильной игры "Talking Angela". Эта игра была выпущена компанией Outfit7 в рамках серии "MyTalkingFriends", и представляет из себя симулятор общения, одновременно с симулятором питомца. Игра была рассчитана на детей до 14 лет, однако даже в оригинальной версии присутствуют странности. Кошечка может задавать вопросы личного характера, по типу: "Как тебя зовут?", "Сколько тебе лет?", "Скажи свой адрес", "А у тебя когда из дома уедут родители?", "У вас есть дома большая и злая собака?" и так далее.

Отличия оригинала от взлома видны сразу - человека в отражении видно лучше, вопросы Анджелы стали откровеннее. Общение при этом становится более осмысленным. При дальнейшем общении кошечка начинает указывать собеседнику, что ему следует делать, угрожая опасностью. Следование инструкциям приводит к летальному исходу.
На начало марта 2014 насчитывается 27 подтвержденных жертв взлома. Все пострадавшие являются детьми школьного возраста, все они выполняли рекомендации Анджелы. Об этом свидетельствуют сохранившееся логи, переписки с кошечкой, где та велела им отправиться в безлюдное место, по типу заброшенного дома, лесополосы и т. д., где тела вскоре были найдены в изуродованном состоянии. В основном случаи происходили в странах Восточной Европы, но наблюдались и в России, США, Аргентине и т. д**.**

Расследование:

Известно, что взломанная версия не только была размещена на нескольких пиратских сайтах игр для Android, но и на AppStore, и даже на несколько

Google PlayMarket`ов. Были обнаружены IP адреса и сим-карты, но те либо вели на уничтоженные компьютеры и модемы, либо были взяты по поддельным документам.

В оригинале картинка в зрачках Анджелы представляет собой изображение парижской улицы, шутки ради добавленное в игру разработчиками. Удалось установить личность человека, лицо которого видно во взломанной версии. На фото Мариуш Трынкевич, гражданин Польши, ранее не раз судимый за преступления сексуального характера.

Фотография, также сделана в Париже, судя по обстановке. Самые странности начинаются тут. Все убийства, связанные с игрой, датируются февралём 2014 года. Трынкевич же в это время отбывал очередной тюремный срок и был выпущен на свободу только в начале марта.

Далее все еще сложнее. Убийца не пытался заметать следы, в изобилии оставляя отпечатки пальцев рядом с телами жертв. Все отпечатки пальцев принадлежат одному и тому же человеку, но ни в одной базе данных не удалось обнаружить соответствия. Одинаковые отпечатки пальцев присутствуют даже на местах преступления, совершённых в различных точках земного шара приблизительно в одно и то же время! Рационального объяснения данному факту до сих пор не предвидится.

Хотим вам привести пример открытой мотивации для кибертеррористов :

Сайт для продажи убийств (любого вида)и детского порно:

Название сайта Forogore.

Обычные поисковые системы не индексируют страницы из «тёмной» части сети, поэтому заказчики обычно пользуются одним из «даркнетовских» поисковиков или же ищут нужные сайты на специальных страницах, где собрано большое количество актуальных ссылок. Кстати, найти адреса площадок из даркнета можно и в обычном интернете, но для того, чтобы открыть ссылки с доменом нужен будет специальное приложение. Найдя необходимый сайт(название сайта мы указали выше), нужно или связаться с администратором, или заполнить специальную форму. И для того и для другого понадобится электронная почта, но использование gmail чревато деанонимизацией, поэтому в ход идут множество анонимных почтовых сервисов.

Прайс-лист чаще всего находится в специальном разделе :если коротко, то разброс цен за убийство от $1500 до 200 000$.

Зависит от того ,чем будет сделано убийство или как будет сделано самоубийство. На данном сайте очень много убийств, самоубийств, порнографии детской и зоофилии.
Он находится в свободном доступе и там, действительно, можно продавать убийства!

Так же, что бы передавать сайту видео нужна специальная площадка Даркнет.

Это скрытая сеть, соединения которой устанавливаются только между доверенными пирами, иногда именующимися как «друзья», с использованием

нестандартных протоколов и портов. Анонимная сеть представляет собой систему не связанных между собой виртуальных туннелей, предоставляющая передачу данных в зашифрованном виде.

Даркнет отличается от других распределённых одноранговых сетей, так как файлообмен происходит анонимно (поскольку IP-адреса недоступны публично), и, следовательно, пользователи могут общаться без особых опасений и государственного вмешательства.

Именно поэтому даркнет часто воспринимается как инструмент для осуществления коммуникации вразличного рода подпольях и незаконной деятельности, в том числе кибертерроризм. В более общем смысле термин «даркнет» может быть использован для описания некоммерческих «узлов» интернета или относиться ко всем «подпольным» интернет-коммуникациям и технологиям, которые в большинстве своём связаны с незаконной деятельностью или инакомыслием

С помощью данной сети группы-смерти продают видео самоубийств,а так же детское порно,избиение.

Данную сеть в открытом доступе можно скачать в России!И данному факту никто не противодействует!

Вашему вниманию мы хотим представить нашу общественную организацию **АКТО** (АнтиКиберТеррористическая организация).

Мы, Абасов Рза и Печинкина Алёна, совместными усилиями создали общественную организацию под названием АКТО.

Организация создавалась для помощи людям, а особенно подросткам, подвергшимся кибертерроризму в г. Барнауле, но уже наша организация известна не только в городе, а и в ближайших районах. Данная организация будет продолжать своё деятельность и дальше развиваться. В ближайшее время будет установлена связь с Краевым домом молодёжи (КДМ) в г. Барнаул. Так же будут проходить митинги против Кибертерроризма, с мотивирующими лозунгами. Совместными усилиями будут блокироваться группы-смерти в социальных сетях.

Наша организация представляет собой защиту людей, а особенно подростков, обратившихся в АКТО. Установлена связь с Психологами, на тот случай, если вдруг понадобиться помощь Психолога. Наша организация в любой момент готова вызвать службу спасения на место преступления, либо передать данные в полицию. Так же в социальной сети ВК каждый день выходят статьи на тему Кибертерроризма, для осведомления подписчиков группы о возможных уровнях опасности. Мы работаем круглосуточно и готовы ответить в любой момент.

Наша организацию установила связь с волонтерским отрядом «Доброзожики Алтая» и это даёт нам возможность в любой момент выйти на помощь при просьбе.

Мы уже сейчас устанавливаем связь с другими учебными заведения. В каждой организации будет человек, который будет следить за возможными причинами мотивации кибертерроризма и терроризма в заведении. И так же это

даёт нам возможность оперативно отвечать и помогать людям, обратившимся за помощью.

Для того, чтобы обеспечить безопасность от кибертерроризма и эффективную систему борьбы с ним, необходимо:

1. Закрепить в законодательстве понятие «кибертерроризм» и выделить какие конкретно преступления к нему относится;
2. Организовать единый международный механизм по борьбе с киберпреступностью, чтобы избежать противоречий в законодательстве других стран;
3. Закрепить статус киберпространства как еще одной среды, которая требует внимания всего мирового сообщества;
4. Разработать единый механизм идентификации пользователей сети для создания системы уголовной ответственности за деятельность в виртуальной среде;
5. Расширить функции правоохранительных органов и служб, осуществляющих антитеррористическую деятельность.

Список литературы:

1. О противодействии терроризму: федер. закон: [принят Гос. Думой 26 февраля 2006 г.:одобрен Советом Федерации 1 марта 2006 года] / Российская Федерация. - «Собрание законодательства РФ». - N 35-ФЗ.
2. Об информации, информационных технологиях и о защите информации: федер. закон: [принят Гос. Думой 27 сентября 2006 г.:одобрен Советом Федерации 27 ноября 2006 года] / Российская Федерация. – «Собрание законодательства РФ». – 01.01.2018. – Ст.15.1.

Ельникова Софья Михайловна
Колледж АлтГУ, г. Барнаул
Научный руководитель: Мария Александровна Стародубцева,
ассистент кафедры уголовного права и криминологии
юридического института АлтГУ

Ельникова С.М. РАСПРОСТРАНЕНИЕ ПОЛИТИЧЕСКОГО ЭКСТРЕМИЗМА СРЕДИ МОЛОДЕЖИ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ «ИНТЕРНЕТ»

Понятие преступлений экстремистской направленности содержится в различных нормативно-правовых актах, к числу которых относится Уголовный кодекс Российской Федерации, Федеральный закон от 25.07.2002 г. «О противодействии экстремистской деятельности» [1] и Постановление Пленума Верховного Суда Российской Федерации от 20.09.2018 г [2].

Понятие преступлений экстремистской направленности раскрывается в примечании 2 к статье 282.1 Уголовного кодекса Российской Федерации, согласно которому таковыми признаются преступления, совершенные по мотивам политической, идеологической, расовой, национальной или религиозной ненависти или вражды либо по мотивам ненависти или вражды в отношении какой-либо социальной группы, предусмотренные соответствующими статьями Особенной части УК РФ и п. «е» ч. 1 ст. 63 УК РФ[3].

В рамках данной исследовательской работы мы будем говорить только о политическом экстремизме, который выражается в стремлении граждан воплотить в жизнь свои политические взгляды и цели любыми доступными средствами,включаянасильственныеформывоздействиянагосударственные институты, общественных и политических деятелей и отдельных индивидов. Политический экстремизм связан с противоположностью интересов не отдельных индивидов, а различных общественных объединений.

Исследую нормативно-правовую базу, можно заметить, что на законодательном уровне молодежный экстремизм как самостоятельное явление не закреплен. Тем не менее отсутствие такого понятия в нормативно- правовых актах не преуменьшает степень и характер его общественной опасности, подрывающего нормальное социальное, культурное и правовое развитие молодого поколения.

Как известно, одним из качественных признаков экстремизма является то, что он способен «впитывать» специфику социального контекста своего бытования, адаптироваться к нему. В этой связи исследователи справедливо

обращают внимание на то, что «явление экстремизма весьма динамично и с каждым днём приобретает всё новые черты и характеристики. В современном информационном обществе экстремистские организации всё активнее используют достижения коммуникационных технологий, внедряя в свою деятельность, прежде всего, те из них, которые достаточно эффективно воздействуют на массовое общественное сознание» [4].

Многие исследователи помимо существующих форм экстремизма выделяют информационный, который определяется ими «как деятельность, связанную с созданием, хранением и (или) распространением информации, обрабатываемой компьютером, содержащей предусмотренные законом признаки экстремистской деятельности, использованием этой информации для деструктивного воздействия на психику людей, не осознаваемыми ими» [5]. Его характеризует развитие тенденции перехода экстремизма в пространство информационно-коммуникационных технологий. Информационный экстремизм не только начинает свое обозначение и проявление, но и превращается в проблему современного информационного общества[6].

Появление информационно-телекоммуникационной сети Интернет привело к распространению преступлений экстремистской направленности. Многими исследователями отмечается, что система объединенных компьютерных сетей стала удобным средством распространения экстремисткой идеологии, направленную на разрушение сложившихся политических институтов, норм морали и человеческих ценностей.

Последствия преступлений экстремистской направленности, совершаемых с использованием информационно-телекоммуникационной сети, оказывают влияние на политическую, экономическую, духовную и социальную сферы общественной жизни.

Интернет-ресурсы используются в целях вовлечения пользователей в деятельность экстремистских организаций. Проблема распространения экстремизмавсетиИнтернетсвязанастем,чтожертвамипреступленийчасто оказываютсянесовершеннолетние.Многиеизнихвовлекаютсявдеятельность организаций экстремистской направленности. Происходит это потому, что в сознании молодых людей преобладают негативные оценки в отношении государства и его институтов.

Несовершеннолетние не могут участвовать в голосовании по вопросам государственного,регионального илиместногозначения,всвязисчеммногие из них становятся последователями экстремизма, в котором они видят способ изменения существующего политического строя. Несовершеннолетние являются самой незащищенной в культурном отношении категорией населения,котораяпереживаеткризиссоциальнойинационально-культурной идентичности. Противоправные действия представителей государственной власти приводят к тому, что некоторые граждане начинают выражать свое несогласие с существующим политическим строем посредством осуществления экстремистских действий. Таким образом, неучастие молодых людей в

политике является одной из причин их вовлечения в деятельность экстремистского характера.

Необходимо заметить, что в последние годы рассматривается вопрос о повышении возраста активного избирательного права, что в случае осуществления приведет к еще большему недовольству среди молодежи и как следствие к увеличению количества экстремистских преступлений в молодежной среде.

Иными причинами распространения политического экстремизма среди молодых людей являются наступление профессиональных кризисов, с которыми связана неудовлетворенность молодых людей своим социальным и профессионально-образовательным статусом.

Преступления экстремистской направленности в информационно-телекоммуникационной сети Интернет имеют некоторые особенности, которые отличают их от преступлений, совершенных без ее использования. К ним относится анонимное размещение информации, что создает проблему проведения расследований и требует применения новых криминалистических технологий поиска и исследования цифровых следов преступления. Особенностями сети Интернет как инструмента экстремистской деятельности являются также возможность широкого обхвата аудитории, высокая скорость распространения экстремистских материалов и возможность создавать собственные пропагандирующие интернет-ресурсы без финансовых затрат.

В 2019 г.по результатам проведения расследования было заблокировано свыше 81 тыс. интернет-ресурсов с информацией, содержащей террористические и экстремистские угрозы, включая призывы к массовым беспорядкам и насилию.

Нами было проведено исследование, направленное на выявление причин распространения экстремизма в сети Интернет среди молодых людей. Респондентами выступили студенты, получающие среднее профессиональное образование и студенты, обучающиеся в Алтайском государственном университете. Студентам предлагалось ответить на несколькововопросов.

На вопрос «Какие причины экстремистской деятельности среди молодежи Вы можете назвать?» большая часть ответила, что причинами распространения преступлений экстремистской направленности являются отсутствие очевидных перспектив для развития и, что самое главное – их реализации, недоступность информирования о социальных лифтах, отсутствие кандидатов, которые были бы способны удовлетворить интересы молодежи. Некоторые респонденты при прохождении опроса назвали другую причину распространения экстремизма среди молодых людей, а именно несовершеннолетних. В ответе на вопрос респонденты указали, что несовершеннолетние, не имея возможности повлиять на политическую обстановку в стране из-за отсутствия права участвовать в выборах и референдумах стремятся изменить ее другим способом, т. е. посредством участия в экстремистской деятельности.

По мнению респондентов целью экстремистской деятельности является привлечение внимания со стороны государства и его органов к проблемам молодых людей, которые остаются незамеченными в обычной жизни.

На вопрос «Согласны ли Вы с тем, что молодежь является группой населения, наиболее подверженной вступлению в организации, осуществляющие экстремистскую деятельность?» 100% принявших участие в опросе выбрало вариант«да».

Респондентам также был задан вопрос: «Согласны ли Вы с тем, что экстремизм в интернет-пространстве является наиболее опасной формой совершения преступлений экстремистской направленности?». Многие считают, что за счёт массового и почти неконтролируемого быстрого распространения информации, экстремистская деятельность является наиболее опасной формой. Мы согласимся с ними, поскольку интернет- пространство является самой удобной платформой для распространения экстремистских действий и при этом менее уязвимой для внешнего обнаружения.

Наиболее важной составляющей антиэкстремистской деятельности является и устранение причин и условий, порождающих экстремизм.

Предлагаем рассмотреть следующие пути разрешений проблемы распространения преступлений экстремистской направленности в интернет-пространстве.

Выше мы написали о том, что молодые люди в возрасте от 16 до 18 летещенеобладаютизбирательнымправом,нотакже,какисовершеннолетние, ожидают от государства политики, которая бы создавала возможность для их самовыражения и самореализации. Мнение этой категории граждан тоже должно быть услышано.

Интернет представляет собой неконтролируемое информационное пространство, поэтому меры по ограничению в сети будут способствовать лишь нарастанию недовольства от несвободы у молодых людей. Мы предлагаем решать проблему распространения преступлений экстремистской направленности в интернет-пространстве путем информирования и развития сетевой грамотности у молодых людей, но не путем ограничения использования информационно-телекоммуникационной сети Интернет.

Практически безграничные возможности сети Интернет в области передачи обработки информации, обеспечивающие коммуникацию в разных формах, приводят к возникновению такого негативного социального явления, как интернет-преступность. Распространение политического экстремизма в интернет-пространстве среди молодежи создает проблему проведения расследований и требует применения новых криминалистических технологий поиска и исследования цифровых следов преступления. Можно сделать вывод о том, что основным элементом следовой картины интернет-преступлений будут являться информационные следы. Среди таких следов для всех рассмотренных преступных деяний могут быть характерны чаты, блоги, переписка, фотографии и аккаунты пользователей, содержащие экстремистские материалы. Проблема проведения расследований экстремистский преступлений в интернет-

пространстве может быть решена с помощью применения новых криминалистических технологий поиска и исследования цифровых следов преступления.

Список литературы

1. Федеральный закон от 25 июля 2002 г. N 114-ФЗ "О противодействии экстремистской деятельности" (с изменениями и дополнениями) // Собрание законодательства РФ.

2. Постановление Пленума Верховного Суда РФ от 20 сентября 2018 г. № 32 “О внесении изменений в постановление Пленума Верховного Суда Российской Федерации от 28 июня 2011 года N 11 "О судебной практике по уголовным делам о преступлениях экстремистской направленности" // Бюллетень Верховного Суда РФ 2001.

3.Уголовный кодекс РФ от 13 июня 1996 г. № 63-ФЗ // Собрание законодательства Российской Федерации - 17 июня 1996 г. - № 25

4. Мозговой, В.Э. Информационный экстремизм как инновационная девиация социума начала XXI века. [Текст] / В.Э. Мозговой // Гуманитарные, социально-экономические и общественные науки – 2020. - №3 – С. 61-65

5. Алексеева, Д.И., Багаева, А.А. Экстремизм как угроза национальной безопасности россии: основные направления противодействия. [Текст] / Д.И. Алексеева, А.А. Багаева // Юридические науки – 2018. С. 261-263

6. Кудрин, В.С. Экстремистская деятельность молодёжи: классификация, формы и виды. [Текст] / В.С. Кудрин // Мир науки, культуры, образования. – 2015. - №6 – С. 79-83

Мазурова Ангелина Олеговна
Колледж АлтГУ, г. Барнаул
Научный руководитель: Мария Александровна Стародубцева,
ассистент кафедры уголовного права и криминологии
юридического института АлтГУ

Мазурова АО. РАЗВИТИЕ ПСЕВДОИСЛАМСКИХ ТЕЧЕНИЙ ПРАВОГО ТОЛКА И ИХ РАСПРОСТРАНЕНИЕ В СЕТИ «ИНТЕРНЕТ»

На сегодняшний день одной из главных мировых проблем и угроз мировой безопасности признана широкая экспансия ИГИЛ, за 2 года захватившего значительную территорию Ирака, Сирии и Афганистана. По сведениям командующего Генштаба вооруженных сил России данная группировка насчитывает 80 тысяч боевиков, провозгласила на захваченных территориях псевдохалифат, стремится и далее расширять свои приобретения (по разным оценкам контролируемая ИГИЛ территория достигает около 90 тыс. квадратных километров, 8 миллионов человек проживают в районах, захваченных игиловцами в Сирии и Ираке).

Только в октябре и ноябре прошлого года мир потрясли действия боевиков ИГИЛ, взявших на себя ответственность за теракты на борту российского авиалайнера А-321 на Синайском полуострове и в Париже.

В ходе своего выступления 28.09.2015 на Генеральной ассамблее ООН президент России Путин В.В. обозначил, что ключевой задачей международного сообщества во главе с Организации Объединённых Наций остаётся «обеспечение мира, региональной и глобальной стабильности». Отметив активное расширение экспансии ИГИЛ на другие регионы, в целях установления господства в исламском мире и не только там, Президент указал на необходимость руководствоваться не амбициями, а общими ценностями и общими интересами на основе международного права и «объединить усилия для решения стоящих перед нами новых проблем и создать по-настоящему широкую международную антитеррористическую коалицию», которая, «как и антигитлеровская, могла бы сплотить в своих рядах самые разные силы, готовые решительно противостоять тем, кто, как и нацисты, сеет зло и человеконенавистничество». При этом, ключевыми участниками такой коалиции Путиным В.В. обозначены именно мусульманские страны, подчеркнута важность, авторитет и наставническое слово мусульманских духовных лидеров, поскольку «Исламское государство» «не только несёт им прямую угрозу, но и своими кровавыми преступлениями оскверняет одну из величайших мировых религий – ислам», извращает его истинные гуманистические ценности. На церемонии открытия (спустя 10 лет

реконструкции) Соборной мечети в Москве (23.09.2015), на которой присутствовало около 800 тысяч духовных лидеров со всего мира, Президент России также подчеркнул важность отечественного исламского богословия в нашей стране, работы мусульманских духовных лидеров по противодействию пропаганде экстремизма и радикального псевдоислама.

Деятельность международных организаций «Исламское государство» и Джебхат ан-Нусра решением Верховного суда Российской Федерации от 29.12.2014 в нашей стране запрещена. Согласно закону, отныне любое участие в деятельности указанных террористических организаций считается уголовным преступлением и карается по всей строгости закона. Так, Федеральным законом от 02.11.2013 № 302-ФЗ в Уголовный кодекс Российской Федерации введена статья 205.5 «Организация деятельности террористической организации и участие в деятельности такой организации», предусматривающая за организацию деятельности организации, которая в соответствии с законодательством Российской Федерации признана террористической (ч.1 ст. 205.5 УК РФ) наказание в виде лишения свободы на срок вплоть до пожизненного лишения свободы. За участие в деятельности террористической организации (ч. 2 ст. 205.5 УК РФ) предусмотрено уголовное наказание в виде лишения свободы на срок до 10 лет и возможным штрафом в значительном размере. Указанным федеральным законом дополнена также редакция ч. 2 ст. 208 УК РФ, предусматривающая уголовную ответственность не только за участие в вооруженном формировании, не предусмотренном федеральным законом, а также и за участие на территории иностранного государства в вооруженном формировании, не предусмотренном законодательством данного государства, в целях, противоречащих интересам Российской Федерации (наказывается лишением свободы на срок до 10 лет с ограничением свободы на срок до 2 лет).

В последнее время международные террористические псевдоисламские организации заметно активизировались на территории Ирака, Сирии и Афганистана, при этом, вербовку сторонников ведут далеко за пределами этих стран. Только на территории Санкт-Петербурга в 2015 года зарегистрировано 7 (в 2014 году - 1) преступлений террористического характера, 3 из которых зарегистрированы по факту организации и участия в деятельности международной террористической организации «Партия исламского освобождения» («Хизб ут-Тахрир аль-Ислами»), 4 – по факту участия в незаконном вооруженном формировании «ИГИЛ» на территории Сирийской Арабской Республики.

Уже в этом году также возбуждено 1 уголовное дело по факту участия в ИГИЛ на территории Сирии. При этом, обвиняемыми по данным уголовным делам являются, в том числе учащиеся образовательных учреждений города (2-х университетов и 2- х колледжей). О каждом ставшем вам известном факте попытки вовлечения иных лиц в деятельность «ИГИЛ».

История создания Международной организации «Исламское Государство Ирака и Леванта» (ИГИЛ). Международная организация «Исламское

Государство Ирака и Леванта» (ИГИЛ), известная также под названием «Исламское Государство Ирака и Сирии», «Исламское государство Ирака и Шама» (ИГИШ) с лета 2014 года называется «Исламское государство». Она образована с 2006 года в результате слияния радикальных исламистских группировок, которые отпочковались от международной террористической организации «АльКаида». Основные идеологические постулаты организации изложены в Декларации, опубликованной на пяти языках и провозглашавшей создание нового псевдохалифата под властью халифа Ибрагима. Вообще, что такое халифат? Халифат (в переводе с арабского замещение, наследование)- это феодальное арабо-мусульманское теократическое государство, созданное пророком Мухаммедом и в последствии возглавляемое халифами. Примером такой формы государственного управления служит Османская империя, просуществовавшая с 1299 по 1922 год и находившаяся преимущественно на территории современной Турции. Халиф является самым высоким титулом у мусульман, это наместник или исполняющий обязанности Пророка. Он является гарантом соответствия повседневной жизни мусульман последнему божественному Посланию - Священному Корану. Муссульмане-сунниты полагают, что халифом может стать любой мусульманин, член мусульманской общины, независимо от расового, национального, социального и любого иного положения, которое компетентно в вопросах, связанных с государственным управлением. Для избрания халифа хватает проведенного внутри общины простого открытого голосования, на которое вносится ряд предложения о достойных кандидатурах, доказавших обществу свои необходимые навыки в деле управления, права и т.д. Халиф избирается большинством голосов.

Во главе ИГИЛ стоит халиф Ибрахим Аввад Ибрахим Али Мухаммад аль-Бадри ас-Самарраи, обладающий неограниченной властью. При нем действует совещательный орган – Шура, члены которого назначаются халифом. Летом 2014 г. боевики «Исламского государства» взяли под свой контроль ряд крупных городов в западном районе Ирака и вплотную подошли к Багдаду. В Сирии они оккупировали северную провинцию Рака, в центральном городе которой с одноименным названием была размещена штаб-квартира организации. Боевики «Исламского государства» используют флаг и эмблему «Аль-Каиды». Организация обладает боевым потенциалом (около 50 тыс. боевиков в Сирии и около 30 тыс. - в Ираке). В ее создании принимал активное участие иракский террорист Абу Мусаб аз-Заркауи - духовный лидер и ближайший соратник Усамы бен- Ладена. Ближайшей ее целью является создание на территории Сирии, Ирака и Ливана исламского суннитского государства, живущего по законам шариата, а также ведение так называемой священной войны (псевдоджихада) с «неверными» (кафирами) во всем мире.

Что подразумевает под собой понятие «джихад»? Джихад – в переводе с арабского означает усердие на пути Аллаха. Обычно джихад ассоциируется с вооруженной борьбой, однако это понятие значительно шире. Помимо вооруженной борьбы под ним также понимается борьба со своими духовными или социальными пороками, например с ложью, обманом, развращенностью

общества и т.д. Таким образом, джихад – это и борьба со своими страстями, и устранение социальной несправедливости, и постоянное усердие в деле распространения религии и, наконец, ведение войны с военными агрессорами во имя Аллаха. Изначально в исламе джихад является желательным, а не обязательным, и только в случае явных опасностей он становится обязательным. Проявление агрессии и убийства является большим грехом. В Коране сказано: «Кто убьет человека не за убийство или распространение нечестия на земле, то словно убил всех людей, а кто сохранит жизнь человеку, тот словно сохранит жизнь всем людям».

Основной закон в ИГИЛ гласит, что мусульмане обязаны соблюдать все законы шариата, а неверные (кяфиры) являются воплощением дьявола и должны быть либо убиты, либо взяты в рабство (женщины), к кяфирам относятся все мусульмане – шииты, алавиты, езиды, суфисты – неарабы, сторонники властей Сирии, Ирака, Саудовской Аравии, а также «не уважающие ислам и мусульман» христиане и иудеи. Командиры боевиков сами определяют, кто из христиан и иудеев не уважает ислам. Обычно уважаются только богатые люди, которые дают взятки и помогают боевикам в бизнесе, и те, за кого они просят. «Чистая, протоптанная тропа к воде» именно так переводят арабы слово шариат. Это образное выражение означает для каждого мусульманина - Закон, который им дал Аллах через своих пророков и последнего пророка посланника Мухаммеда.

Правила шариата также важны для верующего, как чистая вода для ума и души. Каждый правоверный должен строго следовать правилам и нормам, заложенным в мусульманской системе права. Статья 2 Каирской Декларации по Правам человека в исламе, принятой 05.08.1990 г. членами государств исламского сотрудничества, гласит, сохранение человеческой жизни в течение времени, отпущенного Господом, является обязанностью, предписанной шариатом. Другим правилом ИГИЛ является установленный дресс–код, обязывающий всех мужчин носить бороду, а женщин – носить чадру (легкое женское покрывало белого, синего или черного цвета) и абайу (длинное традиционное арабское женское платье с рукавами). Среди других правил выделяются следующие: - нельзя курить сигареты и употреблять жевательную резинку, за нарушение правила – 80 ударов плетью, - женщинам запрещено передвигаться на улице без сопровождения мужчины, пойманную женщину доставляют домой, а мужчина – опекун подвергается 80 ударам плетью. Проживающим на подконтрольных ИГИЛ территориях христианам запрещено: строить монастыри, церкви и кельи, демонстрировать религиозную символику и литературу, вслух читать церковные тексты и бить в колокола, христиане обязаны придерживаться дресс-кода ИГИЛ и хоронить своих единоверцев на специально отведенных новыми властями кладбищах. При этом, накладывается подать в размере 4 золотых динаров в год на «богачей», 2 – на представителей среднего класса и 1 – на «бедняков».

Боевики ИГИЛ объявили своей «добычей и целью» граждан России и Украины, находящихся в Сирии, посольства Российской Федерации и Украины,

другие объекты, принадлежащие этим странам. Лидеры «Исламского государства» в качестве объекта своих террористических устремлений рассматривают также территорию Российской Федерации. По фактам участия граждан России в незаконном вооруженном формировании «Исламское государство», вовлечения в такое участие, а также прохождения соответствующего обучения следственными органами России возбуждено и расследуется не менее 60 уголовных дел по ст.ст. 205.1, 205.3 и 208 УК РФ.

Правовые и организационные основы противодействия террористической деятельности, ответственность за ее осуществление определены Федеральным законом от 06.03.2006 № 35-ФЗ «О противодействии терроризму». Под терроризмом понимается идеология насилия и практика воздействия на принятие решения органами государственной власти, органами местного самоуправления или международными организациями, связанные с устрашением населения и (или) иными формами противоправных насильственных действий. Понятие террористическая деятельность включает в себя в том числе, организацию, планирование, подготовку, финансирование и реализацию террористического акта, подстрекательство к нему, организацию незаконного вооруженного формирования, преступного сообщества, вербовку, вооружение, обучение и использование террористов, пропаганду идей терроризма. Лидеры и авторитетные представители радикально-исламистских структур (далее - РИС) используют мощный комплекс идеологической обработки своих адептов в виде вырванных из контекста религиозных догматов ислама с целью установления тотальной ориентации членов на ведение агрессивно-наступательных действий, вплоть до подавления страха смерти, самопожертвования (например, самоподрывы террористовсмертников - «шахидов»).

Осознавая преступность своих действий по отношению к действующему законодательству, они, как правило, действуют конспиративно во время подготовки и совершения преступлений, стараются скрыть местоположение своих ячеек, их состав, лидеров, способы связи, часто используя методы конспирации. Адепты радикальных течений причисляют себя к исламской культуре и считают себя наиболее праведными мусульманами, исповедующими так называемый «чистый ислам». Однако, при осуществлении своей деструктивной деятельности представители РИС стараются интегрироваться в мусульманское сообщество региона, исповедующее традиционный ислам, в целях получения прикрытия для своих ячеек, захвата власти в указанной социальной группе путем постепенного втягивания и вербовки большого количества его членов, а также, манипулирования мусульманской общиной - «уммой» (например, инициирование протестных настроений и митингов в ответ на действия правоохранительных органов). Многие РИС создаются и поддерживаются иностранными спецслужбами, как мусульманских (Саудовская Аравия, Пакистан, Катар и другие), так и западных государств (США, Великобритания и другие). Представители РИС, действующие в различных регионах, часто связаны с этническими организационно-

преступными группами, состоящими из их земляков или просто мусульман. Это делается с целью маскировки своих действий под деятельность преступного сообщества, получения доходов для ведения экстремисткой деятельности криминальным путем и использования людских и материальных ресурсов организованных преступных групп.

Особый акцент в привлечении новых членов делается идеологическими лидерами радикально-исламистских структур на вербовке молодых девушек (в среднем 16-25 лет) славянской национальности из Российской Федерации. Это объясняется тем, что, во-первых, неофиткиславянки (неофит – от греч. neophytos – новообращенный, это новый сторонник какого-нибудь учения, новый последователь какой-нибудь религии) впоследствии станут эффективными вербовщицами для своих соотечественниц, вовлекая их рассказами про «хорошую жизнь в справедливом исламском государстве». Во-вторых, их удобно использовать для различных целей на территории Российской Федерации и европейских государств, так как внешность не вызывает особенных подозрений у сотрудников правоохранительных органов, они знают язык и культурные особенности этих стран.

В нашей стране в полный голос о проблеме заговорили после задержания российской студентки Карауловой В., которая через Турцию пробиралась в Сирию, на территорию подконтрольную ИГИЛ. Помимо подростков и женщин, экспертом среди вовлекаемых террористами лиц выделена категория «отъявленных подонков», которые находят для себя выход получить желаемое. Как известно, «Исламское государство» узаконило рабство, возродив рынки невольников и невольниц, где самый ходовой и дорогой товар - маленькие девочки.

Схема вербовки работает следующим образом. На первом этапе наводчик вычисляет потенциальную жертву, выявляет проблемы у члена коллектива. Затем в работу включается мотиватор, который сначала давит на существующие проблемы, преувеличивает их, а потом показывает «выход» - «прекрасный мир» «Исламского государства». Мотиватор заставляет поверить «клиента», что он может сделать нечто очень важное, внести вклад в общее дело, направленное на «спасение» человечества. Как «вдруг» появляется «уникальная возможность» встретиться с «очень важным человеком». Тогда и появляется вербовщик, рассказывающий сказки из серии: «Мы тебя заметили, признали твои способности и готовы тебе поручить важное дело». Не менее активно лидеры ИГИЛ проявляют себя на рынке продажи человеческих органов. Также, ими активно осуществляется торговля на черном рынке нефтью, культурными ценностями, захват заложников с целью выкупа. Следует отметить, что преступный доход поступает исключительно в карманы нескольких лидеров ИГИЛ. ИГИЛ – яркий пример террористической организации, которая обладает развитой медийной инфраструктурой и демонстрирует беспрецедентно высокий уровень владения передовыми информационнокоммуникационными технологиями, включая методы работы в социальных сетях. Особенно активно последними используется мессенджер

Telegram. Согласно данным опроса фонда «Общественное мнение» стремление молодых людей и девушек вступать в ряды террористических организаций, подобно ИГИЛ, связано с широкой пропагандой и зомбированием (так считают 29 % россиян). На сегодняшний день становится ясно, что в террористы начали уходить люди, воспитанные в привычной системе «семья-детсад-школа-вуз», что требует проведение соответствующей работы уже с пятилетними детьми, чтобы общение с потенциальными террористами было таким же табу, как разговор с «чужим дядей» на улице, таким же плохим вариантом при выборе стороны в игре в «войнушку», как «фашисты» и так далее. Хочется надеяться, что приведенные факты должны уберечь вас, молодое поколение, от совершения непоправимых ошибок. От куда уходит культура и просвещение приходят фанатики экстремизма, подменяющие основополагающие понятия одной из основных мировых религий. Не лучше ли направить свою энергию на стоящие занятия и дела (спорт, образование), которые в последующем вам принесут плодотворный доход на гораздо более длительную и привлекательную перспективу.

Список литературы

1. Федеральный закон от 25 июля 2002 г. N 114-ФЗ "О противодействии экстремистской деятельности" (с изменениями и дополнениями) // Собрание законодательства РФ.

2.Уголовный кодекс РФ от 13 июня 1996 г. № 63-ФЗ // Собрание законодательства Российской Федерации - 17 июня 1996 г. - № 25

3. Мозговой, В.Э. Информационный экстремизм как инновационная девиация социума начала XXI века. [Текст] / В.Э. Мозговой // Гуманитарные, социально-экономические и общественные науки – 2020. - №3 – С. 61-65

4. Алексеева, Д.И., Багаева, А.А. Экстремизм как угроза национальной безопасности россии: основные направления противодействия. [Текст] / Д.И. Алексеева, А.А. Багаева // Юридические науки – 2018. С. 261-263

5. Кудрин, В.С. Экстремистская деятельность молодёжи: классификация, формы и виды. [Текст] / В.С. Кудрин // Мир науки, культуры, образования. – 2015. - №6 – С. 79-83

Научное издание

ЭКСТРЕМИЗМ И ТЕРРОРИЗМ В КИБЕРПРОСТРАНСТВЕ: УГРОЗЫ МИРУ И БЕЗОПАСНОСТИ ЧЕЛОВЕЧЕСТВА

Сборник статей по итогам III Всероссийской студенческой научно-практической очно-заочной видеоконференции

Издание публикуется в авторской редакции
Дизайн обложки Ю.В. Плетнева

Подписано в печать
Формат 60х84 1 / 16.
Бумага офсетная.
Усл.-печ. л. 11,62. Тираж 100 экз. Заказ 391

Издательство Алтайского государственного университета

Типография Алтайского государственного университета:
656099 Барнаул, ул. Димитрова, 66