



ОРГАНИЗАЦИОННО-ПРАВОВЫЕ МЕРЫ ПРОТИВОДЕЙСТВИЯ ТЕРРОРИЗМУ В ЦИФРОВУЮ ЭПОХУ

Сборник статей
по итогам всероссийской конференции

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

**ОРГАНИЗАЦИОННО-ПРАВОВЫЕ МЕРЫ
ПРОТИВОДЕЙСТВИЯ ТЕРРОРИЗМУ
В ЦИФРОВУЮ ЭПОХУ**

Сборник статей по итогам всероссийской конференции



Барнаул

Издательство
Алтайского государственного
университета
2022

УДК 343.9
ББК 67.51
О 64

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, преподаватель кафедры уголовного права и криминологии юридического института Алтайского государственного университета, зам. руководителя РАНМЦ «Антитерроризм».

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;

О 64 Организационно-правовые меры противодействия терроризму в цифровую эпоху:
сборник научных статей / под ред. В.А. Мазурова, М.А. Стародубцевой; Министерство науки и высшего образования РФ, Алтайский государственный университет. – Барнаул : Изд-во Алт. ун-та, 2022. – 242 с.

ISBN 978-5-7904-2618-6.

В сборник включены статьи участников проходившей 15 декабря 2021 г. на базе юридического института ФГБОУ ВО «Алтайский государственный университет» IV Всероссийской научно-практической конференции «Организационно-правовые меры противодействия терроризму в цифровую эпоху».

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

УДК 343.9
ББК 67.51

ISBN 978-5-7904-2618-6

© Коллектив авторов, 2022
© Оформление. Издательство Алтайского
государственного университета, 2022

СОДЕРЖАНИЕ

ВВЕДЕНИЕ	6
ПЛЕНАРНОЕ ЗАСЕДАНИЕ	9
Мазуров В.А. О НЕКОТОРЫХ АСПЕКТАХ КОНТРПРОПАГАНДЫ ИДЕОЛОГИИ ТЕРРОРИЗМА, ОРГАНИЗАЦИИ ПРАВОВОГО ОБУЧЕНИЯ ГРАЖДАН КРАЯ, ВОСПИТАТЕЛЬНОЙ РАБОТЫ В ОБРАЗОВАТЕЛЬНЫХ ОРГАНИЗАЦИЯХ.....	9
Стародубцева М.А. ПРОБЛЕМНЫЕ АСПЕКТЫ ОПРЕДЕЛЕНИЯ ПРАВОВОГО СТАТУСА РЕГИОНАЛЬНОГО АНТИТЕРРОРИСТИЧЕСКОГО НАУЧНО-МЕТОДИЧЕСКОГО ЦЕНТРА ФГБОУ ВО «АЛТАЙСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ».....	15
СЕКЦИЯ «ОРГАНИЗАЦИОННО-ПРАВОВЫЕ ФОРМЫ ПРОТИВОДЕЙСТВИЯ ТЕРРОРИЗМУ В ОБРАЗОВАТЕЛЬНЫХ ОРГАНИЗАЦИЯХ»	23
Кравченко И. О. РОЛЬ ВЫСШИХ УЧЕБНЫХ ЗАВЕДЕНИЙ В ФОРМИРОВАНИИ АНТИТЕРРОРИСТИЧЕСКИХ ВЗГЛЯДОВ В СТУДЕНЧЕСКОЙ СРЕДЕ.....	23
Куликов Е.А. МЕЖДУНАРОДНО-ПРАВОВОЕ РЕГУЛИРОВАНИЕ ПРОТИВОДЕЙСТВИЯ ТЕРРОРИЗМУ, СЕПАРАТИЗМУ И ЭКСТРЕМИЗМУ В УСЛОВИЯХ НОВОГО ЭТАПА НАУЧНО-ТЕХНИЧЕСКОГО ПРОГРЕССА: ОПЫТ ШАНХАЙСКОЙ ОРГАНИЗАЦИИ СОТРУДНИЧЕСТВА.....	31
Березовская А.Ю. ПРОФИЛАКТИЧЕСКАЯ РАБОТА ПО ПРОТИВОДЕЙСТВИЮ ЭКСТРЕМИЗМА И ТЕРРОРИЗМА В ВЫСШИХ УЧЕБНЫХ ЗАВЕДЕНИЯХ.....	40
Попова Е.В. ЛИНГВИСТИЧЕСКАЯ ЭКСПЕРТИЗА КАК МЕТОД ПРОТИВОДЕЙСТВИЯ РАСПРОСТРАНЕНИЮ ЭКСТРЕМИЗМА.....	48
Литвинова А.С. ОРГАНИЗАЦИОННО-ПРАВОВЫЕ МЕРЫ ПРОТИВОДЕЙСТВИЯ КИБЕРТЕРРОРИЗМУ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ ОБЩЕСТВА.....	53
Корниенко Л.Ю. ПУБЛИЧНОЕ ДЕМОНИСТРИРОВАНИЕ НАЦИСТСКОЙ СИМВОЛИКИ В СЕТИ ИНТЕРНЕТ.....	60
Богданов И.С. «ФЕНОМЕН ДИПФЕЙКА»: УГРОЗА НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ.....	63

Гоберник Д.В. КИБЕРЭКСТРЕМИЗМ В ДЕЯТЕЛЬНОСТИ МОЛОДЕЖНЫХ СУБКУЛЬТУР ДИСКРИМИНАЦИОННОЙ НАПРАВЛЕННОСТИ.....	68
Захарова А.П. ОСОБЕННОСТИ ПРОФИЛАКТИКИ ПРЕСТУПЛЕНИЙ ЭКСТРЕМИСТСКОЙ НАПРАВЛЕННОСТИ В МОЛОДЕЖНОЙ СРЕДЕ.....	75
Валова Ю.А. РОСТ КИБЕРТЕРРОРИЗМА В СВЯЗИ С ПЕРЕХОДОМ В ДИСТАНЦИОННЫЙ ФОРМАТ	82
Пинчук А.П. НЕКОТОРЫЕ ПРОБЛЕМЫ ИСТОЧНИКОВ ОПЕРАТИВНО-РОЗЫСКНОГО ПРАВА В ОБЛАСТИ ПРОТИВОДЕЙСТВИЯ КИБЕРЭКСТРЕМИЗМУ	90
Матвеева С.В. РЕГИОНАЛЬНЫЕ ОСОБЕННОСТИ ЭКСТРЕМИСТСКОЙ ПРЕСТУПНОСТИ В АЛТАЙСКОМ КРАЕ	103
Башкатова М.М. ПОЛИТИЧЕСКИЕ ИНФОРМАЦИОННЫЕ УГРОЗЫ И ПУТИ ИХ УСТРАНЕНИЯ	108
Стародубцева М.А., Ельникова С.М. СОЦИО-КУЛЬТУРНЫЕ ПРЕДПОСЫЛКИ ФОРМИРОВАНИЯ ТЕРРОРИСТИЧЕСКИХ ВОЗЗРЕНИЙ В МОЛОДЕЖНОЙ СРЕДЕ	113
Стародубцева М.А., Саенко А.А. АНАЛИЗ ВОВЛЕЧЕННОСТИ СТУДЕНТОВ И ПРЕПОДАВАТЕЛЕЙ В КОНТПРОПАГАНДИСТСКУЮ ДЕЯТЕЛЬНОСТЬ В АЛТАЙСКОМ КРАЕ	120
СЕКЦИЯ «НАУЧНО-ПРАВОВЫЕ ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ ТЕРРОРИЗМУ В ЦИФРОВУЮ ЭПОХУ: ВЗГЛЯД СТУДЕНТОВ»	131
Застрожных М.С. ПАТРИОТИЗМ, КАК ОСНОВА КОНТРТЕРРОРИСТИЧЕСКОЙ ПРОФИЛАКТИКИ.....	131
Аксенова А.Д., Домбровская А.А. ВИДЫ ПРЕСТУПЛЕНИЙ В СФЕРЕ ЦИФРОВОЙ ИНФОРМАЦИИ	139
Колесниченко Е.И. ПРОФИЛАКТИКА И ПРОТИВОДЕЙСТВИЕ КИБЕРПРЕСТУПНОСТИ	147
Суварян А.С. НЕКОТОРЫЕ АСПЕКТЫ КРИМИНОЛОГИЧЕСКОЙ ХАРАКТЕРИСТИКИ КИБЕРПРЕСТУПЛЕНИЙ.....	153
Корватко Н.А. ПРОФИЛАКТИКА ЭКСТРЕМИЗМА И ТЕРРОРИЗМА В КИБЕРПРОСТРАНСТВЕ	159
Гауэрт М.В. РАСПРОСТРАНЕНИЕ ИНФОРМАЦИИ ЭКСТРЕМИСТСКОЙ НАПРАВЛЕННОСТИ В СОЦИАЛЬНЫХ СЕТЯХ	172

Монисовой Е.Д., Колосничих А.И. КОНТРПРОПАГАНДА ИДЕОЛОГИИ ЭКСТРЕМИЗМА И ТЕРРОРИЗМА В МОЛОДЕЖНОЙ СРЕДЕ	182
Барсукова А.П. АНАЛИЗ ВЛИЯНИЯ НА МОЛОДЁЖЬ НЕПРИЕМЛЕМОГО КОНТЕНТА В СОЦИАЛЬНОЙ СЕТИ ТИК ТОК В 2021 ГОДУ	192
Юлин М.А. КОНТРПРОПАГАНДА ИДЕОЛОГИИ ТЕРРОРИЗМА И ЭКСТРЕМИЗМА	201
Зеленко А.Б. ПРОБЛЕМА ОСВЕДОМЛЕННОСТИ ГРАЖДАН ОТНОСИТЕЛЬНО ЦИФРОВЫХ АСПЕКТОВ ТЕРРОРИЗМА.....	208
Бойцова А.А. ОТРИЦАТЕЛЬНОЕ ВЛИЯНИЕ ДОРАМЫ «ИГРА В КАЛЬМАРА» НА ЗРИТЕЛЕЙ. МИФ ИЛИ РЕАЛЬНОСТЬ?.....	216
Вдовинков С.С. ПСИХОЛОГИЧЕСКИЕ АСПЕКТЫ КИБЕРТЕРРОРИЗМА	224
Ненашев Е.Д. СПОСОБЫ ПРОТИВОДЕЙСТВИЯ КИБЕРТЕРРОРИЗМУ ...	229
ФОТОАРХИВ КОНФЕРЕНЦИИ.....	238

ВВЕДЕНИЕ

15 декабря 2021 года на базе Юридического института ФГБОУ ВО «Алтайский государственный университет» прошла IV Всероссийская научно-практическая конференция **«Организационно-правовые меры противодействия терроризму в цифровую эпоху»**.

В организации и работе конференции приняли участие представители Экспертного совета по выработке информационной политики профилактики идеологии терроризма в Алтайском крае, Межведомственной комиссии по противодействию экстремизму администрации г. Барнаула, Регионального антитеррористического научно-методического центра ЮИ Алтайского государственного университета, образовательных и волонтерских организаций.

Активное участие в работе конференции приняли представители Барнаульского юридического института МВД России, Алтайского филиала Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации, Алтайского государственного медицинского университета, Алтайского государственного университета, Колледжа ФГБОУ ВО «Алтайский государственный университет».

Конференция проведена в целях формирования платформы между образовательными учреждениями в сфере профилактики идеологии экстремизма и терроризма, деструктивного поведения среди обучающихся, а также совершенствования взаимодействия по данному направлению с органами власти и силовыми структурами.

С приветственным словом к участникам конференции обратился член Экспертного совета по выработке информационной политики в сфере противодействия идеологии терроризма Антитеррористической комиссии Алтайского края, профессор кафедры уголовного права и криминологии Юридического института АлтГУ, доктор юридических наук А. П. Детков. Он отметил, что проблема распространения идеологии терроризма и экстремизма

остается актуальной. В первую очередь идеологи международных террористических организаций стремятся организовать работу в молодежной среде, поэтому особенно важно организовать противодействие распространению идеологии терроризма и экстремизма среди молодежи.

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 В. А. Мазуров в своем выступлении положительно оценил проведение подобных мероприятий на разных уровнях, но с сожалением отметил, что панацея для решения проблемы пока не выработана. Тем не менее, ожидаемые результаты, которые конференция априори позиционировала - формирование платформы для обмена опытом и совершенствования взаимодействия образовательных организаций с представителями власти и правоохранительными органами - заложили фундамент для движения по намеченному вектору.

В интересных и информативных выступлениях представителей различных образовательных организаций прозвучали статистические данные и конкретные примеры, иллюстрирующие необходимость не только огромной и крайне важной работы организаций по предотвращению преступлений экстремистского характера, но еще более важной и сложной профилактической деятельности.

Уникальной особенностью проведенной конференции можно отметить участие в ней лидеров студенческого антитеррористического движения в Алтайском крае. В обсуждении приняли участие секретарь Барнаульского отделения Всероссийской общественной организации «Молодая гвардия Единой России» С. М. Ельников, лидер волонтерского отряда АлтГУ «Антиэкстремизм» А.А. Саенко, подготовившие работы под руководством заместителя руководителя Регионального антитеррористического научно-

методического центра, преподавателя кафедры уголовного права и криминологии М.А. Стародубцевой.

Участники конференции выступали в двух секциях. Особо отмечены были доклады Валовой Ю.А., Литвиновой А.С. –представителей Алтайского филиала Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации и Гоберника Д.В., представителя Барнаульского юридического института МВД России.

В заключительном слове член Межведомственной комиссии по противодействию экстремизму администрации г. Барнаула А. Ю. Деев подвел итоги конференции, поблагодарил участников за плодотворную работу, указав, что приоритетной задачей образовательных учреждений является не просто привить установки на недопустимость использования насилия для решения каких бы то ни было задач, а способствовать формированию полноценной личности, осознающей себя и свое место в жизни и обществе.

ПЛЕНАРНОЕ ЗАСЕДАНИЕ

Мазуров В.А.,

доцент кафедры уголовного права и криминологии АлтГУ, кандидат юридических наук, доцент, руководитель РАНМЦ «Антитерроризм», член Экспертного совета по выработке информационной политики в сфере профилактики терроризма при Антитеррористической комиссии Алтайского края

Мазуров В.А. О НЕКОТОРЫХ АСПЕКТАХ КОНТРПРОПАГАНДЫ ИДЕОЛОГИИ ТЕРРОРИЗМА, ОРГАНИЗАЦИИ ПРАВОВОГО ОБУЧЕНИЯ ГРАЖДАН КРАЯ, ВОСПИТАТЕЛЬНОЙ РАБОТЫ В ОБРАЗОВАТЕЛЬНЫХ ОРГАНИЗАЦИЯХ

(на примере Регионального антитеррористического научно-исследовательского и учебно-методического центра юридического института Алтайского госуниверситета)

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. Угрозу национальной безопасности России сегодня осложняются активизацией враждебной политикой официального Киева, украинских националистов.

Отмечается активизация экстремистских и террористических проявлений и в 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.

В Алтайском госуниверситете порядка 10 лет проводится целенаправленная научно-исследовательская, учебно-методическая и профилактическая работа, сначала в рамках Научно-образовательного центра университета «Правовое обеспечение противодействия экстремизму и терроризму» (Центр). Работа Центра осуществлялась под патронажем Минобрнауки края и аппарата Антитеррористической комиссии Алтайского края.

В декабре 2018 года Президент Российской Федерации утвердил Комплексный план противодействия идеологии терроризма в Российской Федерации на 2019-2023г.г. что предопределило проведение мероприятий по совершенствованию системы противодействия идеологии терроризма в крае. По решению Антитеррористической комиссии Алтайского края, в 2019 году, сформирован и успешно работает Экспертный 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 Алтайского края и рекомендации Министерства образования и науки Алтайского края, на базе юридического института университета образован Региональный

антитеррористический научно-исследовательский и учебно-методический центр (далее – РАНМЦ), разработан и утвержден план работы центра на 2020-2023г.г. Ряд мероприятий РАНМЦ включены в план противодействия терроризму в Алтайском крае на 2021 год. Разработан долгосрочный план профилактики идеологии терроризма в университете, приказом ректора создана рабочая группа по реализации данного плана. Активно и результативно работают входящие в структуру РАНМЦ студенческие волонтерские организации университета – «Кибердружина22» и «Антиэкстремизм». За активную профилактическую деятельность, руководителям этих организаций объявлена благодарность Министерства образования и науки Алтайского края. Студенческое объединение «Антиэкстремизм» - действует с 2016г. на базе Юридического института. Благодаря деятельности объединения обучающиеся могут познакомиться с законодательством Российской Федерации в сфере противодействия экстремизму и терроризму. Студенческая организация «Кибердружина22» - реализуется при поддержке РАНМЦ и молодежного парламента Алтайского края. Основным полем деятельности Кибердружины является борьба с незаконным контентом в сети «Интернет». В рамках проекта проходят образовательные лекции, интерактивы по противодействию экстремизму и идеологии терроризма в социальных сетях. Так, в рамках Правовой акции, проведенной организацией «#КИБЕРДРУЖИНА22» в апреле 2021 г. были обучены 250 студентов.

РАНМЦ отработано взаимодействие с органами исполнительной власти края - Министерством образования и науки Алтайского края, аппаратом Антитеррористической комиссией Алтайского края, Экспертным советом по выработке информационной политики противодействия терроризму, членом которого является руководитель РАНМЦ, правоохранительными органами. С образовательными организациями - вузами края, Барнаульской духовной семинарией и общественными организациями – Общественной палатой края, диаспорами, ветеранскими организациями. Ежегодно проводятся научно-практические конференции, семинары, конкурсы на лучшую научную работу,

видеофильм, презентацию по проблемам противодействия экстремизму как идеологии терроризма и терроризму всероссийского и регионального уровня.

Сегодня можно говорить о том, что в университете создана система мер профилактики экстремизма, идеологии терроризма и иных деструктивных проявлений в студенческой среде, РАНМЦ является одним из звеньев системы противодействия терроризму в Алтайском крае.

Имеют место и проблемы, препятствующие эффективности профилактической работе. Это проблема отсутствия предметно сформулированной и понятной гражданскому населению идеологии России, которую можно и нужно использовать при планировании и проведении контрпропагандистских мероприятий идеологии терроризма. С этой проблемой мы столкнулись при разработке по поручению Минобрнауки края, Концепции противодействия идеологии терроризма в Алтайском крае. Сегодня мы работаем над этой проблемой.

Вместе с тем, в целях повышения эффективности научно-исследовательской, методической и профилактической работы, в рамках плана РАНМЦ и университета 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, привлечены 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 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 медиационных центров, которые формируют информационное образовательное пространство, с привлечением студентов к созданию контента. В этой работе приоритетное место должны занимать управление по воспитательной работе, лига студентов, при поддержке юридического института, РАНМЦ, Экспертного совета по выработке информационной политики противодействия терроризму Антитеррористической комиссии Алтайского края.

- в целях повышения эффективности системы профилактики национализма, экстремизма, терроризма в Алтайском крае, в Министерство

образования и науки и Антитеррористическую комиссию Алтайского края, направлено предложение по созданию онлайн курсов для специалистов и работников сферы образования Алтайского края. Дистанционная форма обучения позволит обучающимся получить адресную юридическую и экспертную поддержку, Программа обучения слушателей подготовлена Центром повышения квалификации и кафедрой уголовного права и криминологии юридического института университета.

Предложенные меры по совершенствованию профилактики национализма, экстремизма, идеологии терроризма носят далеко не исчерпывающий характер. Полагаем, что одним из основных приоритетов государства и общества на современном этапе, является работа по защите молодежи от негативного влияния внешних и внутренних деструктивных сил по моральному разложению россиян, созданию плацдарма для разрушения государства российского. Будущее России за современной молодежью.

Стародубцева М. А.,

преподаватель кафедры уголовного права и криминологии АлтГУ,
зам. руководителя РАНМЦ «Антитерроризм»,
г. Барнаул

Стародубцева М.А. ПРОБЛЕМНЫЕ АСПЕКТЫ ОПРЕДЕЛЕНИЯ ПРАВОВОГО СТАТУСА РЕГИОНАЛЬНОГО АНТИТЕРРОРИСТИЧЕСКОГО НАУЧНО-МЕТОДИЧЕСКОГО ЦЕНТРА ФГБОУ ВО «АЛТАЙСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Введение

Сегодня неотъемлемой частью военно-политического дискурса стала гибридно-информационная война, непрерывно ведущаяся на международной арене. Одним из основных игроков в информационном противостоянии сегодня стал международный терроризм в форме транснациональных террористических объединений, обладающих развернутой системой медиа-ресурсов и практически бесконтрольно распространяющих свои идеологические постулаты в киберпространстве. Причем, зачастую подобные формирования создаются либо спонсируются государствами, что дает основания назвать терроризм и кибертерроризм полноценным оружием гибридной войны.

Уже можно открыто указать, что сегодня внешние и внутренние деструктивные силы, используя возможности медиа-технологий и средств управления массами, проводят работу по моральному разложению российской молодежи, прежде всего развивая в ней негативное отношение к российской власти, недоверие, разжигая националистические и террористические настроения и иные негативные настроения и проявления. К таковым, на взгляд автора, относятся, в частности, всплеск случаев скулшутинга в российских образовательных учреждениях, активизация националистских и террористических организаций, многочисленные суицидальные сетевые

сообщества. По нашему мнению, данные негативные проявления, в конечном итоге, позволяют вовлекать неустойчивую молодежь в экстремистские и террористические организации и группировки в России. Эта работа практически открыто направлена на политическое и экономическое ослабление России.

До недавнего времени профилактическая работа в области противодействия распространению идеологии терроризма среди молодежи проводилась силами отдельных руководителей ВУЗов и координаторов студенческих организаций ряда образовательных учреждений России либо путем создания при образовательных организациях центров профилактики экстремизма и терроризма.

Отсюда, целью настоящего исследования выступает анализ специфики правового статуса центров профилактики экстремизма и терроризма при учреждениях образования.

Методы и материалы

Проблеме правового статуса субъектов научной и образовательной деятельности посвящены труды Бочарникова Д.А., Бочарниковой М.А., Степаненко Ю.В., Савиной А.К., и иных авторов. Однако, нужно сразу же отметить, что ни в их работах, ни на законодательном уровне термин «центр профилактики экстремизма и терроризма» не фигурирует [4, с. 48]. Данные труды посвящены обоснованию необходимости выделения специальной отрасли – научного права, в частности, основной акцент исследователи делают на регламентации правового статуса ученых как индивидуальных субъектов. В анализируемой сфере этот аспект практически не затрагивается, и провести анализ дискуссионных мнений, на взгляд автора, представляется весьма затруднительным. Отсюда автор уже сейчас может увидеть, что изучаемый ими вопрос мало освещен и практически не отражен в научных исследованиях, одновременно, являясь достаточно острым и наболевшим в практическом аспекте.

Новизна проводимого исследования заключается в обосновании назревшей необходимости оформления и детальной регламентации правового статуса центров профилактики экстремизма и терроризма.

Методологическую основу исследования составляют общенаучные (анализ и синтез, сравнительный метод, выявление причинно-следственных связей) и специальные научные методы.

Методы анализа и сравнения помогли проанализировать имеющиеся нормативные акты в области образования, дали возможность построения картины функционирования при образовательных организациях России центров профилактики экстремизма и терроризма, позволили выявить проблемы правового регулирования данных организаций, пробелы и сложности их функционирования.

Результаты и дискуссия

Базовым нормативно-правовым актом в сфере образования выступает Федеральный закон «Об образовании в Российской Федерации» от 29.12.2012 № 273-ФЗ (далее – Федеральный закон № 273-ФЗ) [9, с. 3]. В статье 10 данного закона определена структура системы образования. Из совокупности представленных там учреждений для нас представляет интерес п. 5 ч. 1 ст. 10, где указаны объединения юридических лиц, работодателей и их объединений, общественные объединения, осуществляющие деятельность в сфере образования. Однако, сопоставив данную норму с выявленной нами практикой организации центров профилактики экстремизма и терроризма в образовательных учреждениях, автор может сказать, что большинство подобных центров не являются юридическими лицами, не связаны с объединениями работодателей и не могут заключать от своего имени трудовые договоры [5, с. 7].

Обратившись же к законодательству об общественных объединениях, авторы в ст. 5 Федерального закона от 19.05.1995 № 82-ФЗ (ред. от 30.12.2020) «Об общественных объединениях» (далее - Федеральный закон №82-ФЗ) отмечают, что законодатель понимает под общественным объединением

добровольное, самоуправляемое некоммерческое формирование, созданное по инициативе граждан для решения указанных в программных документах объединения целей [10, с. 8]. Если же мы возьмем в качестве практического примера Региональный антитеррористический научно-методический центр (РАНМЦ), функционирующий на базе ФГБОУ ВО «Алтайский государственный университет», то увидим, что он создан на основании решения Антитеррористической комиссии Алтайского края (протокол №73 от 02.03.2020 года). То есть, под смысл общественного объединения подобная организация не подпадает.

Еще одним нормативным актом в смежной области выступает Федеральный закон от 23.08.1996 №127-ФЗ «О науке и государственной научно-технической политике» (далее – Федеральный закон №127-ФЗ) [8, с. 5]. Он определяет правовое положение научных организаций, государственных академий наук и высшей аттестационной комиссии. Но, углубившись в текст данного закона, мы увидим, что в случае с научной организацией речь снова идет о юридическом лице, причем обладающем, в случае с научным центром, специальным оборудованием и условиями для осуществления научной деятельности. То есть, и в этом случае центр профилактики экстремизма и терроризма остается «не у дел», ведь у таких организаций нет экспериментальных установок, специального оборудования и прав юридического лица [1, с. 8].

В Положении о Региональном антитеррористическом научно-методическом центре АлтГУ отмечено, что данная организация функционирует в качестве опорного центра по методической, научно-исследовательской работе и проведению региональных профилактических мероприятий антитеррористической направленности. Подобное определение дают и учредительные документы аналогичных организаций [2, с. 105]. С этой позиции центр профилактики экстремизма и терроризма может быть причислен к организациям, осуществляющим научно-методическое и ресурсное обеспечение системы образования (ч. 1 ст. 19 Федерального закона № 273-ФЗ).

Однако перечень научно-методических организаций законодатель не дает и полномочия их не раскрывает, сосредотачиваясь далее на деятельности учебно-методических объединений, к коим центр профилактики экстремизма и терроризма, исходя из его полномочий и даже названия, отнести точно нельзя.

В ч. 1 ст. 27 Федерального закона № 273-ФЗ указано, что образовательные организации самостоятельно принимают решения об изменении своей структуры. И в пункте 1.2. Положения о Региональном антитеррористическом научно-методическом центре АлтГУ указано, что упомянутый центр является структурным подразделением университета, без права юридического лица, функционирующим на основании локальных нормативных актов университета и анализируемого положения [3, с. 18].

Далее в ст. 27 Федерального закона № 273-ФЗ законодатель указывает примерный перечень структурных подразделений в образовательных учреждениях, где снова не фигурирует центр профилактики экстремизма и терроризма [9, с. 6]. Мы видим, что образовательная организация вольна внутри себя создавать любые структурные подразделения, даже не поименованные в законе, и подобная автономия, безусловно, важна для учебного процесса и его научно-методического обеспечения. Но эта же ситуация демонстрирует и отсутствие системы в формировании при образовательных учреждениях подобных антитеррористических структур, и отсутствие координации и взаимодействия между ними [6, с. 41]. Ничего из этого не прописано ни на законодательном уровне, ни на уровне подзаконных актов. Даже обратившись к локальным нормативным актам ФГБОУ ВО «Алтайский государственный университет», единственный акт об антитеррористическом центре, который можно найти – это само Положение об антитеррористическом центре.

Рассмотрев аналогичные организации при образовательных учреждениях России, автор и вовсе видит пеструю и хаотичную картину организаций с разными наименованиями, разным подчинением и совершенно разным функционалом. К ним примыкают студенческие волонтерские отряды, чей правовой статус не определен даже в Положении о координирующем их

центре. Зачастую, студенческие отряды не имеют собственных учредительных документов, либо существуют только на бумаге [7, с. 81].

Отсюда, проанализировав правовой статус центра профилактики экстремизма и терроризма можно сделать следующие выводы.

Во-первых, нормы, регулирующие правовой статус центров профилактики экстремизма и терроризма, отсутствуют как таковые, а имеющиеся прямо указывают на правовую неопределенность регулирования декларируемых положений.

Во-вторых, отсутствие в Федеральном законе № 273-ФЗ четкого наименования центров профилактики экстремизма и терроризма существенно снижает роль университетов в осуществлении этой деятельности и роль самих центров.

В-третьих, Федеральным законом № 273-ФЗ не предусмотрен порядок регулирования деятельности центров профилактики экстремизма и терроризма, причем он не прописан и на уровне подзаконных актов [9, с. 11].

На взгляд автора, в этом свете, весьма важным является решение Департамента государственной молодежной политики и воспитательной деятельности Министерства науки и высшего образования Российской Федерации по созданию сети центров по организации и координации работы, направленной на формирование у молодежи активной гражданской позиции, предупреждение межнациональных и межконфессиональных конфликтов, противодействие идеологии терроризма и профилактику экстремизма. ФГБОУ ВО «Алтайский государственный университет» вошел в число 23 ВУЗов России, на базе которых будут созданы координационные центры. Сегодня в университете проводится работа по созданию координационного центра на базе Регионального антитеррористического научно-методического центра. Готовятся предложения по структуре координационного центра и кадровым решениям.

С учетом задач, изложенных в Типовом Положении о Координационном центре, рекомендованном Департамента государственной молодежной

политики и воспитательной деятельности Министерства науки и высшего образования Российской Федерации, проводится деятельность по решению организационных вопросов и разработке программы работы центра. Учитывая имеющиеся наработки, данная работа проводится во взаимодействии и под патронажем Аппарата Антитеррористической Комиссии Алтайского края, Министерства образования и науки Алтайского края, ректората университета.

Автор считает, что проводимая Министерством науки и высшего образования Российской Федерации деятельность по организации и координации работы, направленной на противодействие идеологии терроризма, профилактику экстремизма, весьма своевременна и будет содействовать повышению эффективности данной работы, прежде всего, в молодежной среде.

Заключение

Базовой проблемой, выделенной автором, является нечеткое правовое регулирование статуса центров профилактики экстремизма и терроризма при образовательных учреждениях. Данные организации, обычно являясь структурными подразделениями ВУЗов на практике имеют весьма абстрактный перечень обязанностей, практически не урегулированный на уровне законов и подзаконных актов. А между тем, в связи с нарастающим в обществе напряжением, вызванным гибридно-информационной войной в медиа, и всплесками актов агрессии среди и против молодежи, центров профилактики экстремизма при российских ВУЗах создается все больше. Сегодня уже сделаны первые шаги к созданию единой сети подобных центров. Однако, их правовое регулирование оставляет желать лучшего: во-первых, нормы нечеткие и неопределенные, во-вторых, на уровне законов и подзаконных актов не фигурирует термин «центр профилактики экстремизма и терроризма», и в-третьих, ни на одном уровне не прописан порядок функционирования подобных центров, вследствие чего пока на практике наблюдается путаница и рассогласованность действий.

Список литературы

1. Абазов, К.М. Проблема использования современных информационно-коммуникационных технологий международными террористическими организациями / Вопросы безопасности. – 2018. – № 3. – С. 1 – 9.
2. Абдулатипов, А.М. Понятие информационного терроризма / Юридический вестник Дагестанского государственного университета. – 2019. – № 2. – С. 105 – 111.
3. Авдеев, В.А., Авдеева, О.А. Преступность террористического характера и экстремистской направленности в РФ: состояние и тенденции правового регулирования / Российский судья. – 2018. – № 8. – С. 18 – 23.
4. Бутусова, Л.И. К вопросу о киберпреступности в международном праве / Вестник экономической безопасности. – 2016. – № 2. – С. 48 – 52.
5. Выручаев, А.А. Правовой статус Российской академии наук (современные правовые проблемы) / Известия Института государства и права РАН. – 2008. – С. 1 – 10.
6. Мазуров, В.А. Кибертерроризм: понятие, проблемы противодействия / Доклады ТУСУР. – 2010. – № 1–1 (21). – С. 41 – 45.
7. Обрывко, Е.И., Стародубцева, М.А., Саенко, А.А. О некоторых аспектах повышения правовой культуры в вопросах профилактики экстремизма и идеологии терроризма в образовательной среде / Гуманитарные, социально-экономические и общественные науки. – 2020. – № 11. – С. 81 – 84.
8. О науке и государственной научно-технической политике: федеральный закон от 23 августа 1996 г. №127-ФЗ / Собрание законодательства РФ.
9. Об образовании в Российской Федерации: федеральный закон от 29 декабря 2012 г. №273-ФЗ / Собрание законодательства РФ.
10. Об общественных объединениях: федеральный закон от 19 мая 1995 г. №82-ФЗ / Собрание законодательства РФ.

**СЕКЦИЯ «ОРГАНИЗАЦИОННО-ПРАВОВЫЕ ФОРМЫ
ПРОТИВОДЕЙСТВИЯ ТЕРРОРИЗМУ В ОБРАЗОВАТЕЛЬНЫХ
ОРГАНИЗАЦИЯХ»**

Кравченко И.О.,

кандидат юридических наук, доцент, доцент
Байкальский государственный
университет, г. Иркутск

**Кравченко И. О. РОЛЬ ВЫСШИХ УЧЕБНЫХ ЗАВЕДЕНИЙ В
ФОРМИРОВАНИИ АНТИТЕРРОРИСТЕСКИХ ВЗГЛЯДОВ В
СТУДЕНЧЕСКОЙ СРЕДЕ**

Крайне удручающе выглядит сохранившаяся с «перестроечных времен» тенденция к принижению России, масштабной критике нашего государства на фоне восторгов иностранными спорными достижениями. В научной литературе можно встретить безапелляционные утверждения, что в настоящее время в России гражданское общество так и не сформировалось, и ставится вопрос о возможности его построения в России в принципе [1, с.33]. Подобные отрицательные установки вызывают у молодежи отторжение как идей государственности, так и образа гражданского общества, что, в свою очередь, ведет к формированию неуважительного отношения к Родине. В некоторой сфере это способствует даже формированию некой стыдливости, когда у образованной части молодежи возникает желание покинуть Россию и соединить свою жизнь с «правильным» обществом. Именно студенчество является такой лакмусовой бумажкой, впитывающей в себя, прежде всего, нигилистские убеждения и ярко демонстрирующие свое негативное отношение ко всему, на их взгляд, неправильному и старому. Надо отметить, что данный курс опасен, это убедительно иллюстрируется революционными событиями в нашей стране в XX веке и современными процессами на Украине, например.

Хотя еще Д.Дж. Элейзер отмечал, что для федерализма жизненно важной является идея наличия гражданского общества [2]. В этом смысле сам факт существования Российской Федерации уже сам по себе заявляет не просто о наличии гражданского общества, но его значимой роли в нашей стране.

В этом смысле громко звучит заявление о том, что на Западе гражданское общество формировалось путем завоевания прав снизу, а в России права были дарованы сверху [3, с.10]. Однако, в начале XX века именно Россия приобрела колоссальный опыт «завоевания прав снизу» и, тем не менее, политика двойных стандартов даже этот исторический факт стремится принизить и проигнорировать, продолжая обвинительные умозаключения относительно отсутствия зрелости российского гражданского общества.

Необходимо отметить, что тема поиска путей противодействия терроризму именно среди студентов в настоящее время особенно популярна, только на площадке одной из электронных библиотек elibrary по данному запросу было найдено 285069 публикаций. Масштабы террористической активности в среде молодежи вызывают острую тревогу общества и требуют принятия активных мер противодействия.

Действительно, роль и механизмы действия идеологии в современном российском обществе уже сильно отличаются от советского периода и продолжают меняться, что не всегда возможно адекватно описать в рамках господствующей научно-исследовательской парадигмы [3, с.2].

Эффекты экстремизма на фоне роста ксенофобии – питательная среда для террористических проявлений. Проблема в том, что гражданское общество с разрушенной старой моделью и не до конца сформировавшейся новой идеологий не может эффективно противостоять терроризму, впрочем, как и государство.

Молодежь в силу присущим им характеристикам, как то незрелость собственных суждений, желание самоутвердиться, поиск самоидентичности, максимализм восприятия, мобильность, готовность к активной деятельности, клиповое мышление, отточенное на тестовом методе, склоняет к восприятию

поверхностного слоя информации, преподнесенного под ярким лозунгом, при отсутствии стремления к глубокому анализу. С одной стороны – это нормальная стадия развития человека, стандартные проблемы отцов и детей, но сейчас можно говорить об усугублении этой ситуации огрехами экспериментов над системой образования, начиная от школы и заканчивая вузом.

Вполне убедительными представляются выводы авторов исследования конфликтогенного потенциала молодежи в полиэтнических регионах России о наличии ряда проблем в сфере образования – это, прежде всего, отсутствие или размытость идеологических ориентиров, негативное влияние СМИ и Интернета, снижение общего уровня образования и низкий уровень педагогических кадров[4, с. 114]. Очевидно, что разработка мер по противодействию терроризму должна включать в себя нивелирование обозначенных детерминант.

В качестве основных черт современной российской молодежи в ходе проведенного А.П. Шевчик исследования [5, с. 29], выделены такие заслуживающие внимания факторы, как: отсутствие систематического духовного развития, идеологическая неразборчивость; толерантность к криминалу и иным негативным антиобщественным и антигосударственным явлениям; подверженность манипулятивным технологиям формирования оценок и стереотипов поведения; устойчивая склонность к импульсивным и агрессивным действиям и суждениям.

Цифрофикация современного общества, повсеместное распространение системы Интернет, включая и отдаленные от центральных районов населенные пункты, на фоне всех позитивных достижений несет в себе угрозы распространения терроризма. Особенно остро эта проблема затрагивает молодежь. Ошибочно молодые люди воспринимают интернет среду как безопасную, молодежную площадку, зачастую даже не понимая таящейся там угрозы. При этом преступный мир активно осваивает интернет-ресурсы и использует открывающиеся возможности для достижения своих целей, манипулируя неподготовленным сознанием молодого пользователя. Между

тем, Интернет позволяет поддерживать анонимность недобросовестной стороны, иметь большой охват участников, несвязанных границами, обеспечивает высокие обороты распространения информации, потворствует осуществлению натиска и массивированной психологической атаки, делает возможным использование современных технологий, адаптивных к восприятию молодежной среды. Главное, чтобы молодой человек не оставался один на один с обилием информации из Интернета, чтобы ему оказывалась помощь в фильтрации, анализе и построении прогноза, студенчество не должно быть беззащитным от атак вербовщиков террористов.

Безусловно, окружающая социальная среда является определяющим фактором формирования и развития молодежи. Студенческая среда в этом смысле аккумулирует в себе и в концентрированном виде демонстрирует все проблемы общества.

Повествование о правильных вещах в классической манере выглядит в глазах молодежи долгим и скучным, к сожалению, в априори не может вызвать правильный отклик. Без сомнения, говорить с молодежью нужно на их языке, учитывая особенности восприятия информации этого поколения. Необходимо отметить, что вербовщики террористических организаций уже давно освоили этот метод и активно его используют. Молодежь в настоящее время не смотрит научно-документальные фильмы, интервью умных и знающих людей, даже художественные фильмы востребованы выборочно. Требуется иное преподнесение информации. Запрос у гражданского общества на новый конвент общения с молодежной средой есть.

Немаловажный фактор в формировании агрессивного настроения в молодежной среде является отсутствие социальных гарантий трудоустройства по полученной специальности. Данное положение в целом вызывает апатию и агрессию, но у определенной части это трансформируется в экстремистские и террористические настроения. Интервьюирование студентов однозначно демонстрирует, что доминирующая часть не видит своего будущего, не уверена в своем завтра, боится коррупционных схем трудоустройства, не верит в

значимость своего профессионализма. Спокойствие выражают лишь те студенты, кто уверен в возможностях своих родителей решить вопрос с их трудоустройством. Указанные эмоциональные факторы гасят желание учиться, повышать свой профессиональный уровень, занимать активную гражданскую позицию и настраивают на радикальный лад в стремлении что-то изменить. Не вызывает сомнений, что в основе терроризма лежит конфликт.

Красиво и убедительно Р.Мертон [6] обосновал роль социального напряжения в формировании девиантного поведения, где в качестве основной причины преступности выделяется несоответствие ожидания и реальности, когда возникают противоречия между ценностями, на которые общество нацеливает людей, и возможностями их достижения по установленным обществом правилам. Надо отдать должное, что предложенная концепция особенно ярко проявляется в студенческой среде в современных условиях.

Справедливой и правильной представляется идея о необходимости противопоставления идеологии терроризма идеологией патриотизма. Без сомнения, знание своей истории, гордость за достижения предков, стремление им соответствовать и сделать нечто большее для своей страны, любовь к Родине, развитое чувство собственного достоинства, принятие своей идентичности, преданность своему многонациональному народу – это базисные качества, препятствующие возникновению и развитию идей терроризма.

Участие общественных объединений в выработке стратегии предупреждения терроризма – малоизученный и малоиспользуемый подход. На самом деле, формирование третьего сектора в виде включения гражданского общества в борьбу против терроризма является перспективным и актуальным направлением.

Развал сформированной в советское время модели образования на фоне хаотичных попыток слепого следования западным течениям привели к утрате роли вуза в воспитании молодежи. Действительно, в ситуации, когда образование стало услугой, студент не может понять разницу и продолжает двигаться по знакомому рыночному пути, действуя по принципу «кто платит,

тот прав», что, в свою очередь, ведет к утрате уважительного отношения к преподавателю и восприятию его как Учителя. Кроме того, вуз, даже государственный, поставлен на коммерческие рельсы, ведь государственные дотации ничтожно малы и необходимо «зарабатывать», чтобы защитить свои позиции. В таких условиях сохранение студенческого массива становится необходимым фактором выживания. Профессорско-преподавательский состав лишается возможности реализовать наставнические функции, в силу того, что студент просто не готов так воспринимать преподавателя в предложенной современным миром модели взаимоотношений.

Необходимо отметить, что в ряде высших учебных заведений пытаются сейчас реанимировать реализацию в учебном процессе воспитательной задачи. Однако те мероприятия, которые проходят в обозначенном направлении (конкурсы чтецов, спортивные состязания, фотовыставки и т.д.) – лишь верхушка айсберга. Думается, что главное – это изменение стиля взаимоотношений в сфере студент-преподаватель. Нужно создать условия, прежде всего, для реализации воспитательной функции в образовательной среде. Это и поднятие престижа преподавательской деятельности, и минимизация коммерческого подхода в образовании, и сохранение кадрового потенциала профессорско-преподавательского состава, и введение наставничества как доминирующей функции преподавателя, и, конечно, разработка мер социальных гарантий трудоустройства выпускников по специальности на основе результатов их достижений.

Перспективным представляется создание добровольных объединений студентов, занимающихся научным исследованием и, соответственно, предупреждением терроризма и экстремизма (СНО). На начало 2021 г. такие объединения уже были созданы в 35 субъектах РФ на базе центров научно-исследовательской деятельности, факультетов и институтов вузов [7, с. 16]. Это идеальная модель, ведь участниками становятся студенты, которые осуществляют научную деятельность под кураторством профессорско-преподавательского состава вуза. Таким образом, сами студенты являются

активной стороной процесса, формируют отрицательное восприятие идеологии терроризма и экстремизма.

В эпоху глобализации именно вуз должен стать той защитной стеной между преступным террористическим миром и молодежью. Именно вуз осуществляет социализацию молодого поколения, формируя и оттачивая базисные ценности. Сейчас очевидно, что противодействовать распространению терроризма только за счет использования мер государственного принуждения утопично. Представляется, что решающая роль здесь отводится гражданскому обществу.

Таким образом, реформирование и масштабное изменение образовательной парадигмы в высших учебных заведениях – глобальная стратегическая задача государства в обеспечении безопасности населения страны. Антитеррористическая модель, думается, должна основываться на качественном воспитании молодежи. Конечно, отторжение идей терроризма – это основной принцип деятельности гражданского общества.

Список литературы

1. Кирик В.А. К вопросу о методологии исследования генезиса гражданского общества и взаимодействия общества и государства / В.А. Кирик // Научная мысль Кавказа. – 2009. – № 1. – С.33-38
2. Элейзер Д.Дж. Сравнительный федерализм / Д.Дж. Элейзер // Полис. – 1995. – № 5.
3. Бушуев А.М., Сердобинцев К.С. Идеология в системе взаимодействия государства и гражданского общества / А.М. Бушуев, К.С. Сердобинцев // Социально-гуманитарные знания. – 2012. – №4. – С1-13
4. Маркин В.В., Рогова А.В. Противодействие распространению экстремизма и терроризма в молодежной среде. Часть 2. / В.В. Маркин, А.В. Рогова // Власть. – 2012. – № 12. – С. 114-118

5. Шевчик А.П. Место и роль вуза в формировании антиэкстремистского и антитеррористического сознания молодежи / А.П. Шивчик // Создание воспитательной антиэкстремистской и антитеррористической среды в современном вузе: Материалы Международной научно-практической конференции / под ред. В.Е. Быданова; СПбГТИ (ТУ). – 2016. – С. 27-29

6. Мертон Р. К. Социальная структура и аномия / Р.М. Мертон // Социология преступности (Современные буржуазные теории). — М.: Прогресс, 1966. — С. 299—313.

7. Венцель С.В. Информационная справка по студенческим научным обществам, занимающимся исследованием терроризма и (СНО) / С.В. Венцель // Обзор.НЦПТИ. – 2021. – №2 (25). – С.16-17.

Куликов Е.А.

кандидат юридических наук, доцент,

и.о. заведующего кафедрой

уголовного права и криминологии,

Алтайский государственный университет, г. Барнаул

**Куликов Е.А. МЕЖДУНАРОДНО-ПРАВОВОЕ РЕГУЛИРОВАНИЕ
ПРОТИВОДЕЙСТВИЯ ТЕРРОРИЗМУ, СЕПАРАТИЗМУ И
ЭКСТРЕМИЗМУ В УСЛОВИЯХ НОВОГО ЭТАПА НАУЧНО-
ТЕХНИЧЕСКОГО ПРОГРЕССА: ОПЫТ ШАНХАЙСКОЙ
ОРГАНИЗАЦИИ СОТРУДНИЧЕСТВА**

Правовые инструменты. Основным международным документом в рассматриваемой сфере на пространстве Шанхайской организации сотрудничества (далее - ШОС) выступает Шанхайская конвенция о борьбе с терроризмом, сепаратизмом и экстремизмом от 15 июня 2001 года (далее - Шанхайская конвенция). Она определяет основные термины, обозначает направления и принципы сотрудничества стран-участниц, выступает с момента заключения и вступления в силу основным рамочным актом ШОС в анализируемой сфере. Шанхайская конвенция определяет терроризм как любое деяние, направленное на то, чтобы вызвать смерть какого-либо гражданского лица или любого другого лица, не принимающего активного участия в военных действиях в ситуации вооруженного конфликта, или причинить ему тяжкое телесное повреждение, а также нанести значительный ущерб какому-либо материальному объекту, равно как организация, планирование такого деяния, пособничество его совершению, подстрекательство к нему, когда цель такого деяния в силу его характера или контекста заключается в том, чтобы запугать население, нарушить общественную безопасность или заставить органы власти либо международную организацию совершить какое-либо действие или

воздержаться от его совершения; соответствующие деяния должны быть признаны уголовно наказуемыми в национальном уголовном праве [9]. В приведенном определении содержится указание на возможные последствия, потерпевших, характер деяния, цель совершения деяния, а также на варианты соучастия в этом деянии.

Сепаратизм Шанхайская конвенция определяет как «какое-либо деяние, направленное на нарушение территориальной целостности государства, в том числе на отделение от него части его территории, или дезинтеграцию государства, совершаемое насильственным путем, а равно планирование и подготовка такого деяния, пособничество его совершению, подстрекательство к нему, при условии, что такие деяния уголовно наказуемые в национальном уголовном праве» [9]. Сложность при формулировании трактовки сепаратизма связана с тем, что сталкиваются два международных принципа – уважения и сохранения территориальной целостности государств и права нации на самоопределение вплоть до отделения.

Экстремизм, в соответствии с Шанхайской конвенцией, – это «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, при условии признания их уголовно-наказуемыми в национальном уголовном праве» [9]. Это определение ставит экстремизм в один ряд с терроризмом и сепаратизмом по характеру и степени общественной опасности. Смысл приведенных положений Шанхайской конвенции состоит в понимании «трех зол» как достаточно опасных деяний, не просто наказуемых в уголовно-правовом порядке, но подрывающих конституционный строй, безопасность государства, территориальную целостность и общественную безопасность. В связи с этим необходимым становится взаимодействие государств, особенно граничащих

между собой, в целях пресечения возможности укрыться от уголовного преследования на территории другого государства.

В Аналитической записке по Шанхайской конвенции о борьбе с терроризмом, сепаратизмом и экстремизмом от 21 сентября 2020 года (далее - Аналитическая записка) такой подход подвергнут критике, сказано, в частности, что «некоторые аспекты определений терминов «терроризм», «сепаратизм» и так называемый «экстремизм» в Шанхайской конвенции, а также масштабы упомянутых в ней подготовительных или вспомогательных действий представляются расплывчатыми, чрезмерно широкими и неограниченными, и не дают представления о преступном умысле, который является необходимым элементом уголовного преступления; это вызывает озабоченность по поводу соблюдения принципов законности и определенности, предусмотренных уголовным правом и международными стандартами в области прав человека» [1].

Авторы Аналитической записки уточняют далее свои замечания. «Наиболее проблематичным с точки зрения прав человека является требование об установлении уголовной ответственности за так называемый "экстремизм" или "сепаратизм", поскольку эти термины носят неопределенный и субъективный характер и могут обозначать широкий диапазон действий, а также то, какое воздействие это требование может оказать на свободу мысли, совести, религии или убеждений, свободу выражения мнения, свободу ассоциаций и мирных собраний, свободу участия в политической жизни и свободу самоопределения. Более того, отсутствие обязательных определений таких терминов и возможность принятия государствами-участницами собственных национальных определений в контексте Шанхайской конвенции считаются особенно проблематичными на международном уровне» [1]. Последнее обстоятельство вряд ли вообще следует признать существенным недостатком Шанхайской конвенции, поскольку она определяет вопросы сотрудничества ее участников, а непосредственные меры уголовно-правового реагирования предусматриваются национальным правом (как это, например,

сделано в ст.ст. 205, 280.2, 278 УК РФ). Что же касается универсальных прав человека, то они отражены в основополагающих международных актах о правах человека, на которые Шанхайская конвенция активно ссылается, о некоторых прямо упоминает в Приложении к ней.

Шанхайская конвенция в ст. 6 предусматривает конкретные способы сотрудничества, в частности: обмен информацией; разработка и принятие согласованных мер для предупреждения, выявления и пресечения терроризма, сепаратизма и экстремизма, и взаимоуведомление о результатах их осуществления; обмен нормативными правовыми актами и материалами по практике их применения; обмен опытом работы по предупреждению, выявлению и пресечению проявлений терроризма, сепаратизма и экстремизма; подготовка, переподготовка и повышение квалификации своих специалистов в различных формах, и др. [9]. Хотя необходимость взаимодействия в научной и научно-технической сфере прямо не названа в тексте документа, однако перечисленные направления вряд ли осуществимы без развития научно-технического сотрудничества между странами-участницами ШОС. То же самое можно сказать и про предусмотренную в ст. 7 возможность обмена информацией между участниками Шанхайской конвенции о формах, методах и средствах совершения деяний, представляющих собой проявления терроризма, сепаратизма и экстремизма. Речь идет о сотрудничестве, например, в области криминалистической техники и тактики, напрямую завязанных на достижениях естественных и технических наук. Взаимодействие в научно-технической сфере способно выступить важной составной частью для укрепления совместных усилий по противодействию угрозе «трех зол».

В развитие Шанхайской конвенции принимаются ещё два договора. Во-первых, Конвенция ШОС против терроризма от 16 июня 2009 года (далее – Конвенция против терроризма). В этом документе разграничиваются понятия «терроризм» и «террористический акт», терроризм определяется как «идеология насилия и практика воздействия на принятие решения органами власти или международными организациями путем совершения либо угрозы

совершения насильственных и (или) иных преступных действий, связанных с утрашением населения и направленных на причинение ущерба личности, обществу и государству» [5]. Наблюдается гармонизация международного и национального права в части определения терроризма и общественно опасных его проявлений. Интересна также трактовка в Конвенции против терроризма террористической организации: «преступная группа, незаконное вооруженное формирование, банда, преступное сообщество, создаваемые для совершения преступлений и (или) совершающие преступления, охватываемые настоящей конвенцией; юридическое лицо, от имени, по указанию или в интересах которого осуществляется планирование, организация, подготовка и совершение хотя бы одного из преступлений, охватываемых настоящей Конвенцией» [5]. Обращает на себя внимание двойственность в понимании террористической организации – это и изначально преступное объединение, и юридическое лицо, изначально не являющееся преступным объединением, но совершающее преступления террористической направленности. При этом наблюдается как сходство, так и различие с установленными УК РФ составами преступлений, предусмотренными в ст. 205.4 и 205.5. Сходство состоит в двойственности, различие в том, что юридическое лицо оценивается как террористическая организация после судебного акта о признании ее таковой.

Ст. 7 Конвенции против терроризма устанавливает основные направления сотрудничества между странами-участницами в рамках предмета ее регулирования. «Стороны поощряют межрелигиозный и межкультурный диалог, охватывающий, где это необходимо, неправительственные организации и другие институты гражданского общества, при условии соблюдения национального законодательства в целях предупреждения ситуаций напряженности, которые могут привести к совершению преступлений, охватываемых настоящей Конвенцией» [5]. Необходимым условием успешности такого диалога выступают глубокие социально-антропологические, культурологические и религиоведческие исследования, дабы наметить общие взгляды, точки соприкосновения и общее направление взаимодействия в целом.

Такие исследования невозможны, в свою очередь, без развития взаимодействия в научной и научно-технической сфере между странами – участницами ШОС. Аналогичной наукоемкостью обладают такие предусмотренные в ч. 2 ст. 7 анализируемой конвенции меры, как: периодическая оценка правовых документов, регулирующих противодействие терроризму, и практических мер с точки зрения их эффективности; повышение профессионального уровня сотрудников правоохранительных и иных органов, осуществляющих противодействие терроризму; улучшение защиты физических лиц и объектов, включающее внедрение стандартов, предназначенных для повышения защищенности физических лиц и объектов; создание и внедрение критериев идентификации физических и юридических лиц, причастных к совершению преступлений, охватываемых настоящей Конвенцией; просвещение общественности об опасности терроризма и его негативных последствиях, а также об ответственности за совершение преступлений, охватываемых настоящей Конвенцией; обеспечение возможности населения информировать государственные органы, в том числе анонимно, о любых деяниях, которые могут рассматриваться в качестве преступлений, охватываемых настоящей Конвенцией [5]. Названные направления сами по себе предполагают достаточно высокий уровень развития научной и научно-технической сферы в том или ином государстве. Учитывая же, что террористические преступления выступают преступлениями международного характера [8], взаимный обмен опытом в части научных достижений позволит странам-участницам ШОС, по меньшей мере, не отставать от террористических формирований в освоении и использовании достижений научно-технического прогресса.

Во-вторых, Конвенция ШОС по противодействию экстремизму от 9 июля 2017 г., (далее – Конвенция по противодействию экстремизму). Экстремизм в этой конвенции определяется как «идеология и практика, направленные на разрешение политических, социальных, расовых, национальных и религиозных конфликтов путем насильственных и иных антиконституционных действий» [6]. Конвенция также определяет понятие «экстремистский акт», не известное

на УК РФ, ни федеральному закону от 25 июля 2002 г. N 114-ФЗ "О противодействии экстремистской деятельности" (в случае с последним наблюдается и некоторое расхождение в общем понятии экстремизма, которое он определяет перечневым путем, и перечень этот шире по объёму, чем определено Конвенцией по противодействию экстремизму) [7]. Названные обстоятельства способны вызвать сложности в организации сотрудничества по противодействию данному социально негативному явлению, а также сами по себе требуют дополнительных научных исследований, результаты которых должны быть положены в основу совершенствования правовых предписаний.

Ряд положений ст. 7 Конвенции по противодействию экстремизму практически идентичны уже рассмотренным положениям ст. 7 Конвенции против терроризма. Отметим, однако, также ещё такие направления в Конвенции по противодействию экстремизму, как усиление пропагандистской деятельности по противодействию экстремизму и контрпропаганды против распространения экстремистской идеологии, в том числе в средствах массовой информации и сети Интернет; мониторинг средств массовой информации и сети Интернет в целях своевременного выявления и пресечения распространения экстремистской идеологии; ограничение доступа к экстремистскому материалу, размещенному в информационно-телекоммуникационных сетях, в том числе в сети Интернет; укрепление культурных традиций, духовного, нравственного и патриотического воспитания, призванного побудить граждан осознанно противостоять экстремизму [6]. Речь идет о развитых информационных технологиях, массовости и всеохватности сети Интернет, которая стала удобной площадкой для экстремизма. Скорость же развития информационных технологий, глобальный характер информационно-телекоммуникационных сетей, делают зачастую невозможными противодействие преступлениям, совершаемым в сети Интернет, силами одной страны. Необходимым условием здесь выступает взаимобмен научно-технологическими разработками и слаженная работа правоохранительных органов различных стран.

Конвенция по противодействию экстремизму в пп. 10 ч. 2 ст. 7 содержит прямое указание на необходимость научного сотрудничества между странами-участницами – в качестве одной из мер рассматривается «проведение исследований в сфере противодействия экстремизму, в том числе на международных площадках, участниками которых являются Стороны» [6]. Можно предположить, что это выражение определенной тенденции в информационную эпоху по повышению роли науки, по интернационализации науки и по ее проникновению во все сферы социальной жизни. Научные исследования рассматриваются в качестве одной из составляющих политики противодействия социально вредным явлениям, в том числе угрозе «трех зол».

Список литературы

1. Даффи Х., Грин А. Аналитическая записка по Шанхайской конвенции о борьбе с терроризмом, сепаратизмом и экстремизмом. Варшава: Бюро ОБСЕ по демократическим институтам и правам человека, 2020.

2. Душанбинская декларация двадцатилетия ШОС // <http://rus.sectesco.org/>

3. Заявление Совета глав государств-членов Шанхайской организации сотрудничества о противодействии распространению террористической, сепаратистской и экстремистской идеологии, в том числе в сети Интернет. г. Москва, 10 ноября 2020 г. // URL: <http://rus.sectesco.org/>

4. Заявление Совета глав государств-членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности. г. Москва, 10 ноября 2020 г. // URL: <http://rus.sectesco.org/>

5. Конвенция Шанхайской организации сотрудничества против терроризма. Заключена в г. Екатеринбурге 16 июня 2009 г. // URL: <http://rus.sectesco.org/>

6. Конвенция Шанхайской организации сотрудничества по противодействию экстремизму. Заключена в г. Астана 9 июля 2017 г. // URL: <http://rus.sectesco.org/>

7. О противодействии экстремистской деятельности: федеральный закон от 25 июля 2002 г. N 114-ФЗ // <https://internet.garant.ru/#/document/12127578/paragraph/119:1>

8. Уткин В.А. Международное право борьбы с преступностью: учебное пособие. М.: ЮСТИЦИЯ, 2019.

9. Шанхайская конвенция о борьбе с терроризмом, сепаратизмом и экстремизмом от 15 июня 2001 г. // URL: <http://rus.sectesco.org/>

10. Шанхайская организация сотрудничества: новые приоритеты развития: монография / отв. ред. Т.Я. Хабриева. М.: Институт законодательства и сравнительного правоведения при Правительстве РФ: ИНФРА-М, 2017.

Березовская А.Ю.,
ФКОУ ВО Кузбасский институт ФСИН России,
курсант факультета правоохранительной деятельности, группа 23
Научный руководитель: Обернихина О. В.,
ФКОУ ВО Кузбасский институт ФСИН России, преподаватель
кафедры уголовно-исполнительного права и криминологии,
майор внутренней службы

Березовская А.Ю. ПРОФИЛАКТИЧЕСКАЯ РАБОТА ПО ПРОТИВОДЕЙСТВИЮ ЭКСТРЕМИЗМА И ТЕРРОРИЗМА В ВЫСШИХ УЧЕБНЫХ ЗАВЕДЕНИЯХ

В реалиях современности большой популярностью пользуется пропаганда экстремизма и терроризма, что в перспективе приведет к росту преступности и угрозе обороноспособности государства в целом, и как результат, нарушение прав человека, гарантированных Конституцией Российской Федерации [1].

Российская Федерация предпримет активные попытки предупреждения исследуемой преступности, как социально-негативного явления. Главной заслугой следует считать – формирование и развитие расширенной системы правоохранительных органов, в штат которой входят подразделения, деятельность которых направлена на предупреждение возникновения и развития организованных преступных сообществ и групп, целью которых выступает экстремизм и терроризм. Между тем, профилактические мероприятия, несмотря на их важность, не являются приоритетными по сравнению с предупреждением и пресечением, хотя их значение не умоляется ни в теории, ни в практике.

В некотором роде даже наиболее оправданным было бы изменить приоритеты правоприменителей в сторону развития профилактических

мероприятий, однако, к сожалению, в России на сегодняшний день для этого недостаточно ни финансовых ресурсов, ни человеко-ресурсов.

Согласно последним событиям, которые случились в России за 2016-2021 гг. в образовательных организациях возрос уровень совершения массовых убийств с применением огнестрельного оружия, такие случаи получили общественный резонанс. Средства массовой информации крупномасштабно повествуют нам о том, что причиной совершения таких преступлений послужили как распри и притеснения на расовой и межнациональной почве, так и банальный буллинг (с англ. Bullying – травля). Именно потому, в условиях экономии средств федерального бюджета оптимальным будет проводить более активно профилактическую работу не по всем направлениям, а наиболее криминально опасных, например, в сфере школьного образования и на базе средних и высших образовательных учреждений. Следует отметить, что сознание школьников и студентов более подвержено влиянию со стороны старшего поколения или криминальных групп, которые ведут пропаганду экстремизма, надеясь на поднятие криминального авторитета, получение быстрой выгоды и пр. Еще одной причиной совершения преступлений экстремистской и террористической направленности является то, что студенты, как правило, при поступлении в образовательные учреждения (средние и высшие) меняют место жительства и уезжают от контроля родителей, предаваясь самостоятельной, «разгульной» жизни. Часто в целях предупреждения травли они изначально желают вступить в любую криминально-опасную группу (формирование), чтобы не стать в последствии их же жертвой. Многих влечет интерес и жажда приключений, она изначально готовы и выражают глубокое желание стать частью чего-то большего, пусть даже если это экстремистское сообщество или террористическая организация. Им важен «командный дух» и жажда наживы, поскольку они переняли от родителей ли пришли самостоятельно к мысли о том, что государство не заботится об интересах граждан, коррумпировано и ждать чего-то от него

просто глупая трата времени и сил. Такое заблуждение выступает сильным мотиватором в выборе рода деятельности, в частности преступной.

К основным причинам совершения террористических и экстремистских преступлений следует также отнести:

- слабая или в некоторых образовательных учреждениях и ВУЗах социальная защищённость студентов;

- «юношеский максимализм», который выражается в действиях, словах, суждениях и поступках;

- «инфантилизм», который в свою очередь выражается своей незрелостью и замкнутости [6].

Следует отметить, что вышеуказанные причины знакомы не только криминологам теоретикам, а также правоприменителям, об этом осведомлены и сами преступники, которые используют их при вербовке новобранцев в свои ряды. Именно на стадии вербовки любые профилактические мероприятия будет наиболее эффективными [7].

Говоря о правовом регулировании вопроса профилактики экстремизма и терроризма в образовательных организациях, в первую очередь следует отметить ст. 3 ФЗ «Об образовании в Российской Федерации» [2], где закрепляется принцип приоритета жизни и здоровья человека, его прав и свобод. Исходя из этого следует проводить профилактику противодействия терроризма и экстремизма в образовательных учреждениях, в том числе с участием педагогов, которые будут привлечены к проведению воспитательной работы среди обучающихся по графику.

Согласно Постановлению Правительства Российской Федерации от 04.05.2008 г. №333 «О компетенции федеральных органов исполнительной власти» [3], руководство деятельностью этих самых органов осуществляет Правительство Российской Федерации, в области противодействия терроризму», при этом на Министерство образования и науки возложены следующие функции:

- проводить борьбу с пропагандой экстремистской и террористической идеологией;

- проводить борьбу с материалами, сведениями или рисунками, которые призывают к действиям террористической направленности, а также литература, которая несет в себе экстремистскую идеологию [8].

В настоящий момент данные функции образования осуществляются весьма слабо в образовательных учреждениях Российской Федерации, поэтому важно проводить работу в данной области и осуществлять соответствующую подготовку педагогов, по вопросам пропаганды экстремизма и терроризма. Однако следует учесть, что воспитательная работа подобного рода предполагает наличие у преподавателей (педагогов) знаний в соответствующей сфере, к примеру о том, какие составы преступлений включены согласно уголовного кодекса РФ [4] в категорию преступлений экстремистской и террористической направленности, каковы признаки этих составов преступления и пр. Для этого представляется обоснованным вводить курсы повышения квалификации, соответствующей направленности среди профессорско-педагогического состава образовательных организаций различного уровня, после чего профилактическая работа будет наиболее эффективной. После этого необходимо проводить работу следующего характера:

- прививать преподавателям вузов чувство толерантности у студентов;

- подробно изучать разную религию и культуру стран и народов, особенно тех, с кем мы соседствуем или которые проживают на территории Российской Федерации;

- организовывать совместные научные кружки и обсуждения каких-либо вопросов между студентами разных национальностей.

Следует отметить, что данная воспитательная и профилактическая работа в образовательных учреждениях и вузах должна носить всегда опережающий характер, если опоздать, то данные мероприятия можно считать слабо эффективными. Так с первого курса, с момента поступления студентов в стены

вуза, педагоги уже должны предотвратить конфликтные ситуации или какие-нибудь социальные отклонения. Именно поэтому в образовательных учреждениях и вузах должна вестись постоянная и интенсивная профилактическая работа по противодействию терроризма и экстремизма.

И поэтому было бы рациональнее внести изменения в учебные планы и программы обучения на тему «Профилактические мероприятия по противодействию экстремизму и профилактике терроризма в вузах России».

При разработке программы, направленной на противодействие экстремизма и терроризма среди обучающихся в России, следует учитывать ряд основополагающих принципов, таких как:

1. Принцип «актуальности» - данный принцип важен, тем что предполагает изучение всех детерминантов указанного вида преступности;

2. Принцип информационного опережения – предполагает формирование у обучающихся определенных правил поведения, которые предупреждают их вербовку в экстремистские и террористические группы;

3. Принцип информационной безопасности – педагоги обязаны рассказывать обучающимся полную информацию, которая касается основ экстремизма и терроризма;

4. Принцип «оптимизма» - в данном принципе, важно отметить, что педагоги должны объяснить обучающимся, что все проводимые террористические и экстремистские акты можно пресечь;

5. Принцип активности и самостоятельности обучающихся – сам обучающийся, должен еще кроме образовательной программы, стремиться к саморазвитию и расширению своего кругозора. Так человек становится счастливее, и его он начинает думать и мыслить гораздо масштабнее, чем причинить вред какой-либо группе, расе или национальности.

Программа, которая должна быть направлена на противодействие экстремизма и терроризма должна включать следующие мероприятия:

- сформировать у обучающихся в вузах соответствующий уровень правовой культуры;

- воспитание и развитие у обучающихся должного уровня знаний об основах мировых культур и народов;

- педагоги должны обращать внимание на то, что как и где проводят обучающиеся свой досуг или отдых, и оградить от негативного влияния преступных и незаконных группировок;

- материальная защищенность обучающихся. К примеру, после окончания вуза, помогать при трудоустройстве выпускникам, а также тем, кто находится в тяжелой материальной ситуации.

Следует отметить, что ключевым фактом противодействию экстремисткой и террористической идеологии будет являться научно-методическое обеспечение. Поэтому необходимо организовать взаимодействие образовательных организаций с правоохранительными органами, религиозными организациями, а также сотрудниками правоохранительных структур, которые непосредственно ведут борьбу и противодействуют экстремизму и терроризму. Данные лица могут должным образом повлиять на сознание обучающихся и рассказать случаи и примеры того, чем может быть опасен экстремизм и терроризм.

Таким образом, преступность террористического и экстремистского характера имеет тенденцию роста, отметим, что методы и способы вербовки подростков ежегодно совершенствуются и быстро адаптируются к реалиям современности, а также рассчитаны на первостепенные потребности кандидатов. Наиболее подверженными к негативному влиянию экстремистов и террористов являются несовершеннолетние, обучающиеся в ВУЗах и средне-технических и средне-специальных образовательных учреждениях. Основная причина их склонности – это бесконтрольность и жажда легкой наживы. Более сложными, с точки зрения психологии, выступают причины психологической и моральной неудовлетворенности подростков жизнью, травля сверстников, детские травмы, желание избежать роли жертвы, что предполагает занятие ниши преступника и пр.

В ходе исследования нами было установлено, что помимо организации взаимодействия образовательных организаций с правоохранительными структурами и различными институтами гражданского общества, особую актуальность представляет организация профилактической воспитательной работы со студентами профессорско-преподавательского состава образовательной организации, в рамках профилактики вовлечения студентов в экстремистскую и террористическую деятельность. Между тем, чтобы такая деятельность была наиболее эффективной среди профессорско-педагогического состава образовательных организаций следует провести курсы повышения квалификации. Тогда профилактическая работа будет не только эффективной, а перейдет из разряда устрашающей, в разряд разъяснительно-воспитательной.

Список литературы

1 Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) // Официальный интернет-портал правовой информации <http://www.pravo.gov.ru>, 04.07.2020.

2 Об образовании в Российской Федерации: Федеральный закон от 29 декабря. 2012 г. №273-ФЗ. (ред. от 02.07.2021) // Российская газета. - №303. - 2012 г. - 31 декабря.

3 О компетенции федеральных органов исполнительной власти, руководство деятельностью которых осуществляет Правительство Российской Федерации, в области противодействия терроризму: Постановление Правительства РФ от 4 мая 2008 г. №333. (ред. от 17.04.2021) // Собрании законодательства Российской Федерации. - 2008 г. - №19. - ст. 2172. - 12 мая.

4 Глебов В.В. О роли образовательных организаций в противодействии терроризму / В.В. Глебов // Формы и методы противодействия распространению идеологии экстремизма и терроризма среди молодёжи. Роль и

задачи образовательных организаций: материалы науч.-практ. конф. (г. Москва, 26–27 нояб. 2015 г.). М., 2015. - С. 11–15.

5 Дондоков Г.Д., Дондоков Ц.С. К вопросу об организации деятельности вузов России по противодействию терроризму и профилактике экстремизма среди студенческой молодёжи / Г.Д. Дондоков, Ц.С. Дондоков // Актуальные проблемы государственно-правового развития России. – 2018. – С. 87-93.

6 Матюхин А. В. Необходимые знания студентам о противодействии экстремизму (учебник «политика противодействия экстремизму» под редакцией А.П. Кошкина) / А. В. Матюхин // Журнал политических исследований. – 2021. – Т. 5. – № 1. – С. 178-184.

7 Обернихина О. В. К вопросу о реализации постановления Пленума Верховного суда Российской Федерации от 28 июня 2011 Г. № 11 «О судебной практике по уголовным делам о преступлениях экстремистской направленности» / О. В. Обернихина // Функционирование учреждений и органов, исполняющих уголовные наказания, в условиях реформирования уголовно-исполнительной системы : Материалы научных мероприятий, Псков, 02 ноября – 14 2018 года. – Псков: Псковский филиал Академии Федеральной службы исполнения наказаний, 2018. – С. 50-54.

8 Экстремистская деятельность (понятие, ответственность). Основные направления противодействию экстремизму: URL: <https://29.мвд.рф/document/10960492> (дата обращения 12.01.2021 г.).

Попова Е.В., курсант 4-го курса ФПСПиС,
Барнаульский юридический
институт МВД России,
рядовой полиции, г. Барнаул

Научный руководитель: Моисеев С.В., к.и.н., доцент кафедры ТГИИП
БЮИ МВД России

Попова Е.В. ЛИНГВИСТИЧЕСКАЯ ЭКСПЕРТИЗА КАК МЕТОД ПРОТИВОДЕЙСТВИЯ РАСПРОСТРАНЕНИЮ ЭКСТРЕМИЗМА

В современных реалиях виртуальная система является одним из самых эффективных средств распространения экстремистских материалов. Кроме того, Уголовный кодекс РФ и Кодекс об административных правонарушениях РФ имеют смежные составы, а именно ст.-ст. 280, 282 УК РФ и ст. 20.3.1 КоАП РФ, которые на практике разграничить порой затруднительно.

Лингвистическая экспертиза позволяет выявить побудительный потенциал текста [3], отвечая на такие вопросы как, например, имеются ли в представленных на экспертизу текстах высказывания, в которых выражено побуждение к совершению враждебных (насильственных) действий по отношению к лицу, группе лиц на основании их принадлежности к какой-либо расе, национальности, религии или иной группе, если да, то к кому обращено данное побуждение [1], а также на иные вопросы, постановка которых будет зависеть от признаков состава преступления или правонарушения, усматриваемого органами предварительного расследования в анализируемых материалах.

Говоря о правовом разграничении конкурирующих норм, необходимо обратиться к Постановлению пленума Верховного суда Российской Федерации № 11 г. Москва 28 июня 2011 г. «О судебной практике по уголовным делам о преступлениях экстремистской направленности» [4], который разъясняет, что статьей 280 УК РФ предусмотрена ответственность лишь за публичные

призывы к осуществлению экстремистской деятельности, а уже публичное распространение информации, в которой обосновывается необходимость совершения противоправных действий в отношении лиц по признаку расы, национальности, религиозной принадлежности и т.д., либо информации, оправдывающей такую деятельность, следует квалифицировать по статье 282 УК РФ при наличии иных признаков этого состава преступления. Ответственность по части 1 статьи 282 УК РФ наступает при условии, если действия, направленные на возбуждение ненависти либо вражды, а также на унижение человеческого достоинства, совершены лицом в течение одного года после привлечения его к административной ответственности за аналогичное деяние по статье 20.3.1 КоАП РФ. Ответственность по части 2 статьи 282 УК РФ наступает независимо от того, привлекалось ли ранее виновное лицо к ответственности по статье 20.3.1 КоАП РФ.

Под публичными призывами (статья 280 УК РФ) следует понимать выраженные в любой форме (например, в устной, письменной, с использованием технических средств) обращения к другим лицам с целью побудить их к осуществлению экстремистской деятельности. Под действиями, направленными на возбуждение ненависти либо вражды, следует понимать, в частности, высказывания, обосновывающие и (или) утверждающие необходимость геноцида, массовых репрессий, депортаций, совершения иных противоправных действий, в том числе применения насилия, в отношении представителей какой-либо нации, расы, социальной группы, приверженцев той или иной религии.

Для наглядности представим пример: если в сети Интернет размещен текст, в котором доказывается, что представители экваториальной расы повсеместно притесняют представителей европеоидной расы, избрали курс на ее искоренение и уничтожение, совершают особо тяжкие преступления исключительно по расовому признаку, то в этом случае имеются признаки преступления, предусмотренного ст. 282 УК РФ. Но если по результатам исследования данного текста делается вывод о необходимости сплотиться и

убивать представителей экваториальной расы, то в данном случае наличествует ст. 280 УК РФ.

Нередко органы предварительного расследования производят предварительную проверку по очевидно мнимому материалу, который в контексте не несёт никакой опасности, что в дальнейшем подтверждается экспертами. Это связано с неправильным представлением пользователей социальных сетей о тексте, содержащем призывы к экстремизму, страхом за близких, которые могут быть вовлечены в противоправную деятельность, непониманием разграничения относимости материалов к экстремистским и допущенным к распространению, концентрацией внимания на пугающие их слова без учёта контекста. Однако, благодаря кругу решаемых вопросов экспертами-лингвистами и их соответствующей адаптации, мы можем выделить маркеры, на которые необходимо обращать внимание в случае обнаружения подозрительного текста.

Исходя из наиболее распространённых видов, встречающихся в СМИ, и поступающих на экспертизу, мы выводим следующие маркеры:

1. Характер содержания написанного текста включает слова, предложения, сопряжённые с призывом к враждебности по отношению к другим национальностям, конфессиям, группам людей;

2. наличие фраз, направленных на побуждение к действиям, расцениваемых как экстремизм (уничтожение национальностей, побуждение к скулшутингу, склонение к участию в запрещённых организациях);

3. оправдание и обоснование (подкрепляют фактами и серьёзными доводами) экстремистской деятельности;

4. обоснование и оправдание расового и/или национального превосходства, оправдание совершения военных или других преступлений, направленных на частичное или полное истребление национальной, этнической, социальной, расовой или религиозной группы;

5. использование сленговых слов, а также выражений, характерных для различных субкультур [2];

б. нарочитое почитание лидеров экстремистских организаций, особенно тех, кто был осужден или убит.

Важно отметить, что элементы не должны терять своей значимости в совокупности со всем контекстом. Данные маркеры могут сопровождаться примерами, ориентированными на разные возрастные категории. Говоря о демонстрации материалов экстремистского характера, обратим внимание, что не является преступлением, предусмотренным статьями 280, 280.1 или 282 УК РФ, высказывание суждений и умозаключений, использующих факты межнациональных, межконфессиональных или иных социальных отношений в научных или политических дискуссиях и текстах, не связанных с реализацией намерения побудить других лиц к осуществлению экстремистской деятельности.

Список литературы

1. Российский Федеральный центр судебной экспертизы при Министерстве юстиции Российской Федерации. Лингвистическая экспертиза // [электронный ресурс] – Режим доступа: <http://www.sudexpert.ru/possib/lingv.php>, свободный. – Загл. с экрана. – Яз. Рус. – (Дата обращения: 22.09.2021).

2. О.И. Горюнова, Психолого-лингвистическая экспертиза экстремистских материалов: прикладной аспект // Нижегородский государственный университет им. Н.И. Лобачевского. – Н. Новгород, 2016, №6, с.109-111 – 243с.

3. Кукушкина О. В. Теоретические и методические основы судебной психолого-лингвистической экспертизы текстов по делам, связанным с противодействием экстремизму // О. В. Кукушкина, Ю. А. Сафронова, Т. Н. Секераж; Государственное учреждение РФЦСЭ при Минюсте России. – М., 2011. – 330 с.

4. Постановление пленума Верховного суда Российской Федерации № 11 г. Москва 28 июня 2011 г. «О судебной практике по уголовным делам о преступлениях экстремистской направленности» // [электронный ресурс] // СПС Консультант Плюс / Компания «Консультант Плюс». – Электрон. дан. – [М.]. – URL: http://www.consultant.ru/document/cons_doc_LAW_115712, свободный. – Загл. с экрана. – Яз. Рус. – (Дата обращения: 15.09.2021).

Литвинова А.С., юридический факультет,
Алтайский филиал
РАНХиГС,
г. Барнаул

Научный руководитель: Титаренко А.П., доцент кафедры уголовного права, уголовного процесса и криминалистики Алтайского филиала РАНХиГС,
к.ю.н., доцент

Литвинова А.С. ОРГАНИЗАЦИОННО-ПРАВОВЫЕ МЕРЫ ПРОТИВОДЕЙСТВИЯ КИБЕРТЕРРОРИЗМУ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ ОБЩЕСТВА

В современном мире все больше внимания уделяется компьютерным технологиям: совершенствуются программные обеспечения, создаются более совершенные технические устройства, улучшается защита информационных баз данных государственных органов и частных организаций, но, несмотря на это, каждый год происходят кибератаки, которые подрывают авторитет государственных служб, а также распространяют конфиденциальную информацию о гражданах. Для начала стоит дать определение понятию кибертерроризм, чтобы четко знать на что он направлен и отграничивать его от других преступлений.

Кибертерроризм – это комплекс незаконных действий в киберпространстве, создающих угрозу государственной безопасности, личности и обществу [1]. Данное преступление ставит перед собой несколько целей, главная из которых – это влияние на решение социальных, экономических и политических задач государства. В качестве других целей, которые преследует кибертерроризм является:

1. Взлом личной и конфиденциальной информации банков, спецслужб, организаций.
2. Распространение той же информации в открытом доступе.

3. Нарушение работы оборудования и программного обеспечения.
4. Атаки вирусными программами различных технических устройств.

Немало важно добавить, что, за последние несколько лет прослеживается рост числа киберпреступлений. Как отмечает Генеральный прокурор РФ И. Краснов на заседании Координационного совещания руководителей правоохранительных органов: «За последние 5 лет число таких преступлений возросло в 11 раз», - добавляя также, что в 2019 году было уже зафиксировано 294 тысячи киберпреступлений. А в первом полугодии 2020 года рост составил целых 92% [2]. На основании вышеизложенного можно выделить несколько факторов, способствующих этому.

Во-первых, пандемия и режим самоизоляции из-за коронавирусной инфекции. Огромное количество услуг, работы переместилась в сеть Интернет, вследствие чего стало больше возможностей для взлома и распространении конфиденциальной информации.

Во-вторых, недостаточная защита виртуальных данных, что делает их более легким источником для незаконного получения доступа.

В качестве примера можно привести случай взлома базы данных Российского Визового центра в США в 2016 году, в ходе которого хакер получил личные данные нескольких тысяч людей, которые подавали заявку на получение визы [3]. Неизвестное лицо представило скриншот (от англ. screenshot – «снимок экрана», то есть изображение, полученное устройством и показывающее в точности то, что видит пользователь на экране монитора), на котором располагались имена, электронные адреса, телефоны пострадавших людей. Хакер заявил, что не будет публиковать данную информацию, потому что не преследует такой цели. В этом конкретном случае он хотел донести до администраторов сайта мысль о том, чтобы они защищали данные лучше и понимали последствия такого взлома.

Существует несколько источников подобных кибератак.

1. Организованные преступные группы.
2. Зарубежные государственные структуры.

3. Террористические группы.
4. Передача данных уволенным сотрудником конкурентам.

Согласно части 3 статьи 35 Уголовного кодекса РФ, организованной группой признается устойчивая группа лиц, заранее объединившихся для совершения одного или нескольких преступлений. То есть можно сделать вывод, что главная цель именно этого источника кибератак – это совершение преступления и получение финансовой или иной материальной выгоды.

Вторым источником кибертерроризма служат зарубежные государственные структуры, которые, в первую очередь, интересуются кражей данных, в том числе интеллектуальной собственности у компаний-разработчиков, правительственных агентств и корпораций – военных подрядчиков.

Третьим считаются террористические группы, ищущие новые способы повлиять на политику страны с помощью масштабных кибератак на критические важные объекты инфраструктуры, от которых в существенной степени зависит весь образ жизни людей. Например, в августе 2021 года Общественный штаб по наблюдению за выборами в Москве объявил поиск программиста, который сумел обойти алгоритм электронного голосования во время ее тестирования [4]. После того как хакер вошел в систему онлайн-голосования, он смог отказаться от одного из двух бюллетеней, что ранее считалось невозможным. Таким образом, специалисты смогли выявить недостатки в системе онлайн-голосования.

Четвертый источник (уволненные сотрудники) считается наиболее распространенным в случаях кражи конфиденциальной информации. Аналитический центр компании «Infowatch» провел исследование, в ходе которого было выявлено, что более половины случаев незаконного копирования произошли из-за деструктивных действий уволенных сотрудников (рис. 1) [5].

Распределение деструктивных действий увольняющихся сотрудников в отношении корпоративной информации, 2017

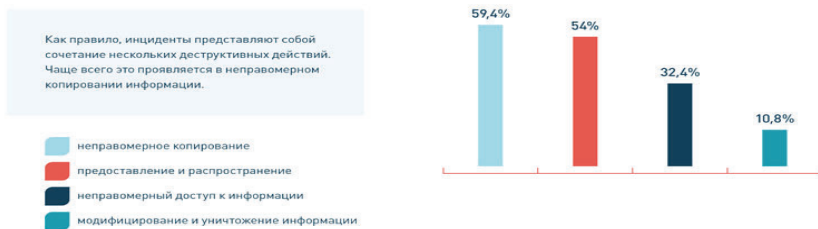


Рис. 1. Статистика деструктивных действий уволенных сотрудников.

Авторы проведенного исследования отмечают, что особая опасность сложившейся ситуации состоит в том, что у сотрудников достаточно широк спектр данных, они имеют доступ как к общей информации, так и к конфиденциальной, что повышает риски распространения данных. Цели совершения таких деяний различные, к ним может относиться: месть, работа на конкурентов, получение материальной выгоды.

Чаще всего распространяют персональные данные – это в 47,2 %, затем следует коммерческая тайна (36,1%), другая информация (13,9%) и государственная тайна (2,8%) (рис. 2)

Тип данных, скомпрометированных увольняющимися сотрудниками, 2017

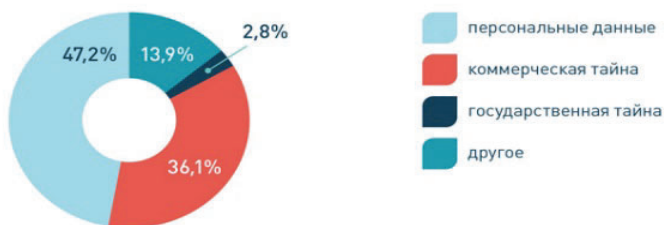


Рис. 2. Типы данных, которые подлежат распространению.

Также необходимо добавить, что в настоящее время чтобы осуществить взлом масштабных баз данных, необходимо иметь новейшие разработки в области информационных технологий для решения различных вопросов, связи с другими членами группы и осуществление контроля. Есть вариант, что такие кибератаки могут финансироваться и контролироваться другими государствами.

Помимо новейших разработок, члены преступных групп используют сайты, предлагая различные услуги. Обычно, ссылки на такие сайты находятся зашифрованными и находятся в Даркнете (от англ. Darknet «Теневая сеть» - сегмент Интернета, который скрыт из общего доступа), но можно найти и в общем доступе. Зачастую используют также онлайн-форумы, где лица пропагандируют свой род деятельности и вербуют новых участников.

На основе приведенной выше статистики можно сделать вывод о том, что России как развивающейся стране необходимо принимать какие-либо меры для обеспечения защиты личной конфиденциальной информации.

Во-первых, на наш взгляд, необходимо передать такой тип преступлений как кибертерроризм в ведомство ФСБ. Так как данный орган имеет более новейшие технологии для борьбы с киберпреступлениями и из-за отсутствия правосознания считается у людей более серьезным, чем МВД, благодаря чему число кибератак снизится, так как произойдет своего рода профилактика преступлений.

Во-вторых, кибертерроризм нужно признать самостоятельным преступлением, так как данное деяние не в полной мере охватывается составом преступления, предусмотренным статьей 272 Уголовного кодекса РФ, хотя с каждым годом число подобных правонарушений растет.

В-третьих, необходимо углублять грамотность в IT-сфере среди людей, потому что все сферы жизни общества постепенно перемещаются в глобальную сеть Интернет, а уровень компьютерной грамотности людей остался на том же уровне, что создает не только негативную ситуацию в сфере Интернет-мошенничества, но и нехватку кадров в сфере IT. Ведь чем больше людей будут

работать над защитой в сети, а затем следить за ней, тем больше будет вероятность, что хакер не сможет проникнуть в систему и украсть конфиденциальные данные.

В-четвертых, необходимо больше изучать, выявлять сайты с незаконными предложениями и товарами в сети Интернет и находить злоумышленников, а не просто блокировать их. Потому что в данном случае пользы от этого действия мало. Любое лицо может легко создать новый сайт и разместить всю ту же информацию, что была и раньше.

Таким образом, России необходима правовая ответственность за преступления такой направленности. Из-за достаточно высокого уровня развития техники террорист посредством подключенного к Интернету компьютера может нанести огромный вред как конкретному человеку, так и всему государству в целом. Данной проблемой уже вплотную занимается ООН, Совет Европы, Интерпол и для полного ее решения требуются усилия всего мирового сообщества.

Список литературы

1. Борьба с терроризмом в цифровую эпоху. 2018 URL: <https://forstrategy.org/ru/posts/20181106> (дата обращения: 05.12.2021).
2. Число киберпреступлений в России выросло в 11 раз за пять лет. 2020. URL: <https://tass.ru/obschestvo/10616343> (дата обращения: 05.12.2021).
3. Хакер заявил о взломе базы данных Российского визового центра в США. 2016. URL: <https://www.rbc.ru/society/27/12/2016/58619a1b9a7947c9018d157e> (дата обращения: 05.12.2021).
4. Неизвестному хакеру заплатят за взлом тестового онлайн-голосования. 2021. URL: <https://iz.ru/1210545/2021-08-21/neizvestnomu-khakeru-dadut-150-tys-rublei-za-vzлом-testovogo-onlain-golosovaniia> (дата обращения: 05.12.2021).

5. Каждый второй случай кражи корпоративной информации сотрудником при увольнении из организации связан с передачей этих данных конкурентам. 2018. URL: <https://www.infowatch.ru/company/presscenter/news/20590> (дата обращения: 05.12.2021).

Корниенко Л.Ю., ФПСПиС,
Барнаулский юридический
институт МВД России,
г. Барнаул

Научный руководитель: Моисеев С.В., к.и.н., доцент кафедры ТГиИП
БЮИ МВД России

Корниенко Л.Ю. ПУБЛИЧНОЕ ДЕМОНСТРИРОВАНИЕ НАЦИСТСКОЙ СИМВОЛИКИ В СЕТИ ИНТЕРНЕТ

В наше время остается актуальной проблема пропаганды или демонстрирования нацистской атрибутики или символики.

Согласно ФЗ от 25 июля 2002 г. №114-ФЗ «О противодействии экстремистской деятельности» экстремистская деятельность включает в себя пропаганду или демонстрирование нацистской атрибутики или символики, либо атрибутики или символики, сходной с нацистской атрибутикой или символикой до степени смешения.

В соответствии со ст.6 Федерального закона от 19 мая 1995г. №80-ФЗ «Об увековечении Победы советского народа в Великой Отечественной войне 1941 - 1945 годов» в Российской Федерации запрещается использование в любом виде нацистской символики и атрибутики.

Под нацистской символикой понимается символика, которая использовалась национал-социалистической немецкой рабочей партией [2]. К такой символике относят свастику, знамена, атрибуты униформы, приветствия и пароли. Профессор МГУ О.Н. Садилов определяет перечень наименований, относящихся к нацистской символике, а именно, эмблема НСДАП, знамя и сопутствующая символика (френчи, фуражки, нарукавные знаки, пряжки); эмблемы штурмовых отрядов, военизированных подразделений НСДАП; символика фашистской организации бывших ветеранов национальной войны-

«Союз ветеранов», Национальной фашистской партии Италии, Фашистской республиканской партии Италии; символика СС; символика гестапо.

Демонстрирование нацистской символики осуществляется как в реальной жизни, так и в сети Интернет посредством публикации фотографий, содержащих изображения вышеуказанной символики.

Так, к примеру, в 2018 году гражданин разместил на сайте "Avito.ru" объявление о продаже военного знака Третьего Рейха "За ранение", содержащего нацистскую символику. Затем этот значок был предъявлен к продаже конкретному лицу.

В 2021 году пользователем сети Интернет в социальной сети «ВКонтакте» были размещены фотографии, содержащие нацистскую атрибутику и символику.

К сожалению, данные примеры не являются исчерпывающими.

Самым распространенным нацистским символом, который публично демонстрируют в сети Интернет, является свастика. Свастика – санскритское наименование символического знака, изображающего крест.

В соответствии со ст. 20.3 КоАП РФ за демонстрацию нацистских символов и символики экстремистских организаций предусмотрено административное наказание в виде штрафа [1], также в соответствии с подписанным В.В. Путиным ФЗ от 01.03.2020 года №31-ФЗ «О внесении изменения в ст.20.3 КоАП РФ» положения ст.20.3 КоАП РФ не распространяются на случаи использования указанной в ст.20.3 КоАП РФ атрибутики или символики, с помощью которой формируется негативное отношение к идеологии экстремизма и нацизма, а также присутствуют признаки пропаганды нацизма или экстремизма.

Подводя итог, можно сделать вывод о том, что для решения данных проблем необходимо предпринять следующие меры:

1. Разработать и утвердить перечень запрещенных символов, в том числе символы нацистской свастики и символики, связанные с нацистской атрибутикой или символикой либо атрибутикой или символикой, сходной с

нацистской атрибутикой или символикой до степени смешения, утвержденный Минюстом России;

2. Проанализировать и обобщить опыт судебной практики в области публичной демонстрации нацистской атрибутики и символики в сети Интернет с запрещенной символикой, в том числе нацистской;

3. Обратить должное внимание на профилактическую работу с молодежью, с целью минимизировать количество совершенных административных правонарушений, касающихся публичной демонстрации нацистской атрибутики и символики в сети Интернет.

Список литературы

1. Кодекс Российской Федерации об административных правонарушениях (КоАП РФ) от 30.12.2001 №195-ФЗ. URL: http://www.consultant.ru/document/cons_doc_LAW_34661/ (Дата обращения: 09.12.2021);

2. Похлёбкин В.В. Словарь международной символики и эмблематики. М.: ЗАО Центрполиграф, 2018. – 354-356, 543 с.

Богданов И.С.,
Алтайский филиал
РАНХиГС,
г. Барнаул

Научный руководитель: Цой Л.В., старший преподаватель кафедры
уголовного права, уголовного процесса и криминалистики,
Алтайский филиал РАНХиГС, г. Барнаул

Богданов И.С. «ФЕНОМЕН ДИПФЕЙКА»: УГРОЗА НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

Технология «Deepfake» (Дипфейк) — это методика синтеза изображения, основанная на искусственном интеллекте (ИИ). В наши дни, она используется пользователями преимущественно в сфере развлечений. Поскольку изначально не позволяла создать качественной копии лица, голоса или тела человека, и соответственно, быть использованной в преступном умысле.

Использование технологии Дипфейк для манипуляций людьми и ведения их в заблуждение, несмотря на подавляющее большинство использований в сфере развлечений, является быстро развивающейся угрозой, которая может реализоваться в ближайшем будущем.

Компания CyberCube — международная аналитическая компания по страхованию от киберпреступлений — подчеркнула в своём отчёте «Социальная инженерия: размытие реальности и фальшивка» (2020 год), что «способность создавать реалистичные аудио- и видео-фейки с помощью ИИ (искусственного интеллекта) и машинного обучения неуклонно растёт». Хотя сегодняшняя технология дипфейков пока не совсем соответствует подлинным видеоматериалам—присмотревшись внимательнее, обычно можно сказать, что видео не является настоящим, однако, технология быстро совершенствуется[1].

В исследовании, опубликованном в журнале Crime Science и финансируемом Dawes Center for Future Crime at UCL, определены 20 способов

использования ИИ для содействия преступности в течение следующих 15 лет. Они были ранжированы по масштабам рисков — в зависимости от вреда, который они могут причинить, потенциальной преступной выгоды и от того, насколько легко их будет выполнить и насколько сложно будет их остановить.

Обеспокоенности добавляет отсутствие международного регулирования технологии. И если в развитых странах, которые сумели сформулировать основные принципы нормативного регулирования для технологий ИИ и робототехники об этом начинают говорить, то тяжело представить в какую катастрофу это может перейти в странах, не определившихся даже с понятием ИИ. Например, в России правовое регулирование ИИ появилось в рамках нацпрограммы "Цифровая экономика", а сейчас запущены экспериментальные правовые режимы - "цифровые песочницы" - которые позволят гибко подходить к регулированию деятельности в данных сферах, в том числе временно отменять действующие предписания или запреты, если это понадобится для нормального функционирования экспериментального режима. В Москве подобный экспериментальный режим запущен с 1 июля 2021 года. Что позволяет оптимистично смотреть на будущую оценку законодателем конкретных технологий, основанных на ИИ, несмотря на отсутствие отечественного определения технологии «Дипфейк»[2].

Наиболее четко определение дипфейка, содержится в отчете Европейского парламента: «Дипфейки определяются, как искусственные видео- и звукокомедиа контент, который кажется аутентичным и создает «живого персонажа», однако эти образы не настоящие, основанные на методах ИИ, в частности, машинного и глубокого обучения»[3].

Использование технологии «Дипфейк» становится доступней, активно коммерциализируется и монетизируется. Основа ИИ – самообучаемый механизм: повсеместное использование дает возможность для анализа и улучшения. Американский исследователь Дуглас Харрис убежден, что скоро потребуется несколько секунд и продукт будет неотличим от оригинала[4].

В перспективе, это создает огромную угрозу, поскольку технологию могут использовать террористические организации. Таким образом, в нынешней парадигме, единственным ограничением для таких организаций, станет их собственное воображение. Мы, конечно, считаем это не допустимо! Но как возможно обезопасить мир от угрозы использования технологии «Дипфейк» против главных лиц государства, не потерять доверие к использованию видео- и аудиосвязи?

В научной среде существует несколько подходов и способов разрешения проблемы неконтролируемого использования технологии «Дипфейк»:

1) Запрет на использование изображений политических лидеров государств и введение уголовной ответственности за распространение дипфейков[5].

Нам кажется такой подход к решению террористической угрозы нереальным в своём воплощении. Уголовное преследование вряд ли сможет напугать террористов и может, наоборот, запутать население. Поскольку прямой запрет со стороны государства может привести к тотальному доверию среди населения к любым видео- и аудиоматериалам с использованием политической элиты и еще сильнее запутать население.

2) Добавлением «спам-фильтра», блокирующего контент с «злонамеренным использованием» технологии «Дипфейк»[6].

Однако специалисты в области кибербезопасности и коммерции не видят способов для реализации такой идеи. Поскольку технология используется в большинстве случаев для развлекательных целей, представляется невозможным создание алгоритма отличающего «злонамеренное» и «добросовестное» использование.

3) Разработка технологий обнаружения подделок[7].

Такой способ, видится, самым разумным. Поскольку в самой основе технологии - борьба между механизмом «создающим подделку» и «находящим подделку». В этом смысле считаем, возможным обязать компании, улучшающие технологию, предоставлять доступ к механизмам «обнаружения

подделки». Это прекрасно вяжется с политикой «ответственного внедрения новых технологий» продиктованной наиболее крупными IT компаниями. Так, например, компания Microsoft уже разработала программу для обнаружения «Дипфейк» в партнерстве с другими компаниями, специализирующимися на обеспечении информационной безопасности[8]. В связи с этим, главной проблемой видится доступность механизмов «обнаружения подделок». Что решается введением на международном уровне политики «ответственного внедрения новых технологий» перед IT-компаниями и обязыванием публиковать механизмы по «обнаружению подделок».

Исходя из вышеперечисленного, можно сделать вывод о том, что потенциальную проблему «злонамеренного» использования технологии Дипфейк террористическими организациями для создания возможных беспорядков необходимо предотвращать при помощи альтернативных технологий для обнаружений подделок. Альтернативные меры, которые могли бы иметь значение при использовании технологии для травли, шантажа и мошенничества не применимы по отношению к международным преступным организациям. Поскольку мы говорим о совершенно разном уровне преступности. Считаем необходимым, отметим, важность сотрудничества в сфере информационной безопасности, поскольку в обратном случае возможен ровно противоположный результат.

Список литературы

1. Designing a Cyber Catastrophe // Cybcube.com: [сайт] . – 2020. — URL: <https://insights.cybcube.com/en/designing-a-cyber-catastrophe-qa> (дата обращения: 5.12.2021).
2. Алпатова, И. Утверждена концепция правового регулирования искусственного интеллекта / И. Алпатова // Российская Газета. – 2020. – 24 Август.

3. Цветков, Ю. Технологию дипфейка можно использовать для травли, шантажа, мошенничества / А. Шафран // Вести ФМ «Стратегия» [сайт]. URL: <https://radiovesti.ru/brand/63899/episode/1361071> (дата обращения: 5.12.2021).

4. Гасанова, Р. Б. Идентификационное значение голосовых сообщений при расследовании преступлений / Р. Б. Гасанова // Закон и власть. – 2021. – №2. – С. 43–46.

5. Киселёв, А. С. О необходимости правового регулирования в сфере искусственного интеллекта: дипфейк как угроза национальной безопасности / А. С. Киселёв // Вестник Московского государственного областного университета. – 2021. – №3. – С. 54–65.

6. The World Needs Deepfake Experts to Stem This Chaos / S. Gregory, T. Simonite // Wired.com: [сайт]. – 2021. — URL: <https://www.wired.com/story/opinion-the-world-needs-deepfake-experts-to-stem-this-chaos/> (дата обращения: 5.12.2021).

7. Matthew G., Epstein Z., Picard R. W. Detect DeepFakes: How to counteract misinformation created by AI / G. Matthew, Z. Epstein, R. W. Picard // Media.mit.edu: [сайт]. URL: <https://www.media.mit.edu/projects/detect-fakes/overview/> (дата обращения: 5.12.2021).

8. Burt T. New Steps to Combat Disinformation / T. Burt // Blogs.microsoft.com: [сайт]. URL: <https://blogs.microsoft.com/on-the-issues/2020/09/01/disinformation-deepfakes-newsguard-video-authenticator/> (дата обращения: 5.12.2021).

Гоберник Д.В.

Барнаульский юридический

институт МВД России,

г. Барнаул

Научный руководитель: Моисеев С.В., к.и.н., доцент кафедры ТГиИП

БЮИ МВД России

**Гоберник Д.В. КИБЕРЭКСТРЕМИЗМ В ДЕЯТЕЛЬНОСТИ
МОЛОДЕЖНЫХ СУБКУЛЬТУР ДИСКРИМИНАЦИОННОЙ
НАПРАВЛЕННОСТИ**

Необходимость рассмотрения данной темы не утрачивает свою актуальность в настоящее время. Периодические локальные конфликты и войны, происходившие в новейший период истории, стимулировали развитие многих деструктивных движений и субкультур радикальной направленности. Актуальность данного исследования складывалась долгие годы борьбы, одних национальностей с другими, так же развитие высоких технологий и сопутствующая этому глобализация общества, поспособствовала развитию проблематики. Появление сети Интернет стало источником проявления экстремизма в новых формах. Раскрытие темы происходит с помощью раскрытия таких проблемных понятий как: национализма, национал-социализм, изнутри. На наш взгляд необходимо рассматривать содержание этих проявлений через анализ агрессивных молодежных субкультур: Скинхеды, Националисты, Около футболисты. Все эти течения объединяют схожие идеи превосходства одной расы над другими, неоправданная ксенофобия и др.

Экстремизм-идеология крайних взглядов и методов действия, затрагивающая честь достоинство а так же безопасность граждан и государства. Экстремизм это основа и идеология терроризма. Зачастую экстремистские проявления курируются из-за рубежа. Это является серьёзной внутренней проблемой нашего государства, которая требует своего решения.

Сложные экономическое, социальное и политическое положение Российской Федерации развал системы образования и воспитания, безработица и кризис 90-х гг. способствовали адаптации зарубежных субкультур в отечественной молодежной среде. Свой образ жизни, внешний стиль, «духовные» приоритеты представители российские субкультур берут из зарубежья, добавляют часть своего и комбинируют получившееся. При этом, как не странно, идеи, жесты, атрибуты символики наши копируют у нацистов Адольфа Гитлера.

С развитием социальных сетей растёт популяция экстремистских группировок. Экстремизм использует самые простые каналы распространения своей идеологии среди молодёжи, что позволяет втягивать в ряды экстремистов сотни, а даже тысячи граждан. Конечно, чаще всего жертвами экстремистских вербаторов становятся несовершеннолетние граждане. Это обуславливается несформированной жизненной позицией. С помощью соцсетей человек раскрывается с той стороны которой, возможно, он боится раскрыться в реальной жизни и часто этим пользуются лидеры экстремистских группировок, нередко имеющие психологическое образование, и незаурядную лидерскую харизму.

Буллинг и кибербуллинг способствует вступлению граждан в экстремистские группировки. Примеров, где издевательства а затем молчание со стороны окружающих, стоило жизни десятков людей, очень много. Уже по праву, такое движение как скулшутинг, можно считать экстремистским. Пермь, Казань, Керчь и другие города нашей страны показали, что может перерасти из простых оскорблений в школе, интернете и семье, в ужаснейшее событие. У людей, совершающих такие ужасные преступления, возникает потребность в наказании своих обидчиков. Определенно, участники данных проявлений имеют признаки всего, чтобы смело заявить, что в России есть культ массовых убийств, а самое страшное, что помимо порицания среди адекватных граждан идёт процесс героизации стрелков в учебных заведениях. Их пытаются всячески оправдать, собираются огромные суммы денег на дорогостоящих

адвокатов. К сожалению, такие люди придерживаются принципа «МОЯ ХАТА С КРАЮ», что показывает их безразличие к сотням жертв этих стрелков, ведь они не встречались с этой проблемой лицом к лицу. Абсурд в том, что почти все стрелки не скрывали своих намерений, публикуя свою позицию в социальной сети, пассивная гражданская позиция, отчасти привела к тому, что мы видим в итоге.

Сложные экономическое, социальное и политическое положение Российской Федерации развал системы образования и воспитания, безработица и кризис 90-х гг. способствовали адаптации зарубежных субкультур в отечественной молодежной среде. Свой образ жизни, внешний стиль, «духовные» приоритеты представители российские субкультур берут из зарубежья, добавляют часть своего и комбинируют получившееся. При этом, как не странно, идеи, жесты, атрибуты символики наши копируют у нацистов Адольфа Гитлера. Непокойная обстановка в стране усугубило общественные волнения на национальной почве. Развитие всемирной сети упростило работу агитаторов группировок

Первая и вторая чеченские компании, многочисленные теракты, организованные боевиками неславянской национальности, захваты школ, театров, больниц, подрывы зданий террористами оставили отпечаток в сознании и мировоззрении граждан. Вспышка и наиболее агрессивное проявление данных субкультур происходит именно в это время.

Свой образ жизни, стиль одежды, вероисповедание российские субкультуры берут из зарубежья, но добавляют много своего, и успешно комбинируют это. Как не странно, многие идеи, жесты, и символики российские представители субкультур берут у национал-социалистической партии Адольфа Гитлера, несмотря на трагическую историю 2 мировой войны.

Статистика показывает, что преступления и правонарушения экстремистской направленности с использованием сети интернет показывают определенную динамику. Так, за 2021 год на территории Алтайского края было выявлено 61 правонарушение экстремистской направленности по ст. 20.29.

Производство и распространение экстремистских материалов было составлено 25 протоколов; по ст. 20.3.2. Публичные призывы к осуществлению действий, направленных на нарушение территориальной целостности Российской Федерации был выписан 1 протокол ;по ст. 20.3.1. Возбуждение ненависти либо вражды, а равно унижение человеческого достоинства было выписано 16 протоколов по ст. 20.3. Пропаганда либо публичное демонстрирование нацистской атрибутики или символики, либо атрибутики или символики экстремистских организаций, либо иных атрибутики или символики, пропаганда либо публичное демонстрирование которых запрещены федеральными законами было выписано 19 протоколов

Национализм часто используется людьми в политической сфере. Он наиболее результативен тогда, когда страна нуждается в культурном и социально-политическом единстве всего населения или отдельных групп. История показывает, что данное явление используется с целью утвердить не только факт наличия нации и ее отдельных интересов, но и превосходство этой нации и ее потребностей над остальными. Высшая оценка национальных приоритетов часто сливается с идеями независимости, что в итоге ведет к необходимости обретения части государственного суверенитета и его политической фиксации. Формируется представление нации об автономии в рамках государства, а также потребность в создании чего-то собственного.

Не стоит упускать такую субкультуру, как скинхеды. Самыми популярными среди скинхедов являются русский национализм и национал-социализм. Приверженцы данных идеологий имеют праворадикальных ,часто идущие в разрез с законом, взгляды . Часто маскируют националистические и нацистские выражения под цифрами .число 18 означает «Адольф Гитлер» а число 88 «хай Гитлер»

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. Через Интернет может быть организовано экстремистское сообщество, например путем сговора и приискания соучастников.

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 [8]. 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.

Проблема радикального экстремизма – это не только мат, файеры и драки фанатов после матчей. Это деструктивное социальное явление, прочно пустившее корни в российскую действительность

В современной реальности место околофутбола является ключевым у молодёжи в возрасте от 15 до 25 лет .

Название околофутбол(околофутболисты)говорит само за себя.Фанаты имеют мало отношения к футболу они около него,на стадионе ,за ним,на опушке леса.

Футбол давно перестал быть просто игрой на поле ,часто футбольные баталии выходят за рамки спортивных площадок всего мира . Футбольные фанаты с каждым годом выходят на более высокой уровень своей организации ,подготовленности , финансового обеспечения и т.д. Всемирная паутина активно способствует численности футбольных фанатов , мнимо романтизируя их деятельность .

Только в Москве существует несколько десятков фанатских группировок- "фирм", к деятельности каждой из которых применим целый набор статей УК. А сам процесс вовлечения подростков в фанатские ряды поставлен на поток. Отслеживанием и последующим промыванием мозгов юным фанатам занимаются циничные рекрутеры, зачастую имеющие психологическое образование и нередко обладающие незаурядной лидерской харизмой. Через определённое время 15-летние дети превращаются в полноценных зомби. Жестоких правонарушителей, у которых в головах нет ни одной мысли — только инстинкты. Ударить. Добить упавшего. Похвастаться подвигами перед друзьями.

Россия многонациональная страна, с населением более 146 миллионов человек и более 200 национальностей, тесно взаимодействующих на одной территории.

Проявление агрессии между представителями разных национальностей просто недопустимо в нашем интернациональном государстве. Лидеры данных группировок проводят качественную пропагандистскую работу, с помощью социальных сетей, в отношении несовершеннолетних граждан. Это является серьёзной проблемой для современного российского общества требующей разрешения. Деятельность таких организаций наносит вред обществу, и гражданам в частности. Исхода из данной деятельности всего 2, либо участники будут привлечены к уголовной ответственности и проведут значительную часть жизни в заключении, либо им нанесут серьёзные травмы в процессе очередной потасовки, которые встречаются очень часто у различных субкультур. Я часто вспоминаю фразу из повести Анатолия Приставкина “Ночевала тучка золотая”: “Нет плохих народов, есть плохие люди”.

Отсутствие желания у заинтересованных структур заниматься решением вопросов связанных с нейтрализацией воздействия радикальных субкультур на молодежь только ухудшает ситуацию и провоцирует развитие негативных последствий.

Список литературы

1. <https://minjust.gov.ru/ru/documents/7822/>

2. Тарасов А. Н. Субкультура футбольных фанатов в России и правый радикализм (на Сен-Жюсте, в «Скепсисе») // Русский национализм между властью и оппозицией. Сборник статей. — М.: Центр «Панорама», 2010. — ISBN 978-5-94420-039-6

Захарова А.П.

аспирант кафедры уголовного права и криминологии
Алтайского государственного университета, помощник судьи
Алтайского краевого суда, г. Барнаул

**Захарова А.П. ОСОБЕННОСТИ ПРОФИЛАКТИКИ
ПРЕСТУПЛЕНИЙ ЭКСТРЕМИСТСКОЙ НАПРАВЛЕННОСТИ В
МОЛОДЕЖНОЙ СРЕДЕ**

Проявления молодежного экстремизма все чаще встречаются в нашей стране и на фоне социальной неустроенности находят благодатную почву, привлекая в свои ряды все новых участников. Противостоять этой угрозе можно, лишь используя современные формы и методы при организации оперативно-профилактических мероприятий, а также современные технологии. По сравнению со взрослым, молодежный экстремизм имеет некоторые существенные отличия. В основном он является производным от взрослого и поэтому менее организован, стихичен, за редким исключением, неглубок идеологически.

Основными тенденциями современного молодежного экстремизма являются возрастающая организованность, сплоченность группировок, формирование в них идеологических, аналитических и боевых структур, усиление мер конспирации, применение для распространения своей идеологии и координации действий новейших информационных технологий.

Во многих регионах Российской Федерации наметилась тенденция использования различными оппозиционными силами молодёжных право- и леворадикальных экстремистских организаций, спортивных, в т.ч. на финансовой основе. Для увеличения численности своих сторонников лидеры и активисты радикальных политизированных структур также ведут вербовочную работу в высших учебных заведениях.

Развитие молодёжного экстремизма представляет особую опасность, потому что связано с недостаточной социальной адаптацией и развитием асоциальных установок в групповом сознании молодого поколения, что влияет на ценности, предпочтительные образцы поведения, оценки социального взаимодействия, то есть в широком смысле связано с социальной и политической культурой российского общества.

В настоящее время задача предупреждения данных преступлений выходит на первый план в деятельности органов государственной власти и местного самоуправления, правоохранительных органов. Наличие данной задачи требует того, чтобы понятие этого вида правоохранительной деятельности было разъяснено законодательно. Однако основная проблема заключается в том, что до настоящего времени ни один нормативный акт не определил единых подходов к содержанию и организации предупреждения преступлений экстремистской и террористической направленности. Отсутствует единый правовой акт, который бы полно определил понятийный аппарат, задачи и принципы превентивной деятельности для ее субъектов, их компетенцию. Также законодательно не определено, что представляют собой политический, национальный, религиозный или молодежный экстремизм.

Современное состояние деятельности подразделений ОВД по предупреждению преступлений экстремистской направленности в молодежной среде не в полной мере отвечает предъявляемым требованиям. Несмотря на наличие определенного положительного опыта в решении вопросов профилактики и предупреждения данных преступлений, необходимо дополнительно исследовать указанную деятельность подразделений ОВД [1]. Международный опыт показывает, что только запретительными мерами разрешить проблему экстремизма и в дальнейшем проявлений терроризма невозможно, необходимо вести работу во всех сферах общества, принять меры, направленные на оздоровление социально-политической и экономической обстановки в стране. Следует отметить, что Федеральный закон «О противодействии экстремистской деятельности» закрепил положение о том, что

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. Согласно положениям Федерального закона «Об общих принципах организации местного самоуправления в Российской Федерации», участие в профилактике терроризма и экстремизма, а также в минимизации и (или) ликвидации последствий проявлений терроризма и экстремизма относится к вопросам местного значения [2].

Отметим также, что профилактика экстремизма в молодежной среде обуславливает необходимость продуманной социальной и молодежной политики на длительную перспективу, создания предпосылок для разумной альтернативы, при наличии которой потенциальные экстремисты смогли бы реализовать себя в иных не связанных с совершением преступлений сферах деятельности.

Можно выделить основные направления профилактики экстремизма в молодежной среде:

- 1) достижение необходимого уровня правовой культуры, прежде всего в образовательных организациях;
- 2) организация воспитательной работы среди детей и молодежи, направленная на устранение причин и условий, способствующих совершению действий экстремистского характера и в последующем преступлений террористической направленности;
- 3) формирование межэтнической культуры, в том числе в молодежной среде;
- 4) общественное осуждение и пресечение любых проявлений дискриминации, насилия, расизма, а также агрессивного поведения;
- 5) информирование молодежи о вопросах противодействия терроризму и экстремизму в целях содействия правоохранным органам в

выявлении правонарушений и преступлений данной категории, а также ликвидации их последствий.

Во многих субъектах Российской Федерации уже выстроена многоуровневая система совещательно-консультативных органов, деятельность которых позволяет своевременно реагировать на возникающие ситуации, связанные с предупреждением экстремизма и терроризма. На краевых, областных уровнях были созданы советы при губернаторах по вопросам межэтнических отношений, имеют место молодежные парламенты. Комитеты по делам молодежи проводят мероприятия, направленные на выявление лиц, имеющих экстремистские настроения и распространяющие в сети Интернет экстремистские идеи. Активно привлекаются волонтеры из молодежной среды, имеющие навыки работы с информационными ресурсами, организовано взаимодействие с различными учебными заведениями [3].

Следует отметить положительный опыт работы в проведении массовых молодежных мероприятий всероссийского и регионального масштабов. Это, так называемые, площадки, на которых общими усилиями органов государственной власти, институтов гражданского общества ведется работа по формированию, в первую очередь среди молодежи, общероссийской гражданской идентичности. Наиболее известные из них: форум организованный Федеральным агентством по делам молодёжи «Территория смыслов», молодёжный форум «Арктика», молодёжные форумы «Выбор молодежи - Интернет без терроризма» и другие.

Одним из средств привлечения молодежи к экстремистской и террористической деятельности является вовлечение в совершение подобного рода преступлений. Вовлечение в совершение преступлений террористического характера может выражаться в любых действиях, направленных на возникновение умысла на совершение преступления. Такими действиями могут быть угрозы, обещания, обман, физическое воздействие и др. Склонение лиц к участию в деятельности террористической организации означает совершение умышленных действий, направленных на возбуждение желания участвовать в

деятельности террористической организации. Законом не дается перечень таких действий, и поэтому они могут быть любыми (советы, уговоры, обещания и т. п.). Но для наличия состава преступления, предусмотренного ст. 205.1 Уголовного кодекса Российской Федерации, важно то, что осуществляется склонение к участию в деятельности именно террористической организации. Это обстоятельство должно охватываться и умыслом виновного, и сознанием склоняемого к участию в такой организации. Вооружение лица в целях совершения преступлений террористического характера заключается в снабжении его оружием или боеприпасами и будет оконченным с момента их получения указанным лицом. Обучение этих лиц в тех же целях состоит в организации и проведении с ними занятий по физической и психологической подготовке к осуществлению преступлений террористического характера, в обучении обращению с оружием, взрывчатыми, отравляющими веществами, тактике совершения преступлений и иным дисциплинам, необходимым для обеспечения эффективных действий [4].

Тяга к сообществам экстремистского толка объясняется отчасти особенностями молодежного возраста. При определенных внешних раздражителях такие особенности становятся фактором вовлечения молодых людей в совершение преступлений террористической и экстремистской направленности. Криминологическая значимость ценностных ориентаций, как отмечают ученые, «заключается в том, что они помогают понять, почему при наличии правильно или неправильно сформированных нравственных и правовых взглядов молодые люди в одних ситуациях ведут себя правомерно, а в других – преступно», почему в некоторых ситуациях подавляются даже твердо сформированные положительные взгляды и убеждения и проявляются экстремистские, а в других же случаях – все происходит наоборот.

Таким образом, несмотря на принимаемые меры по борьбе с преступностью, предупреждение преступлений экстремистского характера в молодежной среде продолжает оставаться одной из самых актуальных проблем современности. Для преодоления этого негативного явления необходимо вести

работу во всех сферах общества, в приоритетном порядке осуществлять профилактические, в том числе воспитательные, пропагандистские, меры, направленные на предупреждение экстремистской и террористической деятельности [5].

Изживание указанных негативных явлений - длительный процесс, предполагающий создание необходимых условий для достижения такой цели. Важно убедить общество, политические силы в том, что спекуляция на объективных трудностях и противоречиях, силовой вариант их решения — это путь, ведущий к катастрофе. Очевидно, для того чтобы удержать молодых людей от терроризма и экстремизма, государство должно выдвинуть им встречное, более привлекательное предложение. В настоящий момент, к сожалению, не создается механизм самореализации для подрастающего поколения. В России наблюдается отсутствие перспектив и дальнейшего развития для молодежи, и это говорит о том, что завтра молодежь будет еще больше обременена, еще более стеснена материально и деморализована [6].

Профилактика экстремизма и терроризма представляется первоочередной задачей, поскольку государству важно добиваться устранения причин, продуцирующих различного рода противоречия и конфликты. Закрепляя права и свободы граждан, суверенитет, территориальную целостность, достойное качество и уровень жизни в качестве основ конституционного строя, Конституция РФ гарантирует их незыблемость, стабильность и необходимость защиты.

Учитывая изложенное, необходимым становится совершенствование молодежной политики государства и проведения реформ в области образования. Это может быть выражено в изменении учебного плана, поощрении инициативности учащихся, пропаганде возможности психологической поддержки, а также повышении уровня социальной ответственности школьников и студентов.

Список литературы

1. Родионов А.В. Противодействие проявлениям молодежного экстремизма // Современные проблемы молодежного экстремизма в Российской Федерации: состояние и тенденции: Материалы круглого стола – М.: ВНИИ МВД России, 2016. [Электронный ресурс] – Заглавие с экрана. URL: <http://cyberleninka.ru/>

2. Федеральный закон от 25.07.2002 N 114-ФЗ (ред. от 25.12.2012) "О противодействии экстремистской деятельности" // [Электронный ресурс] - Заглавие с экрана. URL: <http://base.consultant.ru/>

3. Бучаев, С.М. Социально-биологическая и нравственно-воспитательная характеристика личности преступника-террориста // Пробелы в российском законодательстве . 2016. №6. [Электронный ресурс] – Заглавие с экрана. URL: <http://cyberleninka.ru/>

4. Вишневецкий, К.В. Место виктимологической теории в криминологии // Теория и практика общественного развития. 2011. №5. [Электронный ресурс] – Заглавие с экрана. URL: <http://cyberleninka.ru/>

5. Сукиасян, С. Г. Терроризм: иллюзии и реальность / С. Г. Сукиасян // Психология и психотехника. — 2010. — № 5 (20). — С. 60.

6. Сафронов, А.А., Калужный, К.Ю. Терроризм и экстремизм — современная реальность в контексте вероисповедания // Психопедагогика в правоохранительных органах . 2014. №4 (59) С. 39.

Валова Ю.А., юридический факультет,
Алтайский филиал
РАНХиГС,
г. Барнаул

Научный руководитель: Цой Л. В., старший преподаватель кафедры
уголовного права, уголовного процесса и криминалистики Алтайского филиала
РАНХиГС

Валова Ю.А. РОСТ КИБЕРТЕРРОРИЗМА В СВЯЗИ С ПЕРЕХОДОМ В ДИСТАНЦИОННЫЙ ФОРМАТ

В марте 2020 года эпидемия коронавируса получила официальный статус пандемии в связи с тем, что за короткий срок данный феномен охватил более 100 стран. Кроме очевидных проблем, с которыми столкнулись государства, и Российская Федерация в частности, таких как удар по здоровью людей, сокращение населения, локдаун, проблемы с экономикой, пандемия также повлекла за собой резкий рост киберпреступлений. В связи с тем, что на территории России был введен длительный дистанционный формат обучения и рабочих процессов, почти каждый третий гражданин стал проводить за компьютером гораздо больше времени. Всё это привело к значительному ухудшению кибербезопасности.

Как отмечает в своем докладе «Состояние преступности в России» управление правовой статистики и информационных технологий Генеральной прокуратуры, в 2020 году рост киберпреступности вырос в 11 раз за последние 5 лет [1]. Несмотря на то, что по статистике МВД самым частым киберпреступлением стало – мошенничество, кибертерроризм встречался не менее часто.

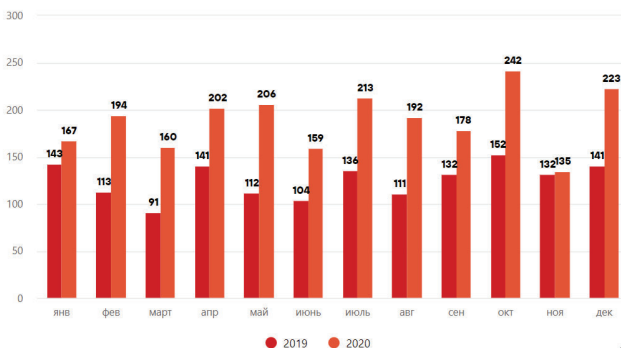


Рис. 1. Количество киберпреступлений в России в 2019 и 2020 годах

Так, директор Департамента международной информационной безопасности МИД России Андрей Крутских в рамках онлайн-дискуссии клуба "Валдай" обозначил, что сейчас актуальны сразу две пандемии. Одна - это биопандемия, связанная с распространением коронавируса и ухудшением здоровья граждан. Параллельно с ней углубляется и другая глобальная проблема, которую он обозначил как киберпандемия. То есть возможность втягивания человечества в киберконфронтацию и даже кибервойну. Он пояснил, что проявлениями киберпандемии являются хакерство, кибертерроризм, кибервмешательство в частную жизнь и развитие государств. И это все - следствие развития негативных тенденций при совершенствовании кибертехнологий [2].

Само понятие террористического акта дается в Уголовном кодексе, а именно в ч. 1 ст. 205, согласно которой, террористическим актом признается совершение взрыва, поджога или иных действий, устрашающих население и создающих опасность гибели человека, причинения значительного имущественного ущерба либо наступления иных тяжких последствий, в целях дестабилизации деятельности органов власти или международных организаций либо воздействия на принятие ими решений, а также угроза совершения указанных действий в целях воздействия на принятие решений органами власти или международными организациями.

Исходя из закрепленного на законодательном уровне понятия террористического акта, стоит отметить, что кодифицированного термина кибертерроризма до сих пор не принято. Несмотря на то, что термин используется СМИ и правоохранительными органами довольно часто, он до сих пор не регламентирован ни в Уголовном кодексе, ни в Федеральном законе «О противодействии терроризму», ни в Постановлении Пленума Верховного суда РФ «О некоторых вопросах судебной практики по уголовным делам о преступлениях террористической направленности», ни в Постановлении Пленума Верховного суда РФ «О некоторых вопросах судебной практики по уголовным делам и о преступлениях компьютерной направленности». В наиболее широком смысле принято понимать, что кибертерроризм – это преступление, совершенное в компьютерной среде с использованием дистанционных технологий [3]. Иначе под данным видом компьютерного преступления принято понимать комплекс незаконных телекоммуникационных и компьютерных действий, порожденных самим обществом на определенном этапе его развития.

Опираясь на всё вышесказанное, можно обозначить, что кибертерроризм представляет собой совокупность действий, которые по своей природе реализуются в веб-среде, несут террористический характер и угрозу безопасности как отдельно взятой личности, так и общества или государства в целом, непосредственно связанных с изменением имеющейся информации с целью получения преимущества при решении социальных, экономических или политических задач.

Так, важно указать, что пандемия коронавируса помогла определить ещё один объект атак террористов и то, что такие атаки носят крайне негативный характер. На примере Российской Федерации, можно обозначить, что целью кибератак является выведение различными способами и методами из строя информационной структуры государства, последствия которой являются опасными для нормального функционирования и деятельности государства. В связи с тем, что Россия имеет в своем распоряжении высокие технологии в

области спутниковой связи и глобальных сетей, она оказалась в числе тех стран, в которых на фоне перехода в дистанционный формат, увеличилось количество кибертерактов[4].

Эффективность форм и методов кибертерроризма зависит от гибкости информационной инфраструктуры, умения отражать атаки и степени ее защищенности. На практике совершения подобных преступлений важно выделить несколько видов воздействия, а также, различные приемы кибертерроризма. Традиционно к ним относятся:

1. Захват каналов средств массовой информации, с целью дезинформации населения, а также, для демонстрации мощи террористических группировок и сообществ;

2. Кража или уничтожение информационного, программного и технического ресурсов, которые имеют общественную значимость, совершенные путем преодоления систем защиты или внедрения вирусов;

3. В ходе своей преступной деятельности раскрытие и угроза опубликования или опубликование закрытой информации о функционировании информационной инфраструктуры государства, общественно значимых и военных информационных систем, кодах шифрования, принципах работы систем шифрования, успешном опыте ведения информационного терроризма и многое другое;

4. Воздействие на базы данных государственных органов, с целью получения, модификации или искажения особо важной для страны информации.

Деятельность террористов в сети обычно делится на три основные группы, такие как: кибертерроризм, активность и хакерство.

Хакерство предполагает преступные атаки в сети Интернет, а именно, незаконное проникновение в засекреченные базы данных или веб-сайты с целью извлечения выгоды или данных, или хищения ценной для государства или общества информации.

Активность подразумевает простое использование интернет пространства, где кибертеррористы объединяются в организованные сообщества, а также, данная площадка зачастую используется для рекрутирования новых членов в террористические объединения и группировки.

Под кибертерроризмом, несмотря на то, что он схож с хакерством, всё-таки стоит понимать отдельный вид интернет-атак. Чаще всего, его главной целью является нанесение крупного ущерба важным объектам инфраструктуры с помощью использования информационных технологий.

Для России, в свою очередь, актуальны все три способа преступной Интернет-деятельности. Но самой популярной из них является самая простая деятельность террористов в интернете. Чаще всего, Министерство внутренних дел часто закрывает сайты, где происходит организация в преступные группировки интернет-террористов для последующего осуществления кибертерроризма. Вопрос квалификации деяний таких преступников и сообществ остается открытым, так как на законодательном уровне до сих пор не существует четкого определения кибертеррориста и кибертерроризма.

С резким переходом в дистанционный формат, вызванный вспышкой пандемии, участились не просто случаи кибертерроризма, но и, в свою очередь, он стал эволюционировать и обретать новые признаки. Его опасность заключается, в большей степени в том, что он не имеет определенных географических границ. Террористические акты могут осуществляться из любой точки мира и негативно влиять на кибербезопасность страны.

Из этого большинство юристов и специалистов в сфере компьютерных технологий выделяют наиболее важную проблему: как эффективно отследить кибертеррористов и предотвратить их противоправное деяние, если большинство подобных преступлений совершается с использованием ложных IP-адресов и созданием несуществующих личностей. Всё это затрудняет идентификацию преступников и создаёт проблему в отслеживании местонахождения преступника или целого преступного сообщества [5].

На данный момент вопрос квалификации данного вида киберпреступления остается открытым, в силу того, что существует две точки зрения решения данного вопроса. Первая заключается в том, что некоторые авторы и юристы считают важным внесение в Особенную часть Уголовного кодекса новой статьи о кибертерроризме. Вторая точка зрения заключается в том, что раз кибертерроризм квалифицируется по статьям главы 28 УК РФ, а также значение этого понятия находит выражение в других текстуальных формах («неправомерный доступ», «перехват информации», «нарушение работы информационно-телекоммуникационной системы»), вводить новую статью нецелесообразно.

Мы полагаем, что для полного регулирования кибертерроризма на законодательном уровне нет необходимости вносить отдельный состав, можно ограничиться закреплением термина в Федеральном законе «О противодействии терроризму» и внесением квалифицированного состава в ч. 2 ст. 205 УК РФ в следующем виде – «террористический акт или кибертерроризм, совершенный с использованием информационных технологий, с целью нарушения, изменения или использования особо важной информации, получения несанкционированного доступа в компьютерные системы или создание угрозы посягательства на информационный ресурс либо использование этого ресурса с целью устрашения населения, создания опасной обстановки».

Также для осуществления эффективной политики противодействия кибертерроризму представляется необходимым организация следующих мер:

1. С помощью средств массовой информации информировать население об опасности кибертерроризма и незаконности участия в кибертеррористических сообществах [6];
2. Проводить воспитательные беседы и акции сотрудниками правоохранительных органов в школах, средних профессиональных и высших учебных заведениях на темы профилактики кибертерроризма и методах борьбы с ним, так как именно подростки в связи с дистанционным форматом стали

проводить больше времени в интернете, а также, в силу их умственных и психологических особенностей, именно они склонны к вербовке в террористические сообщества.

3. Усовершенствовать уголовное законодательство Российской Федерации, путем легализации термина «кибертерроризм», а также внесения квалифицированного признака о совершении кибертерроризма в статью 205, либо в одну из статей Главы 28 УК РФ.

Несмотря на то, что на территории Российской Федерации с 2009 года действует Концепция противодействия терроризму, утвержденная Президентом, которая регулирует основные направления противодействия совершения террористических актов, Россия до сих пор нуждается в улучшении и усилении профилактики преступлений террористической направленности, особенно в интернет-среде.

Таким образом, проведя исследование, можно выделить более точное понятие кибертерроризма – это умышленное преступное посягательство на информационный ресурс либо использование этого ресурса с целью устрашения населения, создания опасной обстановки, влекущей гибель людей, причинение значительного имущественного ущерба, либо наступления иных тяжких последствий путем воздействия на принятие решения органами государственной власти.

Во время распространения пандемии коронавирусной инфекции и переход в дистанционный формат, осуществление борьбы с терроризмом в его традиционной форме, а также новой, в виде кибертерроризма, становится все сложнее. Утратив прежние возможности эффективно ограничивать распространение террористической пропаганды в Интернете и контролировать содержание независимых информационных ресурсов, государство оказывается в тяжелой ситуации, когда нужно выходить на новый уровень. То есть, необходимо увеличить контроль за всеми веб-сайтами в интернет - ресурсах, а также, усилить меры по охране особо важной информации, для того, чтобы обезопасить не только государство, но и его население. Одним из инструментов

противодействия кибертерроризму является уголовно-правовой институт, как в рамках национального законодательства, так и на международном уровне. Также важно отметить, что для полного регулирования киберпреступлений, в частности, кибертерроризма, необходимо вносить изменения в нормативные акты, чтобы минимизировать ошибочную квалификацию преступлений совершенных с использованием технических средств.

Список литературы

1. Число киберпреступлений в России. URL. https://www.tadviser.ru/index.php/Статья:Число_киберпреступлений_в_России (дата обращения: 29.11.2021).
2. Новая угроза – киберпандемия. URL. <https://rg.ru/2020/07/02/chto-takoe-kiberpandemiia-i-pochemu-ona-mozhet-obrushit-mirovuiu-ekonomiku.html> (дата обращения: 29.11.2021).
3. Кибертерроризм как новая глобальная угроза. URL. https://spravochnick.ru/mezhdunarodnye_otnosheniya/kiberterrorizm_kak_novaya_globalnaya_ugroza/ (дата обращения: 29.11.2021).
4. Киберпреступность: риски и угрозы. URL. <https://nwb.rgup.ru/rimg/Nauka/Seminar%20and%20conf/11.02.2021/Sbornik.Kiberprestupnost.pdf> (дата обращения: 29.11.2021).
5. Кибертерроризм в России: его свойства и особенности. URL. <https://wiselawyer.ru/poleznoe/76574-kiberterrorizm-rossii-svojstva-osobennosti> (дата обращения: 29.11.2021).
6. Противодействие терроризму средствами уголовного закона. URL. <http://novaum.ru/public/p1067> (дата обращения: 29.11.2021).

Пинчук А.П., аспирант кафедры
уголовного процесса и криминалистики
Алтайский государственный университет, г. Барнаул

Пинчук А.П. НЕКОТОРЫЕ ПРОБЛЕМЫ ИСТОЧНИКОВ ОПЕРАТИВНО-РОЗЫСКНОГО ПРАВА В ОБЛАСТИ ПРОТИВОДЕЙСТВИЯ КИБЕРЭКСТРЕМИЗМУ

Киберпреступность в цифровую эпоху показывает серьезные темпы роста. Молниеносная цифровизация общественной жизни буквально за последние пару десятков лет явилась следствием глобального научно-технического прогресса. Актуализируют указанные проблемы в области цифрового развития общества и внешние факторы. Пандемия коронавируса вынудила многие сферы деятельности перевестись на удаленную систему. Объективно существующие условия вынуждают внедрять цифровые технологии даже туда, где это не всегда целесообразно. Тем не менее, это запрос времени.

В этой связи цифровизация общества имеет не только положительный эффект. Перетекание труда, человеческих и материальных ресурсов в компьютерную сферу и интернет означает автоматический перенос преступного интереса в эту сферу. Мошенничество, вымогательство, диверсии в цифровой инфраструктуре предприятий, незаконное вмешательство в компьютерную информацию – вот далеко не полный перечень распространившихся в этой связи преступных деяний. Однако вслед за преступлениями корыстной направленности в поле цифровой жизни общества вошли и преступления иной мотивации – терроризм и экстремизм с приставкой «кибер».

В Концепции общественной безопасности в Российской Федерации отдельно подчеркнута важность противодействия терроризму и экстремизму: «Члены экстремистских организаций активно используют новые технологии, в

том числе информационно-телекоммуникационную сеть «Интернет», для распространения экстремистских материалов, привлечения в свои ряды новых членов и координации противоправной деятельности. <...> Концепция общественной безопасности в Российской Федерации ставит перед Российским государством задачу постоянного совершенствования системы обеспечения общественной безопасности, включающей в себя правовые меры предупреждения, выявления и пресечения террористической и экстремистской деятельности» [1].

Особенность данных видов преступлений и до их вхождения в цифровое поле заключалась в латентном характере подготовительных действий. Сами акты их проявления извне всегда демонстративные и вызывающие. Но это лишь кульминация преступной деятельности. Основной этап, интересующий правоохранительные органы, представляет стадия подготовки к акту терроризма или экстремизма - готовится взрывчатка, приобретает оружие, составляется план захвата, закупается литература и т.д.

По мере цифровизации этой деятельности возросла и сложность выявления таких преступлений. Теперь тайный характер приобретает не только подготовка к совершению преступления, но и многие действия по его непосредственному совершению.

И если терроризм устоялся в нашем сознании как совершение теракта именно физически, то экстремизм в подавляющем большинстве случаев ассоциируется с сетью «Интернет». Так, судья Верховного Суда РФ О.К. Зателепин на заседании Пленума 20.09.2018 г. сообщил: «За текущий год примерно 90% лиц осуждены за преступления экстремистской направленности с использованием информационно-телекоммуникационных сетей» [2].

Судебная практика и новостные сводки органов внутренних дел демонстрируют актуальность проблемы экстремизма в сети «Интернет» или, так называемого, «киберэкстремизма». Например, в Республике Бурятия в августе 2021 г. к уголовной ответственности за экстремизм был приговорен один из местных жителей. Он разместил на личной странице в социальной сети

высказывания, содержащие признаки возбуждения социальной розни в отношении сотрудников правоохранительных органов [3].

Также в августе 2021 г. в Республике Татарстан провозглашен приговор в отношении жителя города Казани, опубликовавшего в группе одного из мессенджеров аудиосообщения, в которых призывал к противоправным действиям. Согласно судебной лингвистической экспертизе, в аудиосообщениях содержатся признаки призывов к разрушительным действиям, насилию в отношении сотрудников правоохранительных органов, поджогам, погромам, уничтожению имущества, применению взрывчатых веществ. Приговором Советского районного суда г. Казани Республики Татарстан гражданин признан виновным в совершении преступлений, предусмотренных ч. 2 ст. 280 и ч. 3 ст. 212 УК РФ [4].

Государственная политика развивается в направлении усиления защиты информационного пространства в целях недопущения актов террористической и экстремистской деятельности. Так, с 1 августа 2014 г. начал действовать антитеррористический пакет поправок к законодательству. Согласно данному закону, физические и юридические лица, организующие распространение информации и обмен данными между пользователями в Интернете, обязаны сохранять в течение полугода данные о передаче, доставке и обработке голосовой информации, письменные тексты, изображения и т.д. Кроме того, сведения должны передаваться в оперативно-следственные органы, органы госбезопасности и Роскомнадзор. [5]

В Стратегии противодействия экстремизму в Российской Федерации до 2025 года отмечено, что одной из задач государственной политики в сфере противодействия экстремизму является «координация мер, направленных на информационное противодействие распространению экстремистской идеологии в сети «Интернет» (в том числе в социальных сетях) ...» [6]

Роль оперативно-розыскных органов в области противодействия экстремизму трудно переоценить. В основном материалы, признанные

впоследствии экстремистскими, выявляются в ходе оперативно-розыскных мероприятий (далее – ОРМ), проводимых правоохранительными органами.

Сегодня в системе оперативных подразделений, осуществляющих оперативно-розыскную деятельность (далее – ОРД) в сфере противодействия экстремизму, действует, помимо органов безопасности, Главное управление по противодействию экстремизму МВД России (ГУПЭ МВД) и подчиненные ему центры по противодействию экстремизму в субъектах РФ (ЦПЭ). Кроме того, в области оперативно-розыскной деятельности уже давно действует и зарекомендовал себя отдел «К» МВД РФ.

Пример деятельности данных подразделений продемонстрировать не сложно. Так, в сентябре 2020 г. сотрудниками ГУПЭ МВД России во взаимодействии с ФСБ России и Главного следственного управления Следственного комитета России по г. Москве пресечена деятельность интернет-сообщества «UBER ALLES», участники которого в открытом доступе размещали материалы, связанные с публичными призывами к осуществлению террористической деятельности, оправданием и пропагандой терроризма, а также направленные на возбуждение ненависти и вражды, унижение достоинства человека и группы лиц по признакам расы, национальности, языка.

В ходе совместных ОРМ и следственных действий установлено, что указанное праворадикальное движение образовалось в результате слияния аналогичных ультранационалистических сообществ: «Русский Фронт», «Белый Фронт» «Штурмовой корпус», «Argan Partisan», распространявших в социальных сетях статьи и видеоролики, содержащие пропаганду идеологии Национал-социалистической немецкой рабочей партии, а также информационных материалов экстремистского характера и террористического толка.

Собранные результаты ОРД послужили основанием для возбуждения следственными органами ГСУ СК России по г. Москве уголовного дела по признакам составов преступлений, предусмотренных п. «а» ч.2 ст. 282, ч.1 ст. 205.2 УК РФ [7].

Оперативные подразделения в сфере противодействия экстремизму в своем арсенале имеют налаженный контакт с Роскомнадзором – органом, контролирующим цифровое пространство в России. Так в Соглашении о взаимодействии Министерства внутренних дел Российской Федерации и Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций закреплено: «Взаимодействие между Сторонами осуществляется в соответствии с установленной нормативными правовыми и ведомственными правовыми актами компетенцией структурных подразделений и территориальных органов на региональном уровне, в том числе по вопросам пресечения распространения экстремистских материалов, в том числе в информационно-телекоммуникационной сети "Интернет"» [8].

Проблема правового регулирования оперативно-розыскного противодействия экстремизму на сегодняшний день не получила должного научного внимания. С одной стороны, это можно объяснить гораздо более быстрым развитием цифровой преступности, чем российского законодательства, с другой – преимущественно негласным характером ОРД, что само по себе уже делает многие «больные места» оперативно-розыскного правового массива недостижимым для научного сообщества (сравнительно небольшое число российских ученых в сфере ОРД имеют допуск к закрытым источникам). Однако было бы неправильно утверждать, что открытые источники оперативно-розыскного права лишены недостатков.

Обратим внимание на некоторые аспекты.

Источники оперативно-розыскного права в общем виде закреплены в ст.4 Закона об ОРД. Указанная норма закрепляет, что правовой основой ОРД являются «Конституция Российской Федерации, настоящий Федеральный закон, другие федеральные законы и принятые в соответствии с ними иные нормативные правовые акты федеральных органов государственной власти».

Конституция РФ как источник оперативно-розыскного права, обладающий высшей юридической силой, прокладывает вектор дальнейшей работы в области противодействия экстремизму. В России запрещается

создание и деятельность общественных объединений, цели или действия которых направлены на насильственное изменение основ конституционного строя и нарушение целостности Российской Федерации, подрыв безопасности государства, создание вооруженных формирований, разжигание социальной, расовой, национальной и религиозной розни (ч. 5 ст. 13). Запрещаются любые формы ограничения прав граждан по признакам социальной, расовой, национальной, языковой или религиозной принадлежности (ч. 2 ст. 19), пропаганда или агитация, возбуждающие социальную, расовую, национальную или религиозную ненависть и вражду, а также пропаганда социального, расового, национального, религиозного или языкового превосходства (ч. 2 ст. 29) [9]. Это нормы общего характера, относящиеся не только к оперативным подразделениям правоохранительных органов. Тем не менее, вспоминая, что материалы, признанные впоследствии экстремистскими, в основном выявляются в ходе ОРМ, нельзя не признать особую важность конституционно-правовых положений для оперативно-розыскных органов.

Система источников оперативно-розыскного права включает в себя, помимо прочих, и законы о противодействии терроризму и экстремизму.

Например, ч.1.2 ст. 18 ФЗ «О противодействии терроризму» закрепляет: «Федеральные органы исполнительной власти, осуществляющие в пределах своих полномочий противодействие терроризму и уполномоченные на осуществление оперативно-розыскной деятельности, вправе истребовать сведения о законности происхождения денег, ценностей, иного имущества и доходов от них у близких родственников, родственников и близких лиц лица, совершившего террористический акт...» [10]. ФЗ «О противодействии экстремистской деятельности» в ст.12 закрепляет запрет на использование сетей общего доступа для осуществления экстремистской деятельности. В случае использования указанных сетей в деструктивной деятельности применяются меры, указанные в Законе [11]. То есть данным положением закон по всей видимости (проблему наименования сети «Интернет» в действующем

законодательстве мы ещё затронем) провозглашает сеть «Интернет» - местом для совершения преступления.

Тем не менее данные законы непосредственно осуществление ОРД не регулируют. Основным нормативным правовым актом (далее – НПА), которым должны руководствоваться оперативные сотрудники при выявлении и раскрытии экстремистских преступлений в компьютерной сфере, является Федеральный закон «Об оперативно-розыскной деятельности» (далее – Закон об ОРД) [12]. При принятии данного закона о проблеме киберэкстремизма и кибертерроризма речи ещё не шло. Имели место другие вопросы, требующие оперативного вмешательства. Тем не менее, цифровизация социума затребовала определенных новаций. Закон об ОРД отдельно об особенностях работы с преступлениями, совершенными в информационно-телекоммуникационной сети «Интернет» не говорит. В 2016 г. в перечень ОРМ было включено «Получение компьютерной информации» как раз на фоне роста количества киберпреступлений (в целях противодействия, в том числе, терроризму и экстремизму). Но на этом развитие правового регулирования ОРД в компьютерной сфере не остановилось. В мае 2021 г. МВД был внесен законопроект о добавлении перечня ОРМ еще одним – «Исследование компьютерной информации», который мотивирован растущим числом совершаемых преступлений в сети «Интернет» [13]. Несмотря на критику данного законопроекта и остановку работы в этом направлении, весьма интересна и понятна озабоченность компетентных кругов улучшением правового регулирования ОРД.

Как уже выше отмечалось, проблематика правового регулирования оперативно-розыскного противодействия киберэкстремизму не нашла должного научного отражения.

Так, критикуется ОРМ «Получение компьютерной информации». Можно ли считать получение информации из сети «Интернет» посредством компьютера оперативно-розыскным мероприятием «Получение компьютерной информации»? Само по себе это непонимание не влечет необратимых

процессов. Если это не данное ОРМ, то значит это ОРМ «Наведение справок». Тем не менее, в законодательстве имеется двусмысленность. И это не единственная проблема данного ОРМ. Н.Г. Корнаухова и С.В. Катков отмечают, что несмотря на то что ОРМ «Получение компьютерной информации» уже существует относительно продолжительное время, фактически отсутствует нормативно-правовая регламентация, позволяющая четко определить варианты его документального оформления, обеспечивающих максимально эффективное использование полученных результатов, например, в рамках уголовного судопроизводства [14, с.185].

Закон об ОРД содержит лишь одно упоминание сети «Интернет» (ст.12.1), и то не в интересующем нас смысле. А тем не менее, сотрудники оперативных подразделений зачастую занимаются мониторингом информации, размещаемой в именно информационно-телекоммуникационной сети «Интернет». ФЗ «О связи» в ч.2 ст.64 закрепляет: «Операторы связи обязаны обеспечивать реализацию установленных федеральным органом исполнительной власти в области связи по согласованию с уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность или обеспечение безопасности Российской Федерации, требований к *сетям и средствам связи* (курсив мой – А.П.) для проведения этими органами в случаях, установленных федеральными законами, мероприятий в целях реализации возложенных на них задач, а также принимать меры по недопущению раскрытия организационных и тактических приемов проведения указанных мероприятий» [15]. Согласимся с А.В. Кутузовым, который отмечает, что «сеть связи» в том значении, которое раскрывается в ст.2 Закона о связи не тождественно с понятием «информационно-телекоммуникационная сеть «Интернет»» [16, с.10]. В этой связи ни Закон о связи, ни Закон об ОРД не имеют четкого закрепления возможности оперативных подразделений осуществлять свою деятельность, в том числе по противодействию экстремизму, в сети «Интернет».

Таким образом, отсутствие единообразия в использовании формулировок, предполагающих или включающих в себя понятие «сеть "Интернет"», порождает проблему последующего правоприменения. ФЗ «О противодействии экстремистской деятельности» орудует формулировкой «сети общего доступа», Закон об ОРД – «информационные системы», и то, скорее всего, в смысле информационного обеспечения деятельности (напр., АИПС и др.), а не среды проведения ОРМ. В этой связи, в целях снятия имеющихся вопросов целесообразным видится внесения в ст.6 Закона об ОРД наряду с информационными системами формулировку «информационные сети», под которыми будет пониматься, в том числе, и информационно-телекоммуникационная сеть «Интернет».

До сих пор не регламентирована в Законе об ОРД процедура привлечения специалиста для предусмотренного ст.15 изъятия электронных носителей информации. Компьютерная техника зачастую является носителем экстремистского материала. На стадии задержания преступника у оперативных сотрудников в арсенале имеется указанное положение ст.15 Закона об ОРД о возможности изъятия техники. Тем не менее, нерешенной остается проблема: привлечение специалиста – дискреционное усмотрение сотрудников или же обязанность? Исходя из толкования указанной нормы, это право, а не обязанность оперативного сотрудника. Целесообразным видится исключить излишнюю диспозитивность в данном вопросе, поскольку от усмотрения должностного лица оперативно-розыскного органа зависит сохранность материалов на внешнем носителе. Неправильное изъятие носителя в отсутствие специалиста может повлечь необратимый процесс уничтожения данных, в том числе вследствие заранее предусмотренных преступником мер. В законе следует предусмотреть случаи, когда привлечение специалиста обязательно (когда у оперативного сотрудника нет специального образования, изъятие носителя информации в данной обстановке несет риск утраты данных и т.д.).

В науке можно также встретить позицию о необходимости законодательно закрепить полномочия правоохранительных органов на

осуществление мониторинга опубликованных в социальных сетях или иных ресурсах материалов противоправного (в том числе экстремистского) характера, а в некоторых случаях обеспечить проведение соответствующих надзорных, оперативно-розыскных, следственных мероприятий с возможностью получения необходимой информации от провайдеров или Роскомнадзора напрямую без судебного разрешения [17, с.65]. Этому предложению есть свои объяснения. В «Стратегии противодействия экстремизму в Российской Федерации до 2025 года» среди основных направлений государственной политики по противодействию экстремизму выделен «мониторинг средств массовой информации и информационно-телекоммуникационных сетей, включая сеть «Интернет», в целях выявления фактов распространения идеологии экстремизма, экстремистских материалов и незамедлительного реагирования (ст.27) [18].

Ведомственные акты также закрепляют мониторинг как одно из направлений деятельности сотрудников МВД. Так, в приказе МВД России от 17.01.2006 № 19 закреплено, что сотрудники подразделений по противодействию экстремизму проводят мониторинг оперативной обстановки в области противодействия экстремистской деятельности (п. 17.1) [19].

Таким образом, правовое регулирование ОРД в области противодействия киберэкстремизму, как было выяснено, не лишено недостатков. Необходимо дальнейшее совершенствование источников оперативно-розыскного права в части разработки новых методов противодействия киберэкстремизму, создания необходимых условий для проведения ОРМ в целях выявления, предупреждения, пресечения и раскрытия киберпреступлений экстремистской направленности в сети Интернет.

Список литературы

1. Концепция общественной безопасности в Российской Федерации от 14 ноября 2013 г. № Пр-2685. Доступ из справ.-правовой системы «КонсультантПлюс».
2. Заседание Пленума Верховного Суда РФ 20 сентября 2018 г. Выступление О.К. Зателепина, судьи Верховного Суда РФ. URL : <https://www.youtube.com/watch?v=YwrXBxTt1M> (дата обращения: 09.12.2021)
3. В Бурятии двое местных жителей признаны виновными в совершении преступлений экстремистской направленности. URL : https://мвд.рф/mvd/structure1/Glavnie_upravlenija/Glavnoe_upravlenie_po_protivod_ejstviju_j/Publikacii_i_vistuplenija/item/25719033/ (дата обращения: 09.12.2021)
4. Житель Казани признан виновным в призывах к экстремистской деятельности и массовым беспорядкам. URL: https://мвд.рф/mvd/structure1/Glavnie_upravlenija/Glavnoe_upravlenie_po_protivod_ejstviju_j/Publikacii_i_vistuplenija/item/25491032/ (дата обращения: 09.12.2021)
5. Госдума приняла "антитеррористический" пакет законопроектов. URL: <https://www.rbc.ru/politics/28/02/2014/5704186f9a794761c0ce741b> (дата обращения: 09.12.2021)
6. Указ Президента РФ от 29 мая 2020 г. № 344 «Об утверждении Стратегии противодействия экстремизму в Российской Федерации до 2025 года» // Собрание законодательства РФ. – 2020. - № 22. - Ст. 3475
7. Сотрудниками правоохранительных органов задержан администратор националистического интернет-сообщества «UBER ALLES». URL: https://мвд.рф/mvd/structure1/Glavnie_upravlenija/Glavnoe_upravlenie_po_protivod_ejstviju_j/Publikacii_i_vistuplenija/item/21331201/ (дата обращения: 09.12.2021)
8. «Соглашение о взаимодействии Министерства внутренних дел Российской Федерации и Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций» (утв. МВД России,

Роскомнадзором 23.08.2017). Доступ из справ.-правовой системы «КонсультантПлюс».

9. Конституция Российской Федерации от 12 декабря 1993 г. Доступ из справ.-правовой системы «КонсультантПлюс».

10. О противодействии терроризму: федеральный закон от 6 марта 2006 г. № 35-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

11. О противодействии экстремистской деятельности: федеральный закон от 25 июля 2002 г. № 114-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

12. Об оперативно-розыскной деятельности: федеральный закон от 12 августа 1995 г. № 144-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

13. <https://www.advgazeta.ru/novosti/operativnikam-khotyat-razreshit-issledovanie-kompyuternoy-informatsii-v-ramkakh-ord/> (дата обращения: 09.12.2021)

14. Корнаухова Н.Г., Катков С.В. Получение компьютерной информации: проблемы теории и практики // Вестник Восточно-Сибирского института МВД России. - 2020. - № 1 (92). - С. 182-191

15. О связи : федеральный закон от 07.07.2003 г. № 126-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

16. А. В. Кутузов. Правовое регулирование оперативно-розыскной деятельности в сети интернет в условиях противодействия экстремизму // Вестник Балтийского федерального университета им. И. Канта. Сер.: Гуманитарные и общественные науки. - 2020. - № 3. - С. 5-15.

17. Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий: учебное пособие: в 2 ч. / А.В. Аносов и др. М.: Академия управления МВД России, 2019. Ч. 1.

18. Стратегия противодействия экстремизму в Российской Федерации до 2025 года: (утв. Президентом РФ 28.11.2014 № Пр-2753). Доступ из справ.-правовой системы «КонсультантПлюс».

19. Приказ МВД России от 17.01.2006 № 19 «О деятельности органов внутренних дел по предупреждению преступлений». Доступ из справ.-правовой системы «КонсультантПлюс».

Матвеева С.В., Юридический институт

АлтГУ, г. Барнаул

Научный руководитель: Стародубцева М.А., преподаватель кафедры
уголовного права и криминологии АлтГУ

Матвеева С.В. РЕГИОНАЛЬНЫЕ ОСОБЕННОСТИ ЭКСТРЕМИСТСКОЙ ПРЕСТУПНОСТИ В АЛТАЙСКОМ КРАЕ

Несмотря на строгую политику государства, направленную на борьбу с преступными проявлениями и, проблема предупреждения преступлений как одной из целей уголовного наказания остается приоритетной на сегодняшний день, как на федеральном, так и региональном уровне. Данная проблема актуальна и для посягательств экстремистской направленности.

Важную роль в механизме противодействия экстремизму играют органы внутренних дел. В целях реализации Указа Президента Российской Федерации от 06.09.2008 № 1316 в структуре МВД России образованы Главное управление по противодействию экстремизму МВД России, Центр обеспечения оперативно-служебной деятельности по противодействию экстремизму МВД России, Центр по противодействию экстремизму ГУ МВД России по федеральному округу, центры (группы) по противодействию экстремизму УМВД России по субъектам Российской Федерации, в компетенцию которых входит ряд полномочий по выявлению, пресечению, а также предупреждению рассматриваемой группы преступных посягательств.

Говоря об Алтайском крае, то стоит обратить внимание, что данный регион в течение пяти последних лет входит в рейтинг 15 субъектов РФ по показателю наибольшего количества зарегистрированных преступлений экстремистской направленности.

По статистическим данным управления МВД России по Алтайскому краю за 2020 год на территории края зарегистрировано 2 преступления

экстремистской направленности, а также задокументировано 92 административных правонарушения экстремистской направленности.

С использованием сети Интернет совершено 79 административных правонарушений. В рассматриваемом периоде зарегистрировано 7 преступлений террористического характера (январь-декабрь 2019 года – 4):

- 13.01.2020 возбуждено уголовное дело по ч. 2 ст. 208 УК РФ по факту вступления гражданина Российской Федерации на территории иностранного государства в состав незаконного вооруженного формирования, не предусмотренного законодательством данного государства, в целях, противоречащих интересам Российской Федерации;

- 31.01.2020 возбуждено уголовное дело по ст. 205.3 УК РФ по факту прохождения обучения гражданина Российской Федерации в целях осуществления террористической деятельности в составе незаконного вооруженного формирования, входящего в состав террористической организации «ИГИЛ»;

- 24.06.2020 возбуждено уголовное дело по ч. 1 ст. 30, ч. 2 ст. 205.5 УК РФ по факту приготовления к участию в деятельности организации, которая в соответствии с законодательством Российской Федерации признана террористической;

- 29.07.2020 возбуждено уголовное дело по ч. 1 ст. 205.2 УК РФ по факту публичного оправдания терроризма;

- 04.08.2020 возбуждено уголовное дело по ч. 2 ст. 205.5 УК РФ по факту пособничества в участии в деятельности террористической организации «ИГИЛ»; - 14.08.2020 возбуждено уголовное дело по ч. 6 ст. 205.1 УК РФ по факту склонения граждан к участию в деятельности международной террористической организации «ИГИЛ» и пособничества в участии в деятельности террористической организации «ИГИЛ»;

- 14.08.2020 возбуждено уголовное дело по ч. 2 ст. 205.5 УК РФ по факту пособничества в приготовлении к участию в деятельности организации, которая признана террористической.

В Алтайском крае завершилось несколько громких уголовных дел экстремистской направленности.

Так, 6 августа 2018 года Индустриальный районный суд Барнаула прошло первое заседание по делу Марии Мотузной, обвиняемой в унижении достоинства группы лиц, выделенной по признаку расы (ч. 1 ст. 282 УК) и оскорблении чувств верующих (ч. 1 ст. 148 УК) за публикацию картинок на странице в соцсети "ВКонтакте".

Мотузной вменяют в вину публикацию в соцсети "ВКонтакте" изображений, на одном из которых Иисус Христос пускает сигаретный дым через отверстие в ладони, а на другом крестный ход по разбитой дороге сопровождается подписью "Две главные беды России". Экспертиза выявила в этих картинках *"лингвистические, психологические и религиоведческие признаки выражения неуважения к обществу в целях оскорбления религиозных чувств верующих"*. В двух других изображениях еще одна экспертиза выявила лингвистические признаки *"унижения представителей негроидной расы"* и *"пропаганды превосходства европеоидной расы над негроидной"*.

Закончилось уголовное дело 41-летней жительницы Барнаула Натальи Телегиной. По данным следствия, с 2014 до 2016 год, придерживаясь негативных взглядов "по отношению к религии и лицам, относящимся к уроженцам Кавказа", она разместила в соцсети "ВКонтакте" изображения с текстами, возбуждающими национальную и религиозную ненависть и вражду. Некоторые изображения и тексты, по мнению следствия, выражали явное неуважение к обществу и оскорбляли религиозные чувства верующих.

Одним из важнейших этапов процесса доказывания по делам о преступлениях экстремистской направленности выступает производство судебных экспертиз. Именно экспертиза позволяет следователю, прокурору и суду прийти к выводу о виновности (невиновности) лиц, привлеченных к уголовной ответственности.

К сожалению,

Несмотря на то, на профессиональный уровень подготовки специалистов в области экстремизма, существуют спорные моменты. Разберём некоторые из них:

1. Привлечение в качестве экспертов и специалистов лиц не компетентных в данной сфере.

При назначении экспертизы не всегда в надлежащем объеме выясняется уровень компетентности. Соответствует ли **сфера его деятельности, профессиональный опыт, научные труды** той области специальных знаний, к которой относятся вопросы, подлежащие разрешению. Иногда в качестве экспертов привлекаются лица, относительно которых имеются основания полагать, что они прямо или косвенно заинтересованы в деле.

2. Неправильная постановка вопросов перед экспертами.

Многие постановления о назначении экспертиз не содержат изложения фактических обстоятельств дела. Неверно определяются природа и предмет использования специальных познаний, в то время как по делу требуется установление направленности публикации путем **социально-психологического** (психолингвистического и семантического) анализа текста и языковых приемов, используемых публикатором (оратором), назначается **философская, историческая, искусствоведческая, стилистическая**, гуманитарная экспертиза.

В результате экспертное исследование подменяется историческими, религиоведческими, политологическими, биологическими, и другими рассуждениями, неверными рассуждениями.

3. Неправильная оценка выводов, полученных в результате проведения экспертиз.

Не всегда учитывается требование о том, что заключение эксперта не является обязательным для лиц, осуществляющих производство по делу, и не имеет заранее установленного доказательственного значения применительно к конкретному преступлению. Поэтому оценивать выводы экспертизы необходимо в совокупности с другими доказательствами.

Для того, чтобы решить все эти спорные моменты в России необходимо создать **федеральное экспертное учреждение, которое проводило бы весь комплекс экспертиз по делам об экстремистской деятельности.** Минимизировалось бы допущение ошибок в деятельности экспертов экстремистской направленности. Помимо этого следует воспитывать толерантности и правопослушности самих граждан. Одна из главных целей в противодействии экстремизму является воспитание у населения толерантного сознания и поведения, достижение гражданского мира и согласия в обществе является важнейшей задачей органов государственной власти. В этом вопросе следует уделить особое значение воспитанию подрастающего поколения в духе толерантности и терпимости друг к другу, в том числе к представителям разных национальностей, религиозных конфессий и т. д. Что касается молодежи и несовершеннолетних, для них необходима занятость культурного досуга и пропаганда здорового образа жизни, в стране, что, безусловно, является залогом успешной профилактики экстремизма.

Изложенное позволяет сделать вывод, что решение поставленной задачи по предупреждению экстремизма как цели наказания требует комплексного подхода.

Башкатова М.М., Юридический институт

АлтГУ, г. Барнаул

Научный руководитель: Стародубцева М.А., преподаватель кафедры
уголовного права и криминологии АлтГУ

Башкатова М.М. ПОЛИТИЧЕСКИЕ ИНФОРМАЦИОННЫЕ УГРОЗЫ И ПУТИ ИХ УСТРАНЕНИЯ

Современное развитие социальной жизни человека на рубеже XX-XXI в. связано с нарастающими оборотами информатизации и компьютеризации всех областей науки. Основным продуктом деятельности становится информация, а самой деятельностью человека ее хранение, обработка и распространение.

В результате глобальной информатизации, Интернет стал общедоступной коммуникативной сетью, которая вышла на авансцену социального, культурного и политического развития общества. Революционное развитие Интернета влекло за собой столь же быстрое развитие угроз, возникающих из-за сложностей повсеместного контроля сети. С каждым днем возрастает необходимость сохранения баланса между свободным распространением информации и обеспечением безопасности личности и общества в целом.

Влияние информационных технологий и информатизации неизбежно. И на данный момент информация по праву признается стратегическим ресурсом любого государства. В этой связи возникают различные опасности, связанные с хранением и распространением информации.

Целью статьи является раскрытие темы «Политические информационные угрозы» и рассмотреть пути их устранения.

Понятие «угрозы» описано в Стратегии национальной безопасности Российской Федерации до 2020 года. «Угроза – это прямая или косвенная возможность нанесения ущерба конституционным правам, свободам, достойному качеству и уровню жизни граждан, суверенитету и территориальной целостности, устойчивому развитию Российской Федерации,

обороне и безопасности государства». Угроза информационной безопасности в сети Интернет может обозначаться как потенциальная возможность причинения ущерба жизненно-важным интересам личности, общества и государства с использованием информационно-коммуникативных средств сети Интернет.

На сегодняшний день смена угроз “холодной войны” угрозами “информационной войны” существенно повышает значение информационной безопасности в системе национальной безопасности государства, обуславливает расширение ее содержания. Потеря государственного контроля над российскими коммуникациями может привести к утрате национальной независимости.

Из внутренних угроз информационной безопасности РФ в сфере внешней политики наибольшую опасность представляют:

- нарушение установленного порядка сбора, обработки, хранения и передачи информации в федеральных органах исполнительной власти, реализующих внешнюю политику РФ, и на подведомственных им предприятиях, в учреждениях и организациях
- информационно-пропагандистская деятельность политических сил, общественных объединений, средств массовой информации и отдельных лиц, искажающая стратегию и тактику внешнеполитической деятельности РФ
- недостаточная информированность населения о внешнеполитической деятельности РФ

Основными мероприятиями по обеспечению информационной безопасности РФ в сфере внешней политики являются:

- разработка основных направлений государственной политики в области совершенствования информационного обеспечения внешнеполитического курса РФ
- разработка и реализация комплекса мер по усилению информационной безопасности информационной инфраструктуры федеральных органов исполнительной власти, реализующих внешнюю

политику РФ, российских представительств и организаций за рубежом, представительств РФ при международных организациях

- создание российским представительством и организациям за рубежом условий для работы по нейтрализации распространяемой там дезинформации о внешней политике РФ

- совершенствование информационного обеспечения работы по противодействию нарушениям прав и свобод российских граждан и юридических лиц за рубежом

- совершенствование информационного обеспечения субъектов РФ по вопросам внешнеполитической деятельности, которые входят в их компетенцию

Информационная безопасность, будучи отраслью национальной безопасности государства, обращает внимание и на более глобальные виды угроз – политические. Проблемы политического характера – проблемы информационной безопасности, возникающие из-за информационных войн, кибервойн и электронной разведки в интересах политических групп, компрометации государственной тайны, атак на информационные системы важных оборонных, транспортных и промышленных объектов, неполного информирования и дезинформации руководителей крупных учреждений.

Серьезную опасность представляют собой стремление ряда государств к доминированию в мировом информационном пространстве, разработка рядом государств концепции информационных войн, предусматривающей создание средств опасного воздействия на информационные сферы других стран мира, нарушение нормального функционирования информационных и телекоммуникационных систем, а также сохранности информационных ресурсов, получении несанкционированного доступа к ним. Реалией наступившего информационного века является информационная война, а не противостояние армий, погибающих на полях генеральных сражений. Война в зоне Персидского залива может быть определена как первая полномасштабная

война нового этапа в функционировании вооруженных сил в условиях создания глобального мирового информационного пространства.

Описываемых проблем можно избежать, если рассматривать вопросы информационной безопасности не только при обучении соответствующих специалистов, но и включать в перечень системообразующих компонентов понятия «информационная культура» элементов информационной безопасности, которыми, по нашему мнению, сегодня должен владеть не только специалист в области защиты информации, но и каждый, пользователь компьютера.

В российских условиях существенную угрозу стабильности политической системе несет Интернет. Это связано главным образом с отсутствием эффективных правовых механизмов, регулирующих жизнь в интернет-пространстве.

В результате под влиянием ИКТ система информационно-политических отношений трансформируется не просто в поле информационного противоборства, то есть соперничества политических сил по поводу влияния на ключевые сферы социальных отношений и установления контроля над источниками стратегических ресурсов, а войну компроматов, где не последнее место занимает «черный пиар». Наряду с официальными сайтами органов государственной власти, политических партий, общественных организаций в Интернете создаются информационные площадки для «вброса» в общество компромата на ту или иную политическую силу, так как практически никаких ограничений на характер помещаемой в Сеть информации не существует. Более того, современные интернет-технологии содействуют разрастанию международного терроризма и возникновению принципиально нового высокотехнологичного кибертерроризма. При этом могут применяться как информационно-компьютерные, так и информационно-психологические средства. Интернет же, к сожалению, все активнее используется для распространения идеологии терроризма, вовлечения в противоправную

деятельность новых членов, о чем красноречиво свидетельствует наличие большого количества соответствующих сайтов.

Помимо всего этого, довольно распространенной является точка зрения, что развитие информационных технологий может способствовать росту политической пассивности. Новые пользователи Всемирной компьютерной сети привносят с собой традиционные стереотипы пассивного поведения в информационной среде. Важно также подчеркнуть, что «демократия в киберпространстве» (например, обсуждение политических проблем в Интернете) не означает демократии в реальном мире. Размышления о политических делах в Интернете нечасто приводит к политической активности в реальной жизни. Все эти обстоятельства свидетельствуют об острой потребности государства постоянно укреплять информационную безопасность его политической сферы, содействовать устранению угроз, связанных с использованием ИКТ.

Одним из путей совершенствования системы информационной безопасности видится синергия мировой правовой системы, права отдельно взятой страны и самоконтроль самих пользователей. Только во взаимодействии этих трех уровней можно добиться эффективной работы системы информационной безопасности в сети Интернет.

Ельникова С. М., секретарь Барнаульского
отделения Всероссийской общественной
организации «Молодая гвардия Единой России,
волонтер студенческого отряда
«Антиэкстремизм»
Колледж АлтГУ, г. Барнаул

Научный руководитель: Стародубцева М.А., преподаватель кафедры
уголовного права и криминологии АлтГУ

Стародубцева М.А., Ельникова С.М. СОЦИО-КУЛЬТУРНЫЕ ПРЕДПОСЫЛКИ ФОРМИРОВАНИЯ ТЕРРОРИСТИЧЕСКИХ ВОЗЗРЕНИЙ В МОЛОДЕЖНОЙ СРЕДЕ

Традиционно под культурой принято понимать некую систему хранения и передачи информации, навыков и умений от поколения к поколению. Также в процессе передачи информации и технологий в сознание человека закладывается ряд культурных паттернов, установок, которые, преломляясь через мироощущение конкретного человека, формируют единую картину мира. Именно поэтому обычно в культуре выделяют информационный, технологический и ценностный уровни.

На сегодняшний день все чаще звучит мнение о том, что из вышеуказанных культурных уровней доминируют информация и технология, что означает потерю духовно-нравственных ценностей. Духовность же, дух в понимании В. Соловьева – это единство истины, добра и красоты [2], то есть в традиционном философском понимании – это познавательное, нравственное и эстетическое [6].

Термин «культура» сегодня обычно воспринимается именно с приставкой «массовая». Если изначально массовая культура воспринималась как антипод

культуры «элитарной», то сейчас она фактически поглощает собой последнюю. Это ее реальность и это же распространенный стереотип.

Многие исследования описывают, как массовая культура разрушает все порядочное, что есть в человеке, насаждая хаос [5]. Все это, безусловно, справедливо. Но социум есть сложнее явление и его порождения также сложны и многогранны. Хотя бы поверхностно осознать феномен массовой культуры невозможно без обращения к ее истокам.

Информационную эпоху иногда зовут «цивилизацией протезов», указывая, что поток информации притупляет чувствительность, понижает смысловую нагрузку.

Период «локдаунов» не только вырвал людей из привычного ритма жизни, но и открыл им дорогу в мир эскапизма, позволил сбежать от реальных переживаний в близкий и простой мир бестселлеров и кинохитов.

И здесь нетрудно заметить, что разнообразие массовой культуры происходит из культуры элитарной. Массовая культура становится посредником между человеком и элитарным знанием, решает задачу просвещения.

И здесь, на наш взгляд, может таиться опасность подобного «заражения масс» [3]. Приведем пример. Сегодня во многих отраслях массовой культуры заметна тенденция осмысливания традиционных сюжетов на новый лад, переименования знакомых персонажей для того, чтобы взглянуть на них под другим углом. Каноничным злодеям XIX–XX веков создают глубокие предыстории, объясняющие их мотивы, заставляющие проникнуться к ним сочувствием. Люди по-новому смотрят, например, на стереотипную Круэллу де Виль, превращенную сегодня в антигероиню с изломанной и трагической судьбой, сопереживают безжалостному убийце и психопату Джокеру, ведь им демонстрируется его борьба с обществом. Но, повторимся, в условиях мирового политического и экономического кризиса, в период расцвета эскапистских тенденций муссирование подобных «серых» идеалов может привести к разрушительным последствиям.

Мировая гибридно-информационная война использует рычаги массовой культуры в своих целях. Одним из ее рупоров стала сеть «Интернет», ее основное достоинство – высокая скорость стихийного распространения информации. Информационные технологии через свою техническую организацию несут идею (идеологию) мира, новые способы отношений и восприятия, навязанные им, изменение традиционных структур семьи и группы [4].

По сути речь идет о целенаправленном формировании идеологами террористических организаций нового типа террориста через искажение сознания и мировоззрения. В 2016–2017 гг. мы наблюдали первый опыт подобной вербовки – всплеск активности суицидальных сообществ в социальных сетях. Интернет-страницы игроков смертельных забав стали объектами поклонения, идеалом считается игрок, выполнивший последнее задание – собственно, самоубийство.

На эту почву нестабильной неокрепшей подростковой психики, сформированной на смертельных идеалах, наложилась волна скулшутинга в российских образовательных учреждениях. Происшедший 17 октября 2018 года в Керченском политехническом колледже массовый расстрел во многом повторяет трагедию в апреле 1999 года в США. Речь о взрыве и массовом расстреле в старшей школе «Колумбайн» (штат Колорадо). Тогда террористов было двое: Эрик Харрис (18 лет) и Дилан Клиболд (17 лет) – учащиеся той самой школы.

20 сентября 2021 года в Пермском государственном университете произошла аналогичная трагедия, а за полгода до нее эхо «Колумбайна» прогремело в казанской гимназии №175 11 мая 2021 года.

И это только несколько эпизодов из хронологии скулшутинга в России. Данное явление смогло органично вписаться в массовую интернет-культуру не в последнюю очередь благодаря новому идеалу молодежи – антигерою, бросающему вызов системе, уничтожающему своих врагов исключительно силовыми методами.

Для подтверждения выдвинутых тезисов нами было проведено криминологическое исследование, направленное на выявление причин искажения нравственного облика современного общества и моральных категорий в массовой культуре. Изучалась взаимосвязь между моральными ценностями индивидов и их влиянии на криминогенную обстановку в обществе.

Исследование проводилось среди преподавателей и студентов Колледжа Алтайского государственного университета. Респондентами выступили также преподаватели кафедры уголовного права и криминологии Юридического института, кафедры социальной философии, онтологии и теории познания Института массовых коммуникаций, философии и политологии.

На первый вопрос, который мы задали респондентам «Как Вы оцениваете духовно-нравственное состояние современного общества?» 69,4 % ответили, что ценности современного общества далеки от нравственного идеала. По их мнению, морально-нравственные категории искажены, массовая культура не разграничивает и не противопоставляет нравственное и безнравственное. Ценностный мотив, намерение не всегда соответствуют поступку. Нередко полезные результаты имеют негативную ценностную ориентацию. При этом моральная оценка поступка осуществляется только на основании его результата.

Меняется и сама мораль. 92,7% респондентов согласились, что массовая культура оказывает влияние на миропонимание и поведение человека. Яркий тому пример – кратко охарактеризованная нами субкультура «Колумбайн». Под массивным воздействием отрицательных идеалов рождается новый тип сознания – мышление террориста-индивидуалиста, невротика без четкой гражданской позиции.

Причиной искажения морально-нравственных категорий 83,9% опрошенных видят в низком уровне нравственного сознания, и, как следствие, отсутствии критического мышления.

Нами также был задан вопрос: «Влияет ли искажение моральных и нравственных ценностей на криминогенную обстановку в обществе?». 82,4% опрошенных ответило, что искажение моральных и нравственных ценностей приводит к увеличению количества преступлений. По мнению респондентов, именно нравственное воспитание и моральное совершенствование общества может привести к снижению количества преступлений. Но на вопрос, как именно это сделать, респонденты ответить затруднились. Нередко в информационно-телекоммуникационных сетях распространяются материалы, содержащие публичные призывы к осуществлению террористической деятельности или публично оправдывающих терроризм, другие экстремистские материалы, а также материалы, пропагандирующие порнографию, культ насилия и жестокости, и материалы, содержащие нецензурную брань. По мнению некоторых респондентов, именно введение цензуры в средства массовой информации приведет к уменьшению количества преступлений экстремистской и террористической направленности.

Некоторые материалы несут в себе идеологию насилия в массы. Негативная ценностная мотивация не осуждается обществом, если она приводит к полезным результатам, получению собственной выгоды. Насилие порождается не страстью, а экраном.

Распространение преступлений террористической направленности нельзя объяснять исключительно «объективными причинами» (политическими, социальными, психологическими). Нередко мы можем наблюдать прецессию средств массовой информации в отношении террористического насилия [1]. Именно поэтому терроризм порождается не страстью, а материалами, несущими его идеологию через средства массовой информации. Отсюда, мало ввести институт цензуры, необходимо формирование не менее яркой и четкой ответной антитеррористической идеологии. Идеологии нового типа, основанной не на теоретическом учении, а на клиповых образах. Новый терроризм в цифровой сфере подпитывается идеалами массовой культуры, и

только с их помощью, на наш взгляд, возможно ведение целостной контрпропаганды.

Мы также задали вопрос «Как, по вашему мнению, можно повысить уровень нравственного сознания членов общества?». 50% респондентов указали на необходимость проведения разъяснительных лекций и бесед с малолетними и несовершеннолетними гражданами. Большинство респондентов указало на то, что подобные мероприятия в образовательных учреждениях не проводятся. Мы согласимся с нашими респондентами, но добавим, что даже целостной системы гражданско-патриотической работы сегодня будет недостаточно. Гибридное противостояние государств и неконтролируемая, а зачастую и поощряемая ими террористическая активность в цифровой сфере, породили агрессивный идеал героя нашего времени, и для борьбы с этой триадой требуется прочная идеологическая основа в антитеррористической сфере, создаваемая совместными усилиями государства и институтов гражданского общества.

Список литературы

1. Бодрийяр, Жан. Прозрачность зла. Перевод на русский язык: Л. Любарская, Е. Марковская. — М., 2000. 111 с.
2. В.С. Соловьев, Критика отвлеченных начал, Москва 1880, с. 4; цитирую по: Л.Н. Столович, Красота, добро, истина. Очерк истории эстетической аксиологии, Москва 1994, с. 371.
3. Д.В. Новиков, А.В. Иваньков. Психология массовых коммуникаций: учебное пособие. – Комсомольск-на-Амуре: ФГБОУ ВПО «КнАГТУ», 2012. – 44 с.
4. Общество потребления / Жан Бодрийяр ; [перевод с французского Е. А. Самарской]. – Москва : Издательство АСТ, 2020. – 216 с. – (Эксклюзивная классика).

5. Овчинский А.С. Информационные воздействия и организованная преступность: Курс лекций. М.: ИНФРА-М, 2007. 176 с.

6. Поздняков Э.А. Философия культуры / Поздняков Э.А. Изд. 2-е, исправленное и дополненное. - М.: Издательство "Весь Мир", 2015. - 608 с.

Саенко А.А.

руководитель волонтерского

отряда «Антиэкстремизм», Колледж АлтГУ, г.Барнаул

Научный руководитель: Стародубцева М.А., преподаватель кафедры

уголовного права и криминологии АлтГУ

Стародубцева М.А., Саенко А.А. АНАЛИЗ ВОВЛЕЧЕННОСТИ СТУДЕНТОВ И ПРЕПОДАВАТЕЛЕЙ В КОНТРОПАГАНДИСТСКУЮ ДЕЯТЕЛЬНОСТЬ В АЛТАЙСКОМ КРАЕ

Актуальность нашего исследования заключается в том, что именно молодежь является «группой воздействия» для потенциальных вербовщиков в экстремистские и террористические объединения, поскольку обладает неустойчивым социально-психологическим фоном и не до конца сформированным мировоззрением.

В связи с этим, думается, приоритет лежит именно в среде институтов гражданского общества, напрямую работающих с молодежью. А одним из основных институтов выступает среднее и высшее образование, и именно сеть университетов может стать флагманом формирования антитеррористической идеологии и навыков противодействия терроризму и кибертерроризму.

Для подтверждения нашей гипотезы нами было проведено криминологическое исследование актуальных проблем противодействия распространения идеологии терроризма и кибертерроризма.

В период с октября по ноябрь 2020 г. Региональным антитеррористическим научно-методическим центром совместно с волонтерской организацией «Антиэкстремизм» был проведен первый этап исследования по определению проблемы уровня правового просвещения студентов СПО и преподавательского состава в вопросе профилактики идеологии терроризма и кибертерроризма.

На первом этапе в исследовании приняли участие 103 студента колледжей г. Барнаула (Колледж АлтГУ, Алтайский промышленно-экономический колледж), и 50 респондентов из числа преподавателей и учителей. Возраст респондентов первой группы 15–17 лет, возраст второй группы – 30–50 лет.

Кратко укажем основные результаты первого этапа исследования среди учащихся:

Основными причинами терроризма 38% респондентов указали целенаправленное «разжигание» представителями экстремистско-настроенных и террористических организаций националистической агрессии, 18% отметили напряженную социальную и экономическую обстановку в стране, 14% выделили низкий уровень правовой культуры и недостаточную степень толерантности населения. Можно сделать промежуточный вывод, что респонденты осведомлены о существовании в обществе данного явления, но не знают, в чем именно оно состоит, и в чем заключается основная опасность.

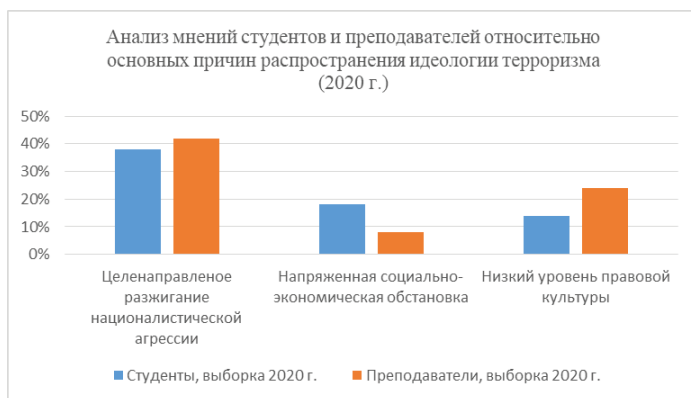


Рис. 1. Анализ мнений студентов и преподавателей относительно основных причин распространения идеологии терроризма (2020 г.)

К принимаемым государством мерам противодействия терроризму отношение у респондентов скорее положительное (32%), 29% относятся

положительно и 29% нейтрально. 10% в целом относятся к мерам по борьбе с терроризмом отрицательно. Можно предположить, что подобное отношение связано с низкой, по мнению респондентов, раскрываемостью преступлений данного вида.

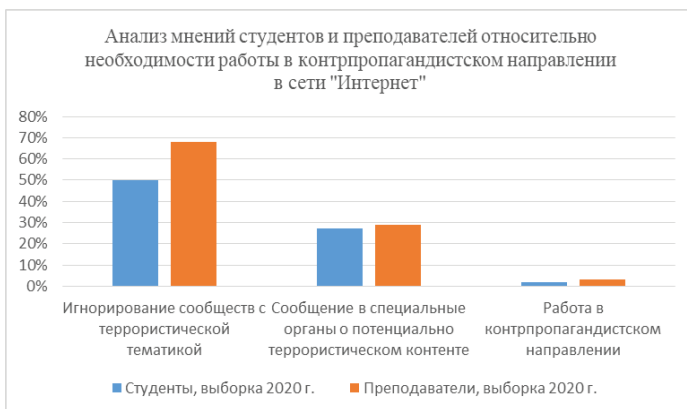


Рис. 2. Анализ мнений студентов и преподавателей относительно необходимости работы в контрпропагандистском направлении в сети «Интернет» (2020 г.)

Далее мы проанализировали мнения студентов и преподавателей относительно необходимости работы в контрпропагандистском направлении в сети "Интернет". 74% опрошенных указали, что принимают меры для ограждения себя от террористической пропаганды в сети «Интернет». 50% игнорируют сообщества с выраженной террористической тематикой. Однако, при этом не уточняются критерии признания сетевого сообщества террористическим. 27% оставляют жалобы на пользователей/сообщества/сайты, которые, на взгляд респондентов, ведут террористическую деятельность. 2% респондентов сообщили, что используют контрпропаганду. По нашему мнению, это шаг вперед в совершенствовании мер профилактики терроризма и иных деструктивных идеологий в сети «Интернет», знак участия гражданского общества в решении обозначенной нами проблемы. Однако, эта же цифра показывает нам весьма незначительное количество пользователей сети «Интернет» среди студенческой молодежи, готовых действительно бороться с

террористической пропагандой. Это означает необходимость дальнейшей работы в указанном направлении.

Основные результаты опроса среди преподавателей отражают несколько иную картину.

Основные причины терроризма, по мнению опрошенных, заключаются в целенаправленном «разжигании» представителями экстремистско-настроенных и террористических организаций националистической агрессии (42%), в низкой правовой культуре населения (24%). Это отражает осведомленность респондентов о достаточно низком уровне правовой культуры по исследуемому вопросу и желании изменить ситуацию.

Далее мы перешли к исследованию мнений относительно необходимости осуществления мероприятий по профилактике терроризма и кибертерроризма в образовательных учреждениях. Здесь, по итогам двухлетнего изучения, мы можем наблюдать заметную динамику.



Рис. 3. Анализ мнений студентов и преподавателей относительно необходимости осуществления мероприятий по профилактике терроризма и кибертерроризма в образовательных учреждениях (2020 г.)

На момент осени 2020 г. 69 % педагогов знают о программах мероприятий по профилактике экстремизма и идеологии терроризма и кибертерроризма в их образовательных учреждениях. Однако 31 % ответил отказом, что означает не вовлеченность 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 не вовлеченных 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 к этому, 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. Это означает необходимость дальнейшей работы в указанном направлении.

После подведения итогов первого этапа исследования мы приступили к организации работы с преподавателями и студентами на базе МКОУ «Гилевская СОШ» и Колледжа АлтГУ. На базе школы были проведены два гражданско-патриотических мероприятия в формате лекций, касающиеся правового просвещения учеников и преподавателей, а на базе колледжа – 8 подобных мероприятий в формате круглых столов, из них 3 для преподавателей. На базе Колледжа АлтГУ круглые столы по правовому просвещению мы сделали ежегодными и добились включения их в календарный план воспитательной работы колледжа. Также, по нашей инициативе в колледже открылась ячейка волонтерской организации юридического института АлтГУ «Антиэкстремизм», собственная волонтерская организация «АКТО», активно участвующие в процессе работы с первокурсниками колледжа в рамках гражданско-патриотического воспитания. На данный момент работа ведется полностью в цифровом формате.



Рис. 4. Анализ мнений студентов и преподавателей относительно необходимости осуществления мероприятий по профилактике терроризма и кибертерроризма в образовательных учреждениях (2021 г.)

В период с сентября по октябрь 2021 г. нами был проведен второй этап исследования – анкетирование студентов юридических специальностей СПО, ВУЗов и преподавателей по проблеме определения уровня правового просвещения в вопросе профилактики идеологии терроризма и кибертерроризма в условиях дистанционного обучения. Изменение темы исследования было осуществлено в связи с практически повсеместным введением в 2020 г. дистанционного обучения в связи с пандемией новой коронавирусной инфекции, повлекшей ухудшение эпидемиологической обстановке в Российской Федерации и в Алтайском крае, в частности.

Методом случайной выборки было опрошено 107 респондентов – учащихся юридических направлений колледжей г. Барнаула (Колледж АлтГУ, Алтайский промышленно-экономический колледж). Возраст респондентов 15-17 лет.

По данным нашего исследования, мы можем увидеть, что перевод обучения на онлайн-рельсы достаточно сильно ударил по уровню мотивации и собранности студентов, их готовности фактически самостоятельно осваивать большие объемы учебного материала. Естественно, дистанционный формат повлиял и на сферу гражданско-патриотического воспитания студенческой молодежи на базе колледжей и техникумов.

29% респондентов указали, что в их учебных заведениях проводятся мероприятия по противодействию идеологии терроризма и кибертерроризма, причем проводятся в очном формате. Сразу же можно отметить, что при очном проведении массовых мероприятий в период пандемии допускается одновременное размещение в одной аудитории не более 40 человек, что означает невовлеченность в подобные мероприятия большей части студентов СПО. 15% сообщили, что подобные мероприятия проводятся в онлайн-режиме, и это указывает на постепенную адаптацию образовательных учреждений к дистанционному формату обучения. Однако, пока достигнутый уровень адаптации недостаточен, поскольку 46% респондентов сообщили, что

гражданско-патриотические мероприятия по профилактике идеологии терроризма и кибертерроризма в их учебных заведениях не проводятся, а еще 10% вообще не осведомлены о подобных мероприятиях.

Когда мы реализовали первый этап исследования, похожая картина наблюдалась при опросе учителей и преподавателей, не соглашавшихся проводить в своих классах, кураторских группах якобы необязательные лекции и семинары по вопросу профилактики терроризма. При этом, учащиеся о подобных мероприятиях были осведомлены. Сегодня ситуация изменилась, мы видим, что в условиях онлайн-режима обучения далеко не вся информация может быть вовремя доведена до сведения обучающихся, что говорит о затрудненном взаимодействии преподавателей и студентов на уровне СПО.

78% респондентов сообщили, что не принимали участие в подобных мероприятиях, и это еще раз подтверждает ранее озвученный нами тезис.

Из тех респондентов, что присутствовали на антитеррористических мероприятиях, 24% отметили свой интерес к происходящему, 12% сообщили о необязательности и скучности подобных лекций. 64% отметили, что на подобных мероприятиях не присутствовали. Возможно, это означает необходимость перевода гражданско-патриотических антитеррористических мероприятий в другую форму, отход от традиционной лекции в пользу видеодемонстрации или общения с волонтерами антитеррористических отрядов. Подобный опыт работы с 2020 г. внедряется в Колледже ФГБОУ ВО «Алтайский государственный университет», однако, пока мы не видим достаточной массовости данных мероприятий в связи с введенными в Алтайском крае коронавирусными ограничениями.

Необходимо отметить, что 70% респондентов все же сообщили об эффективности подобных мероприятий, что говорит о заинтересованности молодежи работать в антитеррористическом направлении.

41% респондентов считают, что работа институтов гражданского общества в сфере профилактики идеологии терроризма и кибертерроризма состоит в совершенствовании информационно-пропагандистской и

воспитательной работы, направленной на профилактику и предупреждение террористических и кибертеррористических проявлений, 35% выступают за совершенствование системы профилактических мер, направленных на противодействие терроризму. 15% предлагают устранение предпосылок и условий возникновения террористических и кибертеррористических проявлений в качестве основной сферы работы гражданского общества, и 8% выступают за вовлечение учащихся и родителей в процесс участия в противодействии террористическим и кибертеррористическим проявлениям. 25% респондентов выразили желание участвовать в подобной работе и это мы считаем основным результатом проведенных исследований. Мы можем проследить яркую динамику роста интереса молодежи к профилактике терроризма и кибертерроризма. Если на первом этапе нашего исследования только 2% учащихся юридических специальностей СПО были готовы работать в антитеррористической сфере деятельности гражданского общества, то сейчас эта цифра выросла почти в 10 раз. 57% затруднились с ответом на данный вопрос и 18% респондентов ответили отказом, что означает необходимость продолжения работы в указанном направлении.

Аналогичный опрос мы провели среди студентов юридического института ФГБОУ ВО «Алтайский государственный университет». Опрошены были студенты 1-4 курсов в возрасте от 18 до 22 лет. В анкетировании приняло участие 63 человека.

46% опрошенных сообщили, что мероприятия по противодействию идеологии терроризма и кибертерроризма в их учебном заведении не проводятся, и 7% о них не знают вообще. Здесь мы можем увидеть необходимость расширения рекламы антитеррористической деятельности среди молодежи. Представителям поколения «клипового» мышления нужен яркий бренд в звучной упаковке, и подобный эффект должен быть достигнут массивным продвижением хэштега «антитерроризм» на базе сайтов либо страниц юридических институтов в социальных сетях. Плюс, это также база будущих абитуриентов. 21% сообщили, что антитеррористические мероприятия

проводятся очно, 24% отметили онлайн-взаимодействие с преподавателями по указанному вопросу. Как мы видим, картина взаимодействия учеников и преподавателей ВО и СПО примерно совпадает. И также, как и на уровне колледжей, 78% студентов-юристов сообщили, что не принимали участие в мероприятиях гражданско-патриотического толка.

Тем не менее, из присутствовавших на подобных акциях, 32% отметили интерес к поданному материалу, что больше, чем на уровне СПО (24%). Думается, это можно объяснить тем, что студенты бакалавриата несколько в большей степени владеют информацией в сфере понимания терроризма и кибертерроризма. Однако, как показывают наши данные, даже этот уровень на сегодняшний день недостаточен, и дело, фактически, пущено на самотек.

Также, как и на уровне колледжей, 70% респондентов указали на эффективность подобных мероприятий, что сообщает о готовности действовать в антитеррористическом направлении.

35% респондентов уверены, что работа институтов гражданского общества в сфере профилактики идеологии терроризма и кибертерроризма состоит в совершенствовании системы профилактических мер, направленных на противодействие терроризму. Идентичный результат был характерен и для студентов колледжей. 33% предлагают устранение предпосылок и условий возникновения террористических и кибертеррористических проявлений. Это более чем в два раза выше результата СПО (15%), что говорит об определенных знаниях студентами сложившейся системы противодействия деструктивным идеологиям в обществе и знании криминологической характеристики указанных видов преступности. Студенты проявляют интерес к информации, но, вследствие неприученности к самостоятельному анализу, достаточно быстро его утрачивают, расплываясь на более конкретные и понятные им аспекты деятельности.

Тем не менее, здесь также видна динамика роста интереса молодежи к профилактике терроризма и кибертерроризма от менее 2% до 32% за полтора года исследований. Однако, 19% сообщили, что не собираются участвовать в

борьбе с терроризмом и кибертерроризмом, что показываем нам, по сути, поведенческий абсентеизм, осознанный и целенаправленный. Почти треть студентов бакалавриата не желает занять какую-либо активную гражданскую позицию в обществе, а учитывая популярность юридических специальностей и вес юриспруденции в обществе подобная ситуация недопустима и требует корректировки.

На втором этапе нашего исследования мы также провели опрос среди преподавателей юридических дисциплин Колледжа АлтГУ и юридического института АлтГУ. Опрошено было 35 человек, возраст 35-50 лет.

60% респондентов знают о мероприятиях по профилактике идеологии терроризма и кибертерроризма, которые проводятся в их образовательном учреждении, и 57% из них принимают активное участие в подобных мероприятиях. Эти результаты отражают яркую динамику по сравнению с данными конца 2020 года, когда фактически 79,3% преподавателей сообщили нам, что, либо не знают о проводимой в ОУ гражданско-патриотической работе, либо не собираются в ней участвовать. На сегодняшний день, как мы видим, ситуация значительно переменялась в лучшую сторону. 37% отметили, что сами проводят антитеррористические лекции и круглые столы в очном формате, 31% - в онлайн-режиме. 46% сообщили, что им удалось вовлечь в подобные мероприятия студентов собственных кураторских групп. Они же оценивают данные мероприятия как достаточно эффективные.

Также необходимо отметить, что 73% преподавателей изъявили желание участвовать и в дальнейшем в реализации контрпропагандистской и гражданско-патриотической работы с молодежью, что означает, по нашему мнению, определенный шаг к созданию целостной системы патриотического воспитания в регионе.

Как ожидалось, рост вовлечения преподавателей в цифровую среду должен повлечь за собой рост правового просвещения и обучаемой ими молодежи. Этот тезис в полной мере подтверждается результатами нашего исследования.

**СЕКЦИЯ «НАУЧНО-ПРАВОВЫЕ ПРОБЛЕМЫ
ПРОТИВОДЕЙСТВИЯ ТЕРРОРИЗМУ В ЦИФРОВУЮ ЭПОХУ: ВЗГЛЯД
СТУДЕНТОВ»**

Застрожнов М.С., магистрант Юридического
института АлтГУ, г. Барнаул

Научный руководитель: Мазуров В.А., кандидат юридических наук,
доцент кафедры уголовного права и криминологии АлтГУ

**Застрожнов М.С. ПАТРИОТИЗМ, КАК ОСНОВА
КОНТРТЕРРОРИСТИЧЕСКОЙ ПРОФИЛАКТИКИ**

Современная практика показывает, что контртеррористическая пропаганда, которая ведется в России в настоящий момент, не очень эффективна. И проблема не в плохом выполнении задач, а в том, что осуществляющие эту пропаганду люди, организации связаны законами и некими правилами, в то время как наши оппоненты никакими правилами не связаны [1]. Сегодня нам жизненно необходимы социальная стабильность, поступательное развитие страны и устойчивость к внешним влияниям, а также консолидация всех граждан и народов, населяющих нашу страну. Все это обеспечило бы рост экономики, укрепление российской государственности, рост качества жизни граждан нашей страны. По сути, речь идет о формировании национальной идеологии.

У нас часто недооценивают роль идеологии в жизни общества, а ведь ее наличие, вырабатывает у граждан государства типы мышления и поведения содействующие укреплению государственности. В связи с чем, отсутствие у людей общих идей и взглядов, делает их идеологически уязвимыми, что в свою очередь, привлекает внимание вербовщиков террористических организаций.

Террористы-вербовщики ведут свою работу планомерно, независимо от терактов и военных действий. Их цель — мировая религиозная революция.

Вербовщики действуют по отработанным технологиям, активно используя в этих целях Интернет. Как показывают результаты мониторинга СМИ и признаний пострадавших, опубликованных в прессе, в большинстве случаев пропаганда радикальных идей и вербовка происходит преимущественно популярных социальных сетях Facebook, ВКонтакте, Twitter и др. Подобные негативные тенденции в Интернете усилились на фоне сирийского кризиса и активизации ИГИЛ (Террористическая организация запрещенная в РФ). Именно эта организация одной из первых создала административные структуры со штатом блогеров для ведения целенаправленной работы в Интернете, привлечения новых рекрутов и распространения идеологии терроризма.

Разберемся подробнее, кто же попадает в «зону риска» быть завербованным.

Муфтий Москвы и Центрального региона, член Общественной палаты РФ Альбир Крганов считает, что вербовщики достигают своих целей там, «где есть большое количество несправедливо обиженных людей». По его словам, даже сами террористические акты в числе прочего работают на информационное воздействие на будущих потенциальных членов организации. Позже среди этих людей найдутся те, кто будет готов пойти на страшные преступления во имя высших целей [2]. Сам Крганов напоминает, что традиционные религиозные конфессии не могут быть радикальными, что «никакие небесные религии не признают насилие и убийства».

Директор Центра этнополитических и региональных исследований Владимир Мукомель считает, что наиболее «чувствительной» к призывам вербовщиков ИГИЛ является молодежь, которая очень бурно и эмоционально реагирует на проявление социальной несправедливости, что и толкает некоторых на радикальные действия.

Почему среди молодежи так много людей становятся жертвами террористических группировок? Выделяют несколько причин:

- низкая самооценка;

- зависимость от чужого мнения;
- проблемы в семье;
- сильная потребность в восстановлении справедливости в мире;
- ощущение потерянности и чувство одиночества.

Подростки могут найти поддержку и понимание в лице вербовщика, который будет делать для него всё до тех пор, пока тот не окажется в смертельной ловушке.

Противодействие терроризму является насущной проблемой в настоящее время не только в Российской Федерации, но и во всем мировом сообществе в целом и требует от органов государственной власти всех уровней принятия решительных, эффективных мер и согласованных действий, направленных на предупреждение и пресечение любых форм его проявления.

На наш взгляд, правовая основа и деятельность государственных органов в контртеррористической борьбе не стоит на месте. Проблемы в борьбе с терроризмом обуславливаются тем, что перед государством и его органами стоит ряд проблем, в различных сферах и проявлениях, что делает невозможным уделять необходимое количество средств для борьбы с данным явлением.

Считаем, что в основе профилактики и борьбы с терроризмом, наряду с установленной законодательством Российской Федерации ответственностью; пропагандой этой ответственности, и всевозможных лекций в образовательных учреждениях различного уровня, прежде всего должна быть общественная идея. Содержанием которой будет объединение всех граждан нашего государства, воспитание в человеке чувства любви к родине, преданности своему делу, товарищество и братство. Одним словом – это патриотизм. На протяжении всей нашей истории, именно он был одной из основных причин, которая могла бы сплотить наш народ, помочь преодолевать трудности и проблемы.

Знаменитый отечественный филолог С.И. Ожегов понимает сущность патриотизма как «преданность и любовь к своему Отечеству, к своему народу»

[3]. По мнению авторов Философского словаря, составленном под редакцией И.Т. Фролова рассматриваемое понятие трактуется как нравственный и политический принцип, социальное чувство, содержанием которого является любовь к отечеству, преданность ему, гордость за его прошлое и настоящее, стремление защищать интересы родины. Военно-энциклопедический словарь объясняет рассматриваемое понятие патриотизм шире, как «любовь к родине, своему народу, стремление своими действиями служить их интересам».

Говоря о нашем времени, актуальной проблемой является воспитание чувства патриотизма у молодежи. В новостях периодически можно встретить информацию о том, что молодежь буянит по различным поводам связанными с современной культурой. Это говорит о том, что в них нет патриотизма. Таких людей нельзя назвать патриотами, потому что они не знают и не понимают его содержания и почему он так важен для современного общества. Примером может служить инцидент произошедший в Евпатории. 23 ноября 2021 года в полицию поступило сообщение о том, что неизвестные лица привязали к памятнику-бюсту С. М. Кирову (советский государственный и политический деятель) автомобильную шину и разрисовали его нацистской символикой – свастика и нацистский крест – говорится в сообщении. В результате оперативно-розыскных мероприятий сотрудникам полиции удалось установить и задержать виновных лиц – подростков 17, 18 лет. Еще один вопиющий случай произошел в Москве. Следственными органами Главного следственного управления Следственного комитета Российской Федерации по городу Москве возбуждено уголовное дело по признакам преступления, предусмотренного ч. 4 ст. 354.1 УК РФ (осквернение символов воинской славы России, оскорбление памяти защитников Отечества, совершенные публично) [4]. По данным следствия, молодой человек, находясь на территории Восточного административного округа города Москвы, осквернил объект, посвященный памяти защитникам Отечества. Им оказался 19-летний блогер, который разместил в своем аккаунте Instagram видео, на котором видно, как он мочится на стенд содержащий информацию о ветеране Великой отечественной войны. А

ведь социальные сети, на сегодняшний день, являются самым мощным источником информации, конечно не всегда достоверным, но при правильном использовании, его можно использовать в профилактике терроризма.

Алексей Алексеевич Филатов — советский и российский военнослужащий, подполковник ФСБ, сотрудник Управления «А» Центра специального назначения ФСБ России. Вице-президент Международной ассоциации ветеранов подразделения «Альфа» по вопросам информационного сопровождения, связям с общественностью и военно-патриотическому воспитанию молодежи. В своих аккаунтах в социальных сетях и на сайте освещает проблему терроризма. Помимо анализа террористических актов, оценки контртеррористических операций, возможных путей решения проблемы терроризма, всегда делает акцент на том, что главная роль в борьбе с ним, должна отводиться именно профилактике.

Ярким примером служит задержание 7 декабря текущего года, вооруженного 18-летнего молодого человека, возле школы № 1297, в Москве. Перед этим в своем аккаунте, он разместил запись о планах устроить теракт в школе. Департамент образования при мониторинге соц. сетей обнаружил запись и передал информацию в МВД. Удалось избежать последствий как в Казани и Перми, из чего следует вывод, что профилактические мероприятия работают.

Патриотизм, как связующее целое различных социальных групп, граждан в единое целое, имеет свои функции. Н.М. Ильичевым выделяются: мировоззренческая, методологическая, коммуникативная, регулятивная, ценностная [5]. Посредством их реализации патриотизм и выполняет свое социальное назначение. Помимо названных, представляется обоснованным выделение и других функций патриотизма: познавательная, мобилизационно - побудительная, воспитательная, интегративная.

Дадим им более подробную характеристику. Мировоззрение, как известно, представляет собой систему наиболее общих взглядов человека на мир и на свое место в нем. Основное заключается в понимании своего места в

родной стране и положительном отношении к ней. А это, собственно говоря, и есть патриотический срез мировоззрения. Поэтому патриотизм, безусловно, способствует формированию мировоззрения личности.

Методологическая функция патриотизма заключается в том, что использование имеющихся в нем знаний способствует осуществлению духовной и практической деятельности по преобразованию социальной жизни.

Познавательная функция связана, прежде всего, с основным структурным элементом сознания - знанием. Но не только с ним, а, так или иначе, со всеми элементами сознания. Генезис патриотического сознания связан с познавательным этапом, когда его первоначальными компонентами становятся патриотические знания, суждения, мысли, идеи, представления об Отечестве. Патриотическое познание осуществляется в тех же формах, в каких существует знание. Знания об Отечестве первоначально накапливаются на обыденном уровне сознания граждан, затем закрепляются на теоретическом уровне, и в этом смысле предвосхищают патриотическое отношение и патриотическую деятельность, как элементов патриотизма.

По мнению Н.М. Ильичева, ценностная функция выражается в том, что положения патриотического содержания являются теми критериями, которые обеспечивают определенные качества, направленность поступков, как отдельных людей, так и различных социальных групп. Именно благодаря ценностной функции, становится возможным выявлять всевозможные антипатриотические настроения, периодически появляющиеся в СМИ.

Существенна и мобилизационно-побудительная функция, которая выражается в том, что любовь к Родине вдохновляет и побуждает человека к патриотической деятельности, к служению обществу. Наиболее ярко это проявляется в системе военной службы, когда происходит мобилизация всех сил на защиту Отечества, на преодоление трудностей военного дела и достижение конкретных результатов в бою.

Регулятивная функция выражается в добровольном выполнении личностью, различными социальными группами патриотических норм и

принципов, обуславливающих развитие страны. Она проявляется в том, что патриотизм выступает одним из мощных универсальных средств регулирования деятельности, как отдельных людей, так и многочисленных коллективов. При этом выражается способность социальных субъектов определять соответствие своих действий интересам Отечества.

Не менее значима и воспитательная функция патриотизма, реализующаяся в процессе формирования у граждан качеств гражданина-патриота. Примеры реализации воспитательной функции патриотизма имеются во все времена и у всех народов. Ярким примером является российская армия, где всегда уделялось серьезное внимание воспитанию воинов в духе любви и преданности Отчизне. Известный военный педагог М.И. Драгомиров писал: «...самоотвержение не берется, оно дается. Это есть равнодействующая всего склада жизни и занятий. Там, где человек любит свою Родину, любит свою часть; там, где вследствие этого общее дело становится его личным делом, где оскорбление или неудача его Родины - его личная неудача, - там он не задумывается жертвовать собою для их блага» [6].

Коммуникативная функция, по мнению Н.М. Ильичева, проистекает из того, что патриотизм сплачивает, объединяет людей для решения наиболее кардинальных задач и проблем общественной жизни.

Подытоживая сказанное, согласимся с утверждением о том, что патриотизм представляет собой важнейший ресурс сохранения и развития российского общества. Реалии сегодняшней жизни свидетельствуют о необходимости воссоздания действенной системы патриотического воспитания, вобравшей в себя все самое ценное из накопленного опыта. Именно эта объединяющая, граждан, идея поможет противостоять такой угрозе как терроризм и сопровождающими ее проблемами .

Список литературы

1. Официальный сайт Главного следственного управления Следственного комитета по городу Москве [Электронный ресурс] URL: <https://moscow.sledcom.ru/> (дата обращения 15.11.2021)

2. Кузьмин А.В., Трифанов Ю.Н. Значение патриотизма в жизни российского общества: функциональный подход [Электронный ресурс] URL: <https://cyberleninka.ru/article/n/znachenie-patriotizma-v-zhizni-rossiyskogo-obshchestva-funktsionalnyy-podhod> (дата обращения 15.11.2021)

3. Алексей Филатов [Электронный ресурс] URL: <https://alfafilatov.com> (дата обращения 07.12.2021)

4. Силантьев Р.А. Новые подходы к антитеррористической пропаганде. Выступление на III Всероссийской научно-практической конференции. Москва, 18-19 октября 2012 года [Электронный ресурс] URL: <http://nac.gov.ru/publikacii/vystupleniya-i-intervyu/silantev-ra-novye-podhody-k.html>

5. Драгомиров, М.И. Избранные труды. Вопросы воспитания и обучения войск / Под ред. Л.Т. Бескровного. - М.: Воениздат, 1956. – 433 с.

6. Ильичев, Н.М. О сущности, содержании и значении патриотизма / Н.М. Ильичев // Вестник Российского философского общества. 2003. №3. С.84-89.

7. Военный энциклопедический словарь / В 2 томах. Том 1. – Редкол.: А.П. Горкин, В.А. Золотарев, В.М. Карев и др. – М.: Большая Российская энциклопедия, «РИПОЛ КЛАССИК», 2001.

Аксенова А.Д., Домбровская А.А.

Колледж АлтГУ, г. Барнаул

Научный руководитель: Стародубцева М.А., преподаватель кафедры
уголовного права и криминологии АлтГУ

Аксенова А.Д., Домбровская А.А. ВИДЫ ПРЕСТУПЛЕНИЙ В СФЕРЕ ЦИФРОВОЙ ИНФОРМАЦИИ

В настоящее время с развитием цифровых технологий всё большее распространение получают преступления в сфере цифровой информации. Изменяется технологический уклад, а также развитие робототехники и искусственного интеллекта ведет к трансформации производств и колоссальным сдвигам трудовых ресурсов. Угасают некоторые привычные и приходят новые, неизвестные ранее профессии. Стремительные изменения всего увеличивают риски преступлений. Люди становятся всё более уязвимыми и беззащитными. Каждого из нас можно подслушивать, за каждым можно подглядывать через телефон, ноутбук или же компьютер. Отслеживать с помощью камер видеонаблюдения и другого оборудования наши перемещения, взаимодействия с другими людьми.

В теории и практике нет единого определения таких преступлений. Всеобщее развитие цифровых технологий обостряет данную проблему и вызывает необходимость разработки соответствующей государственной политики. Опасность таких преступлений заключается не только в масштабах пагубных воздействий, но и в возрастании их количества. В последние годы замечается парадокс кибертерроризма, который способен нападать на объекты жизнеобеспечения и имеет возможность привести к большому количеству жертв и разрушений.

Преступники становятся более смышлёнными и опытными, используют новейшие технические решения и программное обеспечение, а также использование технических приспособлений позволяет преступникам

эффективно координировать свои действия и избегать ответственности. С другой стороны, техническое и программное обеспечение правоохранительных органов, которые расследуют киберпреступления, не совершенствуется со временем, что приводит к сложностям при расследовании

Понятие и виды преступлений в сфере цифровой информации

Определение киберпреступности было дано еще в 2000 году, когда проводилась работа сессии десятого Конгресса ООН по предупреждению преступности и уголовному правосудию. Тогда же было признано, что компьютерное преступление касается любого преступного деяния, «которое может совершаться с помощью компьютерной системы или сети, в рамках компьютерной системы или сети или против компьютерной системы или сети. Оно охватывает любое преступление, которое может совершаться в электронной среде».

Подобные преступления также часто называют «компьютерными». Уголовно-правовая наука содержит ряд позиций, которые определяют понятие преступления в сфере цифровой информации. Например, Л.Е. Шведова и В.А. Номоконов в состав компьютерных преступлений включают те деяния, где компьютер — это объект или орудие совершения преступления. Другие авторы относят к компьютерным преступлениям только ряд неправомерных действий в сфере обращения информации, которая циркулирует в информационно-телекоммуникационных системах. Существует и третья точка зрения, в соответствии с которой компьютерные преступления — это информационные преступления[1].

Виды преступлений в сфере цифровой информации

Совет Европы принимает значительные усилия по приведению к единообразию законодательств стран – участниц в сфере правового регулирования компьютерных преступлений.

Исторически первым нормативным актом Совета Европы, посвященным вопросам регулирования киберпреступности, была Рекомендация № R 89 (9) Комитета Министров стран – членов Совета Европы о преступлениях,

связанных с компьютерами, принята 13 сентября 1989 г. В соответствии с данным документом государствам – членам Совета Европы надлежит при разработке национального законодательства принять во внимание Отчет Европейского комитета по проблемам преступности о преступлениях, связанных с компьютерами. В рамках данного Отчета Комитет по проблемам преступности дал оценку явлению компьютерной преступности и представил руководящие указания для криминализации противоправных деяний в законодательстве стран – участниц.

Преступления, совершаемые с использованием компьютерных технологий, разделяют на два перечня: минимально необходимые к включению в национальное законодательство и дополнительные.

К минимально необходимым преступлениям относятся:

1. Компьютерное мошенничество, которое определяется как ввод, изменение или удаление данных или программ компьютера или иное вмешательство в процессы обработки данных, влияющее на итоги обработки данных, которое причиняет экономический ущерб или приводит к уничтожению собственности другого лица, совершаемое с целью получения незаконным путем экономической выгоды для себя или для другого лица.

2. Компьютерный подлог, т. е. ввод, изменение или удаление данных (программ) компьютера либо другое вмешательство в процесс обработки данных, совершенное способом или при условиях, установленных нормами национального законодательства, которыми эти деяния квалифицируются как подлог, и совершены в отношении традиционного объекта правонарушения.

3. Причинение ущерба компьютерным данным или компьютерным программам, т. е. незаконное удаление, причинение ущерба или ухудшение качества данных или программ компьютера.

4. Компьютерный саботаж: ввод, изменение или удаление данных или программ компьютера, или создание помех компьютерным системам с целью воспрепятствования работе компьютера или телекоммуникационной системы.

5. Несанкционированный доступ, представляющий неправомерный доступ к системе или компьютерной сети путем нарушения мер охраны.

6. Несанкционированный перехват, т. е. неправомерный и осуществленный с применением технических средств перехват сообщений, направленных в систему или сеть компьютеров, исходящих из системы или сети компьютеров и передаваемых в рамках системы или сети компьютеров.

7. Несанкционированное воспроизведение компьютерной программы, охраняемой авторским правом. Под ним понимается совершенное неправомерно распространение, воспроизведение или передача в общественное пользование компьютерной программы, охраняемой законом

8. Несанкционированное воспроизведение микросхемы, т. е. совершенное неправомерно воспроизведение микросхемы изделия на полупроводниках, если она охраняется законом, либо неправомерное использование или импорт в коммерческих целях микросхемы или изготовленного с ее применением изделия на полупроводниках.

Дополнительный перечень правонарушений в соответствии с

Отчетом включает в себя следующие составы противоправных деяний:

1. Неправомерное изменение данных или программ в компьютере.

2. Компьютерный шпионаж, который в соответствии с Рекомендацией определен как получение незаконными способами или раскрытие, передача или использование торговой или коммерческой тайны лицом, не имеющим на это прав или какого-либо иного законного основания, с целью причинения экономического ущерба лицу, имеющему доступ к этой тайне, или получения незаконной экономической выгоды для себя или третьего лица.

3. Несанкционированное использование компьютера – это незаконное использование системы или сети компьютеров, которое совершается: а) лицом, которое имеет право использовать систему, с осознанием того, что действия этого лица увеличивают риск причинения ущерба системе или ее функционированию либо причиняют такой ущерб; б) любым лицом с целью

причинения ущерба управомоченному пользователю системы, функционированию системы или самой системе; в) любым лицом с фактическим причинением ущерба системе в целом, функционированию системы или управомоченному пользователю системы.

4. Несанкционированное использование компьютерной программы, охраняемой законодательством: неправомерное использование охраняемой законом компьютерной программы либо воспроизведение без права на это, совершаемые с целью получения незаконной прибыли для злоумышленника или третьих лиц либо причинения правообладателю ущерба.[2]

Ответственность за преступления в сфере компьютерной информации предусмотрена в главе 28 Уголовного Кодекса РФ

1. Неправомерный доступ к компьютерной информации (ст. 272 УК РФ). Это один из часто встречающихся видов преступления в киберсфере. Информация, доступ к которой запрещен посторонним, может составлять государственную, банковскую, врачебную, служебную или иную тайну. Для невозможности посторонним лицам воспользоваться сведениями устанавливается специальная защита, особое программное обеспечение, система паролей и кодов. Несанкционированный доступ к любой охраняемой информации на компьютерах или носителях может стать основанием для привлечения в качестве обвиняемого, если это повлекло: уничтожение данных (приведение системы в состояние, которое исключает ее использование по назначению); блокировку (становится невозможным правомерный доступ к программе); модификацию (внесение изменений в программу, в текст с информацией и др.); копирование охраняемой информации (на любые носители: бумажный, флеш-карту и т.д.). В зависимости от признаков преступления виновному может быть назначено от штрафа 200000 рублей до лишения свободы до 7-ми лет.

2.Создание вредоносных программ (ст. 273 УК РФ). Такой вид преступления в сфере компьютерной информации тоже распространен, есть множество примеров уголовных дел. Речь идет о намеренном создании таких

компьютерных продуктов (программ, комбинаций), с помощью которых можно: блокировать; уничтожить; модифицировать; копировать информацию, безопасность которой охраняется. Кроме того, создатель таких вредоносных программ может преследовать цель отключения защиты, которая специально установлена в целях обеспечения безопасности тех или иных сведений. По ст. 273 УК РФ, может быть назначено следующее наказание: от ограничения свободы на срок 4 года, до лишения свободы на срок до 5-ти лет со штрафом от 100000 до 200000 рублей.

3.Нарушение правил хранения компьютерной информации (ст. 274 УК РФ). Данный вид преступления может быть и бездействием. В ст. 274 УК РФ предусмотрена ответственность должностных лиц, на которые возложены обязанности по правильному: хранению; эксплуатации (использованию); обработки; передачи компьютерной информации. В статье не отражены требования, которые должны быть соблюдены теми или иными должностными лицами. В каждом конкретном деле нужно обращаться к федеральным законам, должностным инструкциям, уставам, в которых подробно указан порядок обращения с информацией. Виновному лицу может быть назначено следующее наказание: от штрафа 500000 рублей, до лишения свободы сроком на 5 лет.

В статье 274.1 УК РФ объединены различные формы совершения компьютерных преступлений: неправомерный доступ, создание вредоносных программ и т.д., с той разницей, что все эти действия совершаются относительно критической информационной инфраструктуры страны. Поскольку данный состав преступления подразумевает угрозу безопасности государства и населения, расследованием таких дел занимаются сотрудники ФСБ. Наказание может достигать 10 лет лишения свободы.

Заключение

Мы живем в эпоху информационного общества, и наша жизнь тесно связана с различными технологиями и сетью Интернет. И практически каждый раз, взаимодействуя с компьютерными технологиями, мы подвергаем себя

угрозе стать жертвой киберпреступников. Поэтому всестороннее изучение компьютерных преступлений позволит разработать эффективные меры по их предупреждению и расследованию. Защита информации является ключевой задачей в современных условиях взаимодействия глобальных и корпоративных компьютерных сетей. В реальном мире много внимания уделяется физической безопасности, а в мире электронного обмена информацией необходимо заботиться также о средствах защиты данных.

Список литературы

1. Бегишев, И. Р. БЗ7 Преступления в сфере обращения цифровой информации / И. Р. Бегишев, И. И. Бикеев – Казань: Изд-во «Познание» Казанского инновационного университета, 2020. – 300 с. (Серия «Цифровая безопасность»).

2. Криминология интернет-пространства УДК 343.9 ББК 67.51 В.А. Номоконов, Т.Л. Тропина. Киберпреступность как новая криминальная угроз.

3. Попов, А. Н. Преступления в сфере компьютерной информации : учебное пособие / А. Н. Попов. — Санкт-Петербург : Санкт-Петербургский юридический институт (филиал) Университета прокуратуры Российской Федерации, 2018. — 68 с.

4. Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий : учебное пособие : в 2 ч. / [А. В. Аносов и др.]. – М. : Академия управления МВД России, 2019. – Ч. 1. – 208 с.

5. Уголовный кодекс Российской Федерации [Электронный ресурс] : федер. закон : [принят Гос. Думой 24 мая 1996 г. : по состоянию на 18 февраля 2019 г.] // Справ.-правовая система «Консультант Плюс». – М., 1997.

6. <https://admber.ru/reporting/prestupleniya-v-sfere-kompyuternyih-tehnologii-prestupleniya-v.html>

7. <https://finance-credit.news/dlya-ekonomistov-informatika/ugrozyi-bezopasnosti-metodyi-51078.html>

Колесниченко Е.И., магистрант Юридического
института АлтГУ, г. Барнаул

Научный руководитель: Мазуров В.А., кандидат юридических наук,
доцент кафедры уголовного права и криминологии АлтГУ

Колесниченко Е.И. ПРОФИЛАКТИКА И ПРОТИВОДЕЙСТВИЕ КИБЕРПРЕСТУПНОСТИ

Причины и условия преступности в целом и отдельных категорий преступности являются одной из фундаментальных категорий, изучаемых наукой криминологией.

Затрагивая тему причины появления той или иной преступности необходимо разобраться с определением. Многие авторы в своих трудах предлагали свои варианты раскрытия данного понятия, но, на мой взгляд, одним из наиболее полных определений является следующее - «причинами преступности называется совокупность социальных явлений и процессов, которые во взаимодействии с обстоятельствами, играющими роль условий, детерминируют существование преступности как социального явления, наличие отдельных составных ее частей, а на индивидуальном уровне – совершение конкретных преступлений» [1]. Другими словами, причины, в едином комплексе с условиями преступности, выступают в качестве порождающих преступность детерминант, именуемых также в науке факторами преступности.

Как указывается специалистами, «условиями преступности являются различные явления социальной жизни, которые не порождают преступность, но содействуют, способствуют ее возникновению и существованию. Причина создает возможность определенного следствия. Условия же способствуют реализации этой возможности».[2]

О соотношении категорий причин и условий преступности в науке есть множество дискуссий, однако, авторы едины во мнении о том, что причины и

условия, выступая в качестве детерминант преступности, действуют не в отрыве друг от друга, а в комплексе, обуславливая преступность.

Вопрос о причинах и условиях киберпреступности относится к разряду неоднозначных и дискуссионных. Киберпреступность, как отмечается отдельными авторами, с одной стороны, порождается теми же причинами и условиями, что и преступность вообще. С другой стороны, она имеет свои сугубо специфические причины и условия вследствие ее особенностей.[3]

К числу детерминант киберпреступности можно отнести:

- широкую распространённость и всё большую доступность информационных технологий;

- растущее число пользователей глобальной сети «Интернет» как в мире, так и в Российской Федерации.

- возрастающую зависимость функционирования отдельных сфер общественной жизни (социальной, экономической и т.д.) от современных информационных технологий;

- рост в структуре национальной экономики торговли и оказания услуг через электронные (компьютерные) средства телекоммуникации (в частности, Интернет-торговля);

- стремительное развитие информационных технологий, сопряжённое с возникновением новых технологий и средств доступа в сеть «Интернет».

- несовершенство средств защиты информации в сети «Интернет» при использовании информационно-коммуникационных технологий в отдельных процессах, равно несовершенство средств защиты телекоммуникационных систем и их сетей и т.д.

Эффективному же противодействию совершению киберпреступлений препятствует, как отмечается в отдельных работах:

- отсутствие скоординированной и комплексной государственной политики в сфере обеспечения информационной безопасности;

- несоответствие темпа развития средств выявления и противодействия киберпреступлениям объективным темпам развития средств и способов

совершения противоправных посягательств, а также сокрытия следов данных посягательств;

– возможность совершения преступных посягательств в сети «Интернет» из любой точки планеты, имея доступ к сети и соответствующее устройство, обеспечивающее доступ в сеть и возможность использования необходимого для этого программного обеспечения;

– обезличенность (анонимность) взаимодействия, осуществляемого через сеть «Интернет», возможность скрывать индивидуализирующие пользователя сети данные о местонахождении, точке доступа в сеть;

– низкий уровень специальной подготовки сотрудников правоохранительных органов, которые должны предупреждать, раскрывать и расследовать преступления в сфере информационных технологий и т.д.

Профилактика преступности в сфере Интернете (киберпреступности) включает в себя комплекс разноплановых мер, включая меры предупреждения совершения киберпреступлений. Именно этот аспект противодействия киберпреступности наиболее полно представлен в современных научных публикациях, с учётом того, что недопущение совершения конкретных киберпреступлений, посредством эффективного предупреждения данных преступлений – желаемый в обозначенном направлении результат. Реагирование на уже совершённое преступление – вынужденная мера, находящаяся на последующем этапе противодействия, когда меры предупреждения оказались не эффективными и преступление (или покушение на его совершение) всё же состоялось.

Как отмечается отдельными исследователями, «основные направления профилактики киберпреступности сегодня должны быть нацелены на решение проблем, связанных с расширением законодательства, выработкой мер предупреждения и снижением уровня латентности преступлений, совершаемых в киберпространстве» [4].

Без сомнений, главным звеном регулирования подобной деятельности может и должно выступать государство в лице соответствующих органов,

наделённых властными полномочиями, так как именно государство реализует правоохранительную функцию, стоит на защите интересов личности, общества и государства, имея возможности для обеспечения реализации названной функции использовать меры государственного принуждения. В частности, полномочиями, связанными с выявлением и расследованием преступлений (в том числе, совершаемых в сети «Интернет»), обладают исключительно правоохранительные органы.

Предпринимаемые со стороны государства меры должны быть направлены, в первую очередь, на предупреждение киберпреступлений, должны носить системный характер, должны объединяться едиными задачами. В противном случае разрозненные, противоречивые меры не будут эффективными.

В этой связи, следует поддержать идею о принятии Концепции стратегии кибербезопасности Российской Федерации и продолжить работу над её созданием. Данный документ мог бы стать необходимым и даже ключевым демократическим по своей сути элементом системы противодействия преступлениям, совершаемым в сфере Интернет (киберпреступлениям).

При этом сугубо государственных полномочий в сфере противодействия киберпреступлениям может и не хватить, поэтому можно и нужно привлекать, на законной основе, коммерческие организации, имеющие необходимый потенциал и желание его использовать в контексте противодействия преступлениям в сфере Интернет.

Необходимо развивать государственно-частное партнёрство в направлении противодействия киберпреступности. В виде глобальной цели такого партнёрства выступает создание отлаженной и максимально эффективной системы противодействия киберпреступности.

Для государства, в лице правоохранительных структур, важно повысить эффективность выявления, раскрытия и расследования преступлений в сфере «Интернет», а также повысить уровень подготовленности кадровых сотрудников правоохранительных органов.

Обеспечив комплексный подход в противодействии киберпреступности, можно рассчитывать на постепенное достижение значимых результатов в данном направлении.

Важно при этом осуществлять как совершенствование действующих уголовно-правовых норм, так и осуществлять предупреждение совершения рассматриваемых преступлений, путём разработки и реализации Концепции стратегии кибербезопасности Российской Федерации и расширения государственно-частного партнёрства в указанном направлении.

При этом нельзя забывать о международное сотрудничество и координацию в профилактике киберпреступности. Наряду с выработкой и внедрением международных соглашений в сфере предотвращения и расследования киберагрессии, возможно создание международного органа с региональными представительствами. В свою очередь данный орган должен работать по двум направлениям, это научно-аналитический уровень и исполняющий уровень. Научно-аналитический уровень, изучал бы риски кибербезопасности в соответствии с вероятностями реализации киберугроз и размерами негативных последствий; актуализировал средства и методы обеспечения кибербезопасности, разрабатывал рекомендации и методики. Исполняющий уровень, осуществлял бы координацию по двум направлениям – внутреннему (между национальными структурами, ответственными за выявление и противодействие киберугроз) и внешнему, когда координация осуществляется между национальными структурами и схожими иностранными региональными/международными учреждениями. Возможно было бы наделить его полномочиями выступать и активно участвовать в развитии международного сотрудничества в области структурах, направленных на выявление киберугроз, своевременно обнаруживать, предотвращать, защищать, а также минимизировать последствия.

Список литературы

1. Бугаев В.А., Чайка А.В. Факторы преступности в сфере компьютерных технологий // Ученые записки Крымского федерального университета имени В.И. Вернадского. Юридические науки. 2019. Т. 5. № 4 (71). С. 139-145.
2. Казакова В.А. Условия, способствующие росту вооруженной преступности в России // Современное право. 2003. № 7. С. 32-35.
3. Криминология / Под ред. В.Н. Бурлакова, Н.М. Кропачева. М., 2004
4. Ханахмедов А.С. Основы противодействия киберпреступности на территории Российской Федерации // Вестник Уфимского юридического института МВД России. 2019. № 3 (85). С. 44-48.

Суварян А.С., Юридический институт

АлтГУ, г. Барнаул

Научный руководитель: Стародубцева М.А., преподаватель кафедры
уголовного права и криминологии АлтГУ

Суварян А.С. НЕКОТОРЫЕ АСПЕКТЫ КРИМИНОЛОГИЧЕСКОЙ ХАРАКТЕРИСТИКИ КИБЕРПРЕСТУПЛЕНИЙ

Рост объёмов информации, компьютерных сетей и числа пользователей, упрощение их доступа к циркулирующей по сетям информации существенно повышает вероятность хищения или разрушения этой информации.

В настоящее время значимость проблемы защиты информационных ресурсов, в том числе личных, определяется следующими факторами:

- развитием мировых и национальных компьютерных сетей, и новых технологий, обеспечивающих доступ к информационным ресурсам;
- переводом информационных ресурсов на электронные носители и концентрацией их в информационных системах;
- повышением "цены" создаваемой и накопленной информации, служащей реальным ресурсом социально-культурного и личностного развития;
- разработкой и совершенствованием информационных технологий, которые могут эффективно использоваться криминальными структурами.

Компьютерная преступность стала настоящим бичом экономики развитых государств. Так, например, 90% фирм и организаций в Великобритании в разное время становились объектами электронного пиратства или находились под его угрозой, в Нидерландах жертвами компьютерной преступности стали 20% различного рода предприятий. В ФРГ с использованием компьютеров ежегодно похищается информация на сумму 4 млрд. евро, а во Франции - 1 млрд. евро.

Наибольшую общественную опасность представляют преступления, связанные с неправомерным доступом к компьютерной информации. Известно,

рассматриваемое правонарушение имеет очень высокую латентность, которая по различным данным составляет 85-90% . Более того, факты обнаружения незаконного доступа к информационным ресурсам на 90% носят случайный характер.

В современных условиях социально-экономического развития Российской Федерации компьютерная преступность стала реальностью общественной жизни.

Подтверждением роста компьютерных преступлений в России являются статистические данные Совета безопасности Российской Федерации, согласно которым выявлено более 800 000 попыток осуществления компьютерных атак на официальные информационные ресурсы органов государственной власти, при этом более 69 000 из них - на официальное Internet-представительство Президента России.

О динамике и масштабах компьютерных преступлений наглядно свидетельствуют следующие данные. За последние десять лет их число возросло в 22,3 раза и продолжает расти в среднем в 3,5 раза ежегодно. Ежегодный размер материального ущерба от этих преступных посягательств составляет 613,7 млн. руб. Средний ущерб, причиняемый потерпевшему от одного компьютерного преступления, равен 1,7 млн. руб. С определенной долей успеха расследуется лишь около 49% преступлений, обвинительные приговоры выносятся лишь в 25,5% случаев от общего числа возбужденных уголовных дел.

Средний показатель - число уголовных дел, по которым производство приостановлено, составляет 43,5% и ярко отражает низкую степень профессионализма сотрудников правоохранительных органов в деятельности по раскрытию, расследованию и предупреждению этих преступных посягательств.

Для более точного сравнения можно привести следующие данные. По материалам подразделений "К" возбуждено 1673 уголовных дела, что на 45% больше, чем за аналогичный период предыдущего года. Число выявленных

преступлений возросло почти на 6% и составило 4295 против 4057 в предыдущем году.

По сообщению Управления “К” МВД России удалось раскрыть свыше 7000 преступлений в сфере высоких технологий, более 4000 из них подпадают под ст. 272 Уголовного Кодекса (УК) “Неправомерный доступ к компьютерной информации”. Основная часть преступлений - это компьютерные преступления, связанные с незаконным доступом к информации и с использованием вредоносных программ. Анализ сложившейся ситуации показывает, что около 16% злоумышленников - молодые люди в возрасте до 18 лет, 58% - лица от 18 лет до 25 лет, около 70% из них имеют высшее либо незаконченное высшее образование.

Цель - изучить проблемы развития киберпреступности в мире и России и найти способы ее профилактики.

Задачи

1. Изучить понятие киберпреступность.
2. Рассмотреть виды киберпреступлений.
3. Провести опрос в социальных сетях.
4. Найти примеры киберпреступлений в мире, России.
5. Дать рекомендации противостояния хакерам в домашних условиях.

Вопросы анкетирования	Количество опрошенных лиц в процентах (%)
1 Ваш пол	
А. Женский	62,5%
Б. Мужской	37,5%
2 Сколько вам лет?	
А. 14-19	6,3%
Б. 20-39	81,3%

В. 40-50	12,5%
3. Знаете ли вы, что такое киберпреступность?	
А. да	87,5%
Б. нет	12,5%
4. С каким из видов киберпреступлений Вы сталкивались?	
А. хакерство	73,3%
Б. кардинг	20%
В. фишинг	33,3%
Г. киберхулиганство	33,3%
Д. диффамация	13,3%
Е. спамерство	66,7%
5. теряли вы свои средства либо данные о себе после атак?	
А. да	68,8%
Б. нет	31,3%
6. Как Вы думаете, что толкает человека на совершение киберпреступления?	
А. Малоразвитая правовая система по отношению к этому явлению	50%
Б. Анонимность сети Интернет	68,8%
В. Неостребованность обществом специальных знаний в сфере компьютерных технологий	43,8%
Г. Ненависть и агрессия, которые толкают на совершение киберпреступлений	43,8%
7. Какая по Вашему мнению ситуация в данный момент с преступлениями, совершаемых в вашем городе?	
А. Спокойная	12,5%

Б. Напряженная	56,3%
В. Кризисная	18,8%
Г. Затрудняюсь ответить	12,5%

Киберпреступность уже стала большой проблемой для всего мира - и проблема стремительно нарастает. Правоохранительные органы пытаются угнаться за ней - законодатели принимают новые законы, полицейские агентства формируют специальные подразделения по борьбе с киберпреступностью. Киберпреступление, как и любое другое преступление есть не только правовая, но и социальная проблема. Чтобы успешно бороться с киберпреступностью, должны привлекаться ИТ - специалисты и те в обществе, кого затрагивает, прямо или косвенно преступная деятельность, нашедшая благоприятную среду - виртуальное пространство.

Необходимо создать унифицированную классификацию и формальную модель киберпреступлений, которые облегчат и противодействие, и расследование киберпреступности.

Список литературы

1. Преступления, связанные с использованием компьютерной сети / X конгресс ООН по предупреждению преступности и обращению с правонарушителями // A/CONF. 187/10.
2. Шидловский А. В. Установление уголовной ответственности за киберпреступления – новый сегмент в правовой охране электронного государства // Сборник материалов VI Международной науч.-практ. конф. 2018.
3. Преступления, связанные с использованием компьютерной сети / X конгресс ООН по предупреждению преступности и обращению с правонарушителями // A/CONF. 187/10

4. URL: <https://www.web-canape.ru/business/vsa-statistika-interneta-na-2019-god-vmire-i-v-rosii/>.

5. Хусяинов Т. М. Интернет-преступления (киберпреступления) в российском уголовном законодательстве // Уголовный закон Российской Федерации

Корватко Н.А., магистрант Юридического
института АлтГУ, г. Барнаул

Научный руководитель: Мазуров В.А., кандидат юридических наук,
доцент кафедры уголовного права и криминологии АлтГУ

Корватко Н.А. ПРОФИЛАКТИКА ЭКСТРЕМИЗМА И ТЕРРОРИЗМА В КИБЕРПРОСТРАНСТВЕ

Анализ информационной обстановки в Сети показывает, что контент основных Интернет-ресурсов по продвижению идеологии насилия (террористической, экстремистской, националистической и др. направленности) носит наступательный, агрессивный характер, отличается хорошей теоретической базой, продуманным спектром методов управляемого информационно-психологического воздействия на пользователей и защищенностью ресурсов. Подавляющее большинство сайтов, блогов и форумов указанной направленности поддерживается из-за рубежа и направлено на дестабилизацию обстановки не только на Северном Кавказе, но и в других регионах России, внесение разногласий в деятельность межгосударственных структур с участием России.

Основными формами продвижения террористической и экстремистской идеологии избраны такие, как культивирование экстремизма, насилия (террора), религиозного фундаментализма, сепаратизма, национализма, шовинизма и других. Наибольшую опасность для российского общества представляют русскоязычные Интернет-ресурсы, вовлекающие молодежь в экстремистскую и террористическую деятельность, в том числе популяризирующие образ «террориста-героя». Нацеленность таких ресурсов направлена в первую очередь на молодежь тех республик, в которых традиционной религией является ислам, а также регионов с компактным проживанием мусульманского населения. Традиционный терроризм не угрожал обществу как таковому, не затрагивал основ его жизнедеятельности.

Современный же высокотехнологичный терроризм способен продуцировать системный кризис в любом государстве с высокоразвитой информационной инфраструктурой. Поэтому компетентный и научный подход, профессиональная организация прогнозирования, ранняя и своевременная диагностика, научно-технологическая экспертиза, выявление новейших факторов риска, нейтрализация сфер и зон террористической деятельности могут существенно снизить вероятность разворачивания информационно ориентированного терроризма и уменьшить угрозу человеческой жизни. На сегодняшний день любой человек, будь то обычный студент или маленький ребенок, зайдя в Интернет, может наткнуться на сайты, содержащие детскую порнографию, видео с актами насилия, пропаганду экстремизма и террора. Содержание таких сайтов может в корне перевернуть его представление о мире, нанести непоправимую моральную травму и склонить его на путь разврата, нетерпимости, насилия и деградации.

С целью борьбы с данным явлением необходимо принять меры профилактического характера. Профилактика правонарушений представляет собой совокупность мер социального, правового, организационного, информационного и иного характера, направленных на выявление и устранение причин и условий, способствующих совершению правонарушений, а также на оказание воспитательного воздействия на лиц в целях недопущения совершения правонарушений или антиобщественного поведения (ст. 2 Федерального закона от 23 июня 2016 г. № 182-ФЗ «Об основах системы профилактики правонарушений в Российской Федерации», далее – ФЗ № 182).

Механизм профилактики должен быть нацелен на:

1) устранение (нейтрализацию, «замораживание», ослабление криминогенного воздействия) объективных факторов, способствующих совершению преступлений;

2) корректирующее воздействие, «гасящее» криминогенный потенциал субъективного фактора (умысел совершения преступлений, нарастание

психологической готовности к его осуществлению, поиск возможных единомышленников и соучастников, вариантов и путей реализации преступного посягательства и т. д.;

3) внесение дисфункции в цепочку криминогенных взаимодействий объективных и субъективных факторов, ведущее к саморазрушению самого процесса приближения к посягательству на совершение преступления.

Выделяют два основных вида профилактики правонарушений: общую профилактику и индивидуальную профилактику.

Общая профилактика правонарушений направлена на выявление и устранение причин, порождающих правонарушения, и условий, способствующих совершению правонарушений или облегчающих их совершение, а также на повышение уровня правовой грамотности и развитие правосознания граждан. Индивидуальная профилактика правонарушений направлена на оказание воспитательного воздействия на лиц определенных категорий, на устранение факторов, отрицательно влияющих на их поведение, а также на оказание помощи лицам, пострадавшим от правонарушений или подверженным риску стать таковыми.

Индивидуальная профилактика правонарушений может осуществляться с применением специальных мер профилактики правонарушений. В Федеральном законе Российской Федерации от 6 марта 2006 г. № 35-ФЗ «О противодействии терроризму» одним из направлений такого противодействия названо предупреждение терроризма, включающее выявление и последующее устранение причин и условий, способствующих совершению террористических актов (профилактику терроризма).

Широкое и развернутое определение профилактики терроризма содержится в Модельном законе СНГ «О борьбе с терроризмом», в котором она трактуется как деятельность органов государственной власти, органов государственной власти административно-территориальных образований государства, органов местного самоуправления и общественных объединений по предупреждению терроризма и (или) террористической деятельности,

закрывающаяся в выявлении, локализации и устранении причин и условий, способствующих возникновению и распространению терроризма и осуществлению террористической деятельности, совершению актов терроризма; защите потенциальных объектов террористических посягательств; создании условий, препятствующих совершению актов терроризма, минимизации их последствий, а также в воздействии на физических лиц, которые вовлекаются или могут быть вовлечены в террористическую деятельность и (или) совершить акты терроризма.

Стратегия противодействия экстремизму в Российской Федерации до 2025 года (утв. Президентом РФ 28.11.2014 № Пр-2753) предусматривает следующие направления государственной политики в сфере противодействия экстремизму в сфере образования и государственной молодежной политики, носящие преимущественно профилактический характер и нацеленные на молодежь:

- включение в региональные и муниципальные программы по развитию образования и воспитанию несовершеннолетних 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;

- проведение в образовательных организациях занятий по воспитанию патриотизма, культуры мирного поведения, межнациональной и межконфессиональной дружбы, по обучению навыкам бесконфликтного общения, а также умению отстаивать собственное мнение, противодействовать

социально опасному поведению, в том числе вовлечению в экстремистскую деятельность, всеми законными средствами;

- включение в учебные планы, учебники, учебно-методические материалы тем, направленных на воспитание традиционных для российской культуры ценностей;

- повышение профессионального уровня педагогических работников, разработка и внедрение новых образовательных стандартов и педагогических методик, направленных на противодействие экстремизму;

- обеспечение активного участия коллегиальных органов управления образовательных организаций в профилактике экстремизма среди учащихся и студентов;

- проведение социологических исследований социальной обстановки в образовательных организациях, мониторинга девиантного поведения молодежи, анализа деятельности молодежных субкультур в целях выявления фактов распространения экстремистской идеологии;

- повышение престижности образования, полученного в российских религиозных образовательных организациях, а также осуществление мер государственной поддержки системы общественного контроля за выездом российских граждан для обучения в иностранных религиозных образовательных организациях;

- включение в федеральный государственный образовательный стандарт по специальности журналистика образовательных программ по информационному освещению вопросов противодействия экстремизму;

- усиление роли общественных советов при федеральных органах исполнительной власти в деятельности по воспитанию патриотизма и формированию гражданского самосознания у молодежи;

- взаимодействие с молодежными общественными объединениями и организациями футбольных болельщиков в целях профилактики экстремистских проявлений при проведении массовых мероприятий.

Профилактика терроризма и экстремизма в молодежной среде имеет определенную специфику. Как известно, именно молодежь выступает основным объектом информационно-пропагандистской и вербовочной деятельности террористических и экстремистских организаций. Соответственно она должна выступать приоритетным объектом профилактической работы со стороны государственных органов и иных субъектов профилактики правонарушений.

Очевидно, что к молодежи могут применяться общие средств и методы профилактического воздействия, предусмотренные национальным законодательством государства. Так, упомянутый выше российский ФЗ № 182 выделяет следующие формы профилактического воздействия:

- 1) правовое просвещение и правовое информирование;
- 2) профилактическая беседа;
- 3) объявление официального предостережения (предостережения) о недопустимости действий, создающих условия для совершения правонарушений, либо недопустимости продолжения антиобщественного поведения;
- 4) профилактический учет;
- 5) внесение представления об устранении причин и условий, способствующих совершению правонарушения;
- 6) профилактический надзор;
- 7) социальная адаптация;
- 8) ресоциализация;
- 9) социальная реабилитация;
- 10) помощь лицам, пострадавшим от правонарушений или подверженным риску стать таковыми.

В то же время они должны быть дополнены специализированным инструментарием, ориентированным именно на молодежную среду. Зарубежный опыт профилактики терроризма и экстремизма В связи с глобальным характером террористической и экстремистской угрозы

в различных государствах мира реализуются меры по профилактике вовлечения молодежи в экстремистскую и террористическую деятельность. Большинство экспертов сходится в том, что наиболее оптимальным направлением работы являются меры по предотвращению вербовки. В данном направлении в Европе применяются следующие методы работы.

1. Кампания по формированию общенациональной идентичности, направленная на интеграцию мигрантов-мусульман. Например, в Австрии с 2011 г. действует программа «Вместе: Австрия», которая комбинирует информационную кампанию в Интернете и элементы школьной программы. Важный механизм австрийской программы по интеграции мигрантов – привлечение к ней успешных представителей диаспор для лекций в школах. Более 300 «послов» посещают образовательные учреждения, рассказывая о своем опыте успешной жизни в Австрии. Аудитория программы составляет более 20 тыс. человек.

Подобный опыт, на наш взгляд, представляет особый интерес для столичных регионов стран Содружества с высокой долей мигрантов.

2. Разработка и реализация комплексных программ по борьбе с экстремизмом в системе образования. Во Франции была принята специальная программа Министерства образования и науки «Большая мобилизация образования в поддержку ценностей Республики» (*Grande mobilisation de l'École pour les valeurs de la République*), опубликованная 9 февраля 2015 года. Помимо прочего, программа предусматривала: подготовку 300 000 учителей-методистов в данной сфере; развитие системы школьных СМИ, посвященных соответствующей теме; взаимодействие с национальными СМИ и интернет-порталами; введение 9 декабря (дата принятия Закона об отделении церкви от государства) в учебных заведениях Дня светского государства; проведение памятных мероприятий патриотического характера; введение Дня национальной обороны и гражданственности; введение Недели борьбы с расизмом и антисемитизмом как формами радикального поведения; развитие исследований в сфере изучения радикализации; распространение методических

пособий с указанием возможных признаков вовлеченности учащихся в радикальные религиозные организации.

В докладе сенатской комиссии по борьбе с радикализацией от 1 апреля 2015 года были сформулированы предложения по дальнейшему их развитию:

1. Усиление подготовки профессионального сообщества, работающего с детьми и подростками, с точки зрения методик выявления радикального поведения.

2. Организация круглосуточной телефонной линии с целью приема звонков от граждан, интересующихся проблемами радикализации и путями эффективной борьбы с ней.

3. Широкое распространение среди населения информации о признаках радикализации, разработка экспертами системы критериев, свидетельствующих о потенциальной вовлеченности в экстремистские организации и о степени этой вовлеченности.

4. Введение в школьную программу образовательного курса по критическому восприятию информации в Интернете, развитие у учащихся навыков распознавания материалов экстремистского содержания.

5. Активное использование Интернета для контрпропаганды, направленной против экстремизма, распространение в Интернете, особенно в социальных сетях, свидетельств бывших религиозных радикалов, вставших на путь исправления.

6. Помощь развитию «французского ислама», который станет гарантией против экстремизма, расширение доступа к высшему образованию для французских мусульманских религиозных деятелей (для этого предлагается удвоить число университетов, где они могли бы получать образование).

7. Введение в школьные программы курса преподавания религиозной культуры светскими учителями в светских учебных заведениях, где учащиеся будут читать религиозные тексты без обязательства принимать соответствующую веру, что позволит лишить радикалов монополии на распространение информации о религии.

8. Разработка программы по возвращению бывших членов экстремистских группировок к нормальной жизни, для чего предлагается создать сеть индивидуальных наставников.

В июле 2015 года французские законодатели вновь вернулись к этой проблеме. Комиссия национального Сената, сформированная после терактов 7–9 января 2015 года, одобрила перечень мер по усилению работы образовательных учреждений, направленной на пропаганду светских ценностей. В числе предложений сенаторов, в частности, введение «Клятвы учителя», произносимой при вступлении в должность и содержащей обязательство пропагандировать среди учащихся знания о лучших страницах французской истории с целью укрепления единства общества. Во Франции также уже получает широкое распространение практика проведения комплексных антиэкстремистских семинаров для преподавателей, медиков и социальных работников по вопросам противодействия экстремизму.

В ФРГ агентства политического образования при министерствах по делам семьи и молодежной политики на уровне земель ежегодно проводят семинары для школьников по вопросам экстремизма. Изначально данные меры были направлены на борьбу с ультраправым, неонацистским экстремизмом. Лишь постепенно в последние годы начала появляться и ориентация на борьбу с исламским религиозным экстремизмом.

3. Налаживание специальных программ взаимодействия школы и полиции. Например, еще в середине 1997 года в Норвегии сотрудники полиции и родители, дети которых оказались вовлечены в радикальные группировки, инициировали программу «Выход».

В ее цели входили: поддержка молодых людей, желающих покинуть радикальные группировки, проповедующие насилие; поддержка родителей, чьи дети оказались вовлеченными в подобные группировки; разработка и распространение информации и методов работы для учителей и соцработников. Сначала программа была направлена в основном на борьбу с ультраправым расистским экстремизмом. Однако принципы «Выхода»

впоследствии распространились и на повседневную работу полиции и служб, занимающихся проблемой радикализации молодежи и вербовки религиозных террористов. Ключевым элементом норвежской стратегии дерадикализации стали «доверительные беседы» (собеседования со специалистами-психологами в полиции), нацеленные на удержание личности в общественно приемлемых рамках как альтернативу уголовному преследованию. Выявление потенциально проблемных молодых людей находится в компетенции широкого круга лиц: полицейских, учителей, религиозных лидеров, молодежных клубов, соседей.

4. Создание специального программного обеспечения для мониторинга интернет-активности. В Великобритании, согласно новому антитеррористическому законодательству, которое вступило в силу 1 июля 2015 года, школы должны использовать специальное программное обеспечение, которое будет осуществлять мониторинг интернет-активности учеников, включая их переписку в соцсетях, на предмет характерных терминов, которые употребляют вербовщики террористов. Несколько компаний (Impero, Future Digital, Securus) уже опробовали опытные образцы подобного ПО в ряде школ, продемонстрировав хорошие результаты. На основе анализа видео- и печатной агитационной продукции экстремистов был составлен подробный словарь экстремистских терминов, который и лег в основу мониторинговых программ.

В Российской Федерации в настоящее время одним из направлений профилактической работы общественных объединений выступает мониторинг сети «Интернет», включая социальные сети и блогосферу, на предмет выявления экстремистского контента и иных экстремистских и террористических угроз. Несмотря на организацию правоохранительными органами постоянного мониторинга сети «Интернет», в том числе с использованием автоматизированных систем, отследить активность многочисленных информационных ресурсов террористических и экстремистских организаций и их сторонников в Сети не представляется возможным.

Помимо традиционных каналов передачи информации в правоохранительные органы (личное обращение в дежурную часть, направление письменного или электронного обращения) рядом некоммерческих организаций учреждены специальные «горячие линии». Так, активную работу по данному направлению, как уже было указано выше, проводит Общественная палата Российской Федерации во взаимодействии с Международным общественным фондом «Российский фонд мира». Широко известны «горячие линии» «Центра безопасного Интернета в России» и «Лиги безопасного Интернета». Хотя основным профилем их деятельности выступает выявление детской порнографии в Сети, они также принимают сообщения о контенте экстремистской направленности и организуют реагирование на них.

Положительной стороной работы перечисленных общественных «горячих линий» является самостоятельная предварительная проверка их достоверности, что позволяет отсеять необоснованные жалобы. В последние несколько лет в российских регионах получила распространение практика создания т. н. «кибердружин» – групп активистов студенческих объединений на базе вузов, которые осуществляют мониторинг сети «Интернет» с целью выявления противоправного контента и последующего информирования правоохранительных органов.

Другим направлением привлечения институтов гражданского общества выступает информационно-разъяснительная и контрпропагандистская работа, направленная на противодействие идеологии экстремизма и терроризма. В рамках данного направления деятельности общественные организации по инициативе или при содействии правоохранительных органов могут организовывать проведение публичных акций антиэкстремистской и патриотической направленности (собраний, шествий, митингов, культурно-массовых мероприятий), изготовление и распространение материалов наглядной агитации. Через общественные объединения и подконтрольные им ресурсы (интернет-сайты, аккаунты в социальных сетях, сетевые сообщества и группы) возможно ведение разъяснительной и контрпропагандистской

работы в сфере противодействия пропагандистской и вербовочной деятельности. Кроме того, посредством них могут стимулироваться общественные акции антиэкстремистской направленности как в сети «Интернет» (например, конкурсы рисунков или демотиваторов, разоблачающих истинную сущность МТО и их деструктивной идеологии), так и в офлайне (например, флешмобы, разъясняющие пагубные последствия вступления неофилов в ряды террористических организаций).

Таким образом в настоящий момент существует, а так же действует множество институтов профилактики и борьбы с экстремизмом в сети интернет, но к сожалению, надо признать тот факт, что отдельные руководители образовательных учреждений и представители профессорско-преподавательского состава, родители студентов и школьников наших стран не в полной мере представляют реальную угрозу обществу, исходящую от международного терроризма и религиозного экстремизма, ошибочно полагая, что это сфера деятельности только спецслужб и правоохранительных органов. Вскрываемые сегодня компетентными органами факторы и условия, способствующие распространению идеологии терроризма и радикализма, являются последствиями упущений, недоработок, ошибок и бездействия, допущенных другими структурами, не считая вопросов соответствующего влияния институтов семьи, воспитания, образования и общественности.

Список литературы

1. Петрищев В. Е. Профилактика терроризма // Терроризм в современном мире. 2-е изд. / под ред. В. Л. Шульца; Центр исслед. проблем безопасности РАН. М.: Наука, 2011. С. 321.

2. Казанцев А. А. Проблемы вербовки и возврата боевиков-террористов: опыт Европы и перспективы России. № 27 (2016);

3. Российский совет по международным делам (РСМД). М.: Спецкнига, 2016. С. 20.

Гауэрт М. В.

Юридический институт,
АлтГУ, г. Барнаул.

Научный руководитель: Стародубцева М. А.

преподаватель кафедры уголовного права и криминологии
Юридический институт АлтГУ, г. Барнаул

Гауэрт М.В. РАСПРОСТРАНЕНИЕ ИНФОРМАЦИИ ЭКСТРЕМИСТСКОЙ НАПРАВЛЕННОСТИ В СОЦИАЛЬНЫХ СЕТЯХ

С развитием интернета распространение различного рода информации стало происходить гораздо быстрее и охватывать намного большее количество людей. Повысилась скорость коммуникации и появилось множество возможностей взаимодействия между людьми, независимо от их места нахождения. Различные социальные сети стали неотъемлемой частью нашей жизни. Каждый день, находясь в интернете, человек просматривает большое количество разнообразного контента. Возможность легко и быстро донести до широкой аудитории какую-либо информацию, а также интерактивность, анонимность и слабый контроль со стороны государства сделали социальные сети очень привлекательным средством для экстремистской деятельности. Таким образом, вследствие информатизации общества люди стали все чаще подвергаться пропагандированию и распространению идеологии экстремизма.

Согласно статье 1 ФЗ "О противодействии экстремистской деятельности" к экстремистской деятельности относится:

насильственное изменение основ конституционного строя и (или) нарушение территориальной целостности Российской Федерации (в том числе отчуждение части территории 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;

использование нацистской атрибутики или символики, либо атрибутики или символики, сходных с нацистской атрибутикой или символикой до степени смешения, либо атрибутики или символики экстремистских организаций, за исключением случаев использования нацистской атрибутики или символики, либо атрибутики или символики, сходных с нацистской атрибутикой или символикой до степени смешения, либо атрибутики или символики экстремистских организаций, при которых формируется негативное отношение к идеологии нацизма и экстремизма и отсутствуют признаки пропаганды или оправдания нацистской и экстремистской идеологии;

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.

Особенно уязвимыми к данному явлению являются граждане от 14 до 25 лет, которые легче поддаются внушению и убеждению и не всегда могут критически отнестись к подобной информации. Кроме того, именно молодые люди являются самыми активными пользователями сети Интернет и пользователями различных социальных сетей. Соответственно, подавляющая часть контента в Интернете создается и потребляется именно лицами данной возрастной категории и это, как можно предположить, является основной причиной такой высокой вовлеченности молодых граждан в экстремистскую деятельность.

Ввиду этого факта в современной России особенностью экстремизма стало значительное снижение возраста граждан, совершающих данный вид правонарушений.

Количество преступлений, совершаемых с использованием Интернета за последнее время продолжает расти. Согласно отчету МВД о состоянии преступности за 2021 год, практически каждое четвертое преступление совершается с использованием IT-технологий. Однако нужно отметить, что темп роста их количества замедлился за последнее время. Если в первом полугодии 2021 года число киберпреступлений увеличилось на 20,3%, то за десять месяцев текущего года – на 8,1%.

Что касается структуры экстремистских правонарушений, то она свидетельствует о том, что две трети данных правонарушений совершается с помощью использования сети и различных Интернет-ресурсов.

Для того, чтобы выяснить, как часто и в каком масштабе обычные пользователи социальных сетей сталкиваются с контентом, имеющим

экстремистскую направленность, был проведен социологический интернет-опрос. Возраст опрашиваемых составляет от 14 до 25 лет, гендерное соотношение примерно пропорционально.

Опрашиваемым было предложено назвать социальные сети, в которых они зарегистрированы и которыми пользуются на постоянной основе.

Любая социальная сеть представляет собой интернет-площадку, сайт, который позволяет зарегистрированным на нем пользователям размещать информацию о себе и коммуницировать между собой, устанавливая социальные связи. Контент на этой площадке создается непосредственно самими пользователями.

Наиболее популярные соцсети в России — ВКонтакте, Instagram, YouTube, Одноклассники, TikTok, Telegram и Twitter.

Какими из нижеперечисленных соцсетей вы пользуетесь на постоянной основе?

32 ответа

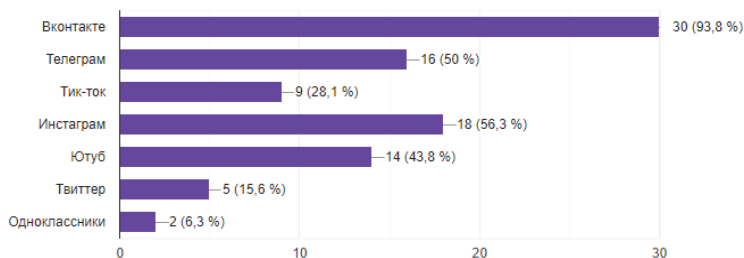


Рис. 1

Анализируя полученные данные, можно сделать вывод, что наибольшей популярностью у респондентов пользуется ВКонтакте (93%). Это самая распространённая социальная сеть в России, ее общая месячная аудитория составляет 97 млн пользователей.

На втором месте находится Instagram (56%) - американская социальная сеть для обмена фотографиями и видео, в России ее месячная аудитория составляет 59,4 млн пользователей.

Телеграмом пользуются 50 % процентов опрошенных, это мессенджер позволяющий обмениваться текстовыми, голосовыми и видеосообщениями, фотографиями, файлами, создавать каналы и группы, размещать в них информацию в различных форматах. С 16 апреля 2018 года по 18 июня 2020 года Телеграм был заблокирован на территории РФ по причине отказа выдать ключи для расшифровки переписки пользователей и предоставлять их по требованию ФСБ России. Однако позднее блокировка была отменена, также нужно отметить, что в Телеграм были усовершенствованы методы обнаружения и удаления экстремистской пропаганды.

Следующим по популярности является Ютуб (43 %) - видеохостинг, предоставляющий пользователям услуги хранения, доставки и показа видео. В России его аудитория насчитывает 62 млн. пользователей.

Тик-ток используют 28% опрошенных, данная социальная сеть является относительно новой, она представляет собой сервис для создания и просмотра коротких видео, принадлежащий пекинской компании «ByteDance».

Твиттером пользуются всего 15 % респондентов, и наименьшее количество пользователей у «Одноклассников», можно сделать вывод, что эта соцсеть не пользуется популярностью у данной возрастной категории.

Далее респондентам предлагалось определить, насколько реальной угрозой общественной безопасности они считают распространение в социальных сетях различной информации экстремистской направленности.

Насколько реальной угрозой общественной безопасности вы считаете распространение в социальных сетях различной информации экстремистской направленности?

32 ответа



Рис. 2

По мнению большинства опрошиваемых (59%), распространяемая в соцсетях информация экстремистской направленности является в определенной степени угрозой общественной безопасности. В тоже время часть респондентов (21%) считает, что опасность такой информации сильно преувеличена, а 18 % придерживаются противоположного мнения. Можно сделать вывод, что большинство граждан относятся к подобному контенту с должным вниманием и настороженностью и поддерживают реализацию определенных мер борьбы с данным явлением.

Далее опрошиваемым предлагалось ответить на вопросы, отражающие отдельные проявления экстремизма в интернете и социальных сетях.

Как часто вы сталкиваетесь в социальных сетях с информацией, унижающей и оскорбляющей людей по признаку социальной, расовой, национальной, религиозной, языковой принадлежности или отношения к религии?

32 ответа

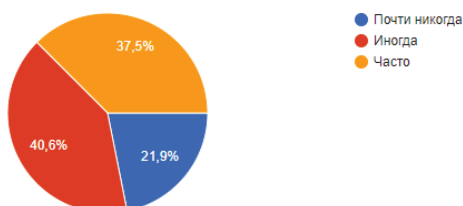


Рис. 3

Исходя из результатов опроса становится понятно, что почти 80% опрошенных так или иначе периодически сталкиваются в соцсетях с информацией, унижающей и оскорбляющей людей по признаку социальной, расовой, национальной, религиозной, языковой принадлежности или отношения к религии. Из них 37% отмечают, что такое происходит часто, и 40% - иногда. И только 21% респондентов указали, что почти не сталкиваются с подобным контентом.

Как часто вы встречаете информацию, призывающую к насилию в отношении людей по признаку социальной, расовой, национальной, религиозной, языковой принадлежности или отношения к религии?

32 ответа

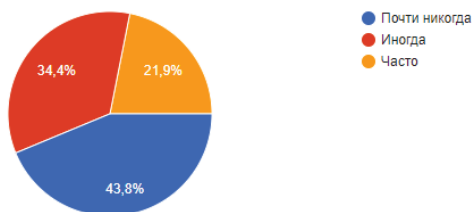


Рис. 4

21% опрошенных указали, что они часто встречают информацию, которая призывает к насилию в отношении людей по признаку социальной, расовой, национальной, религиозной, языковой принадлежности или отношения к религии. 34% респондентов ответили, что лишь иногда сталкиваются с подобным контентом, и 43% почти никогда не встречают в соцсетях такую информацию.

Как часто вы сталкиваетесь с пропагандой идей исключительности, превосходства либо неполноценности человека по признаку его социальной, расовой, национальной, религиозной или языковой принадлежности или отношения к религии?

32 ответа

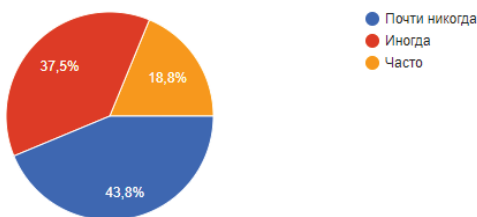


Рис. 5

43% респондентов почти никогда не сталкивается с пропагандой идей исключительности, превосходства либо неполноценности человека по признаку его социальной, расовой, национальной, религиозной или языковой принадлежности или отношения к религии. 37% опрошенных отмечает, что

лишь иногда встречает подобный контент, и 18% видят такую информацию регулярно.

Приходилось ли вам видеть попытки склонения, вовлечения, вербовки людей в социальных сетях для участия в реальных террористических или экстремистских объединениях либо совершаемых ими деяниях?

32 ответа

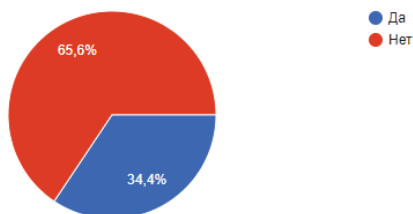


Рис. 6

Из числа опрошенных 34% встречались с попытками склонения, вовлечения, вербовки людей в социальных сетях для участия в реальных террористических или экстремистских объединениях либо совершаемых ими деяниях.

Попадалась ли вам информация, оправдывающая или поддерживающая идеологию и практику терроризма и экстремизма без попыток вовлечения людей в экстремистскую или террористическую деятельность?

32 ответа

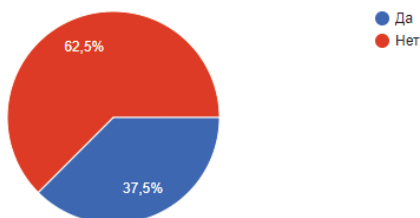


Рис. 7

С информацией, оправдывающей или поддерживающей идеологию и практику терроризма и экстремизма без попыток вовлечения людей в экстремистскую или террористическую деятельность сталкивались 37% опрошенных.

Встречались ли вы в интернете с пропагандой или публичным демонстрированием нацистской атрибутики или символики?

32 ответа

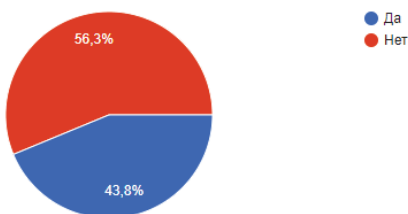


Рис. 8

Пропаганду или публичное демонстрирование нацистской атрибутики или символики видели в социальных сетях 43% респондентов.

Сталкивались ли вы с призывами к насильственному изменению основ конституционного строя и (или) нарушению территориальной целостности Российской Федерации.

32 ответа

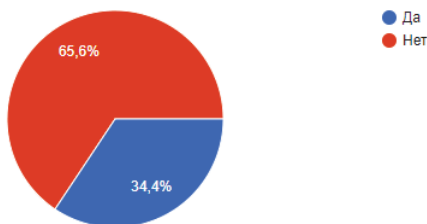


Рис. 9

С призывами к насильственному изменению основ конституционного строя и (или) нарушению территориальной целостности Российской Федерации сталкивались 34% опрошенных.

Проанализировав результаты опроса, можно сделать вывод, что уровень распространения информации экстремистской направленности в интернете, в частности в социальных сетях, на данный момент является достаточно высоким, так как большинство опрошенных лиц, являющихся пользователями

социальных сетей, регулярно сталкиваются с отдельными проявлениями экстремизма.

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: 04.12.2021).
2. ВЦИОМ: Социальные сети: кто туда ходит и зачем? [Электронный ресурс]. URL: <https://wciom.ru/index.php?id=236&uid=1457>
3. 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>
4. Люев Р.Х., «Технологии распространения идеологии экстремизма и терроризма в глобальном информационном пространстве» // Образование и право, № 6, 2021

Монисовой Е. Д.

магистрант Юридического института, АлтГУ, г. Барнаул

Колосничих А. И.

магистрант Юридического института, АлтГУ, г. Барнаул

Научный руководитель: Мазуров В. А.,

кандидат юридических наук,

доцент кафедры уголовного права и криминологии АлтГУ

**Монисовой Е.Д., Колосничих А.И. КОНТРПРОПАГАНДА
ИДЕОЛОГИИ ЭКСТРЕМИЗМА И ТЕРРОРИЗМА В МОЛОДЕЖНОЙ
СРЕДЕ**

Одной из проблем на сегодняшний день является преступность экстремистской и террористической направленностей. Такие явления покушаются на национальную безопасность России, объектами которой выступают независимость и суверенитет государства, основы общественного строя, политическая организация общества, государственная власть и ее институты, и безопасность граждан. В отдельных случаях преступность такого рода подрывает авторитет государственных органов и органов местного самоуправления, и создается большая угроза состоянию и тенденциям развития общества и его жизнедеятельности.

В связи с этим существует комплекс мер, направленных на противодействие террористическим и экстремистским направлениям. Ряд положений регламентирован законными и подзаконными актами. Создаются специальные подразделения правоохранительных органов, учреждаются антитеррористические комитеты и т.п. Уровень обеспеченности таких мер является весьма высоким, при этом существуют определенные проблемы контрпропаганды таких явлений среди молодежи.

Прежде всего, стоит дать определения идеологии этим двум явлениям. В литературе под идеологией экстремизма понимают приверженность к

крайностям во взглядах, оценках и позициях, к крайним средствам достижения поставленных целей в деятельности, как отдельных лиц, так и социальных групп, связанных национальными, политическими, религиозными или иными идеями.[12]

В Стратегии противодействия экстремизму в Российской Федерации до 2025 г. данное явление определяется так: «...идеология экстремизма (экстремистская идеология) — система взглядов и идей, представляющих насильственные и иные противоправные действия как основное средство разрешения социальных, расовых, национальных, религиозных и политических конфликтов».[4] Сюда можно отнести практически все деяния, которые связаны с вышеуказанными мотивами.

В соответствии со ст. 3 Федерального закона от 06.03.2006 N 35-ФЗ "О противодействии терроризму", терроризм - 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.[2]

Помимо этого в международных нормативно-правовых актах и научной литературе насчитывается около 200 определений, но все они сводятся к тому, что идеология терроризма основана на практике насилия и запугивании населения.

Можно сделать вывод, что два этих явления тесно взаимосвязаны, поскольку одно является составной частью другого. Понятие идеологии экстремизма основано на ненависти по вышеуказанным мотивам, а идеология терроризма в свою очередь является крайне агрессивной и более общественно-опасной формой экстремизма.

По данным МВД РФ за 2020 год было зарегистрировано 2342 преступления террористического характера (+29,7%) и 833 преступления экстремистской направленности (+42,4%). Из общего числа зарегистрированных преступлений террористического характера 623 (+67,9%)

преступления совершены в текущем году, в том числе: – пресечено на стадии приготовления и покушения – 71 (+18,3%); – за пределами Российской Федерации – 226 (+218,3%).[6]

Стоит учитывать, что большинство преступлений экстремистской и террористической направленности совершаются при использовании сети «Интернет» посредством различных ресурсов социальных сетей. По данным Генеральной прокуратуры РФ за первую половину 2021 г. значительная часть преступных проявлений экстремизма, которая связана с публичными призывами к осуществлению такой деятельности (+44,1 %, 353) были совершены при использовании сети «Интернет» (332).[7]

Преступления совершаемые посредством Интернет-ресурсов является пропаганда идеологии экстремизма и терроризма, публичные призывы, вербовка в террористические и экстремистские организации, оправдания террористической деятельности, выкладывание видео публичных казней, прочих материалов неприемлемого содержания и ряд других. Таким образом, интернет становится основной вспомогательной платформой осуществления экстремистской и террористической деятельности. Все это негативно воздействует на правосознание граждан, в частности молодежи, поскольку данная категория нередко подвергается такому влиянию, в результате чего возникают проблемы в их ценностной ориентации.

В последние годы участились случаи заведомо ложных сообщений об акте терроризма. Выражается это в том, что зачастую сами дети анонимно звонят и сообщают о заложенных взрывных устройствах, с целью срыва занятий, экзаменов и т.д. Согласно данным МВД РФ, "Количество преступлений, связанных с заведомо ложными сообщениями об актах терроризма, выросло в России в полтора раза в 2019 году, следует из статистики МВД. Как отмечают в ведомстве, за период с начала года до июля включительно органы внутренних дел зарегистрировали 1726 подобных преступлений, по сравнению с прошлым годом их число выросло на 52,5%. При

этом раскрывается меньше половины подобных преступлений – показатель раскрываемости по ним составляет 39,9%, следует из отчета МВД".[8]

Часто мы слышим о таком явлении как, “колумбайн” или же “скулшутинг”, что означает массовые расстрелы в учебных заведениях, жертвами которых становятся школьники, студенты, преподаватели. Одним из примеров является, массовый расстрел в колледже, г. Керчь. 2021 год уже запомнился такими массовыми расстрелами в Казани и Перми. Причиной этого является распространение контента, пропагандирующего идеологию насилия посредством создания сообществ в различных социальных сетях, в которых происходит обмен соответствующей информацией.

Возникает ряд вопросов, по поводу того какие для этого применять меры. Одно из важных направлений в деятельности по профилактике терроризма и экстремизма в студенческой сфере и молодежной среде — это профилактические меры в сети «Интернет». Недопущение размещения в сети «Интернет» инструкций по проведению экстремистских акций и насилия, поиска источников финансирования экстремистской и террористической деятельности, инструкций по изготовлению и применению средств террора, которые должны быть изъяты и заблокированы.[3] С этим нельзя не согласиться, подобным материалам не место в открытом доступе. Но все же, это является борьбой со следствием, а не с причиной.

В постановлении Правительства РФ «О государственной программе «Патриотическое воспитание граждан Российской Федерации на 2016—2020 годы» содержатся положения о необходимости формирования у студентов и школьников патриотические и духовно-нравственные ценности, традиционные для нашей страны, чувства межнационального и межрелигиозного уважения.[5]

На наш взгляд это можно поставить в качестве приоритетного направления контрпропаганды идеологии экстремизма и терроризма, поскольку именно патриотизм является проявлением любви к своей родине и своим ближним, уважению к истории и культуре своей страны, который и нужно воспитывать в молодом поколении.

Как ни странно, ярким примером проявлением патриотизма сегодня является США. Опросы общественного мнения, проводимые в США, показывают, что примерно три четверти граждан США испытывают чувство гордости за свою страну. Около половины американских семей украшают свой дом флагом США. Девять из десяти американцев испытывают чувство гордости, когда звучит мелодия гимна страны. Самыми любимыми символами были названы (в порядке уменьшения популярности): американский флаг, статуя Свободы, государственный гимн, белоголовый орлан (его изображение широко используется в официальной символике, в частности, в гербе США), Белый дом и песня «Боже, благослови Америку». [13]

С первого класса перед началом занятий американские школьники ежедневно произносят Клятву в верности флагу. Клятва звучит кратко и емко: «Я клянусь в верности флагу Соединенных Штатов Америки и Республике, которую он символизирует, одной Нации под Богом, неделимой, со свободой и справедливостью для всех». Это регламентировано большинством законов на федеральном уровне, либо на уровне штата.

Патриотизм в США строится на идеях свободы, равенства и справедливости. Американский философ М. Адлер отмечает, что именно «...на этих трех идеях строится жизнь нашего общества. Они олицетворяют те идеалы, к достижению которых человечество стремится в настоящем и которые хочет передать своим потомкам в будущем». [9]

Еще одним примером является Китайская Народная Республика, которая осуществляет «патриотическое воспитание через интернет-ресурсы развивает интерес студентов к теме патриотизма в условиях взаимодействия китайской социальной сети. В условиях распространения интернета, в том числе Wechat, Weibo, 00, создание специализированных сайтов и форумов представляется весьма эффективным средством патриотического воспитания китайских студентов». [14] Посредством таких Интернет-ресурсов проводятся различные онлайн мероприятия по памятным датам и праздникам. Государственный комитет по образованию КНР рекомендует разучивать различные песни на тему

патриотизма: Гимн страны, песни «О Родине», «Единство — это сила», «Без компартии нет Китая» и другие.

По сравнению с другими странами мира, в России патриотизм развит слабо. Одной из проблем является недостаточная работа образовательных учреждений и прочих организаций, другой является проблема в самой молодежи, которое воспринимает некие его проявления как пережитки советских времен или навязывание абсолютно не нужных духовно-моральных ценностей родителями. Так же, в молодежной среде очень развито недоверие к государству, а какие-то взаимодействия с ним считаются позорными.

На наш взгляд, проблема в идеологии государства, а именно в ее отсутствии. Без идеологии не может быть и патриотизма, поскольку именно она представляет собой определенную систему взглядов и идей, морали и нравственности, которые бы и объединяли российский народ. Таким образом, именно идеология является основой и источником проявления патриотизма. Для того что бы более подробно разобраться следует обратиться к истории нашей страны.

В периоды царской России неоднократно возникала проблема с отсутствием идеологии. Вначале XIX в. была провозглашена официальная идеология «Святая Русь». Это было связано с Отечественной войной 1812 года. Звучал девиз - За Веру, Царя и Отечество (За Бога, Царя и Отечество).

Во времена правления Николая I, в 1833 году С.С. Уваровым была сформулирована такая идеология, которая базировалась на таких идеях-принципах, как «Самодержавие. Православие. Народность».

1. Самодержавие подразумевало собой то, что русский народ не разделяет таких понятий как «царь» и «страна». Для людей это все является единым, гарантирующим счастье, силу и славу.

2. Православие означало, что русский народ является религиозным и почитает духовенство наравне с государственной властью. Религией можно решать вопросы, которые нельзя решить самодержавием.

3. Народность говорила о единстве всех народностей.

В 1832 г. впервые С.С. Уваров говорит и о воспитании молодого поколения, посредством образования: «...чтобы российское образование формировало достойных выпускников, необходимо реализовывать доставшиеся нам от предков три взаимосвязанных великих государственных начала...»[11]

Можно сделать вывод, что экстремистские настроения и акты проявления террора во время царской России по большей части отсутствовали. Но начали они проявляться с того момента, когда такая идеология постепенно переставала быть актуальной для народа. Первые акты террора были связаны с появлением различных политических движений, таких как партия «Народная воля» и ряд других. Начались покушения на убийства императоров. Самый пик таких движений пришелся на начало XX века. Это было связано с формированием большевицкой власти и в дальнейшем с проведением политики «красного террора».

Во время Советской власти, официальной идеологией являлся коммунизм, а именно та система идей, ценностей и идеалов, направленных на построение социального равенства и общественной собственности, что являлось главной целью построения коммунизма, параллельно отвергая либеральные и консервативные идеи. Как указывал Ф. Энгельс, «...коммунизм предполагает наличие высокоразвитых производительных сил, отсутствие государства, денег, без деления общества на социальные классы...»[15]

В соответствии с этим сущность патриотического воспитания сводилась к формированию таких морально-нравственных ценностей как: любовь к своей родине, воспитание детей, добросовестное отношение к труду, высокое осознание общественного долга, взаимоуважение, нетерпимость к несправедливости, межнациональным розням.

Государство играло большую роль в формировании патриотизма. В советские годы «печать, радио, телевидение, кино — это могучие средства идеологического воздействия. В советский период до 70 % городского и сельского населения смотрят телевизионные передачи. Все это создает

широкие возможности для идеологического воздействия, для духовного роста всех слоев населения, и прежде всего молодого поколения».[10]

Также, помимо работы или учебы люди активно участвовали в общественной жизни. Проводилось большое количество праздников и демонстраций. Основная цель государства заключалась в развитии общества и максимальном его сплочении.

Со сменой политико-экономического режима с начало 1990-х годов коммунистические идеи перестали быть актуальными, жизнь страны стала наполняться идеалами западной культуры. В большей степени это коснулось молодежи, что существует и сегодня.

Согласно ст. 13 Конституции РФ 1993 года в России признается идеологическое многообразие. Никакая идеология не может устанавливаться в качестве государственной или обязательной.[1] Это говорит об отсутствии какой-либо конкретной идеологии в нашем государстве.

С другой стороны, она должна быть, иначе не понятно, каким образом выстраивается система ценностных предпочтений, как обосновывается нормативная деятельность государства, его правовая политика, поэтому страна находится в состоянии неопределенности. Так и происходит с человеком, неустойчивость и неопределенность в нравственно-моральных ценностях, религии и жизненной цели, что является причиной возникновения экстремистских мотивов. Основной целью гражданского общества и государства является активное взаимодействие, достижение которого возможно достичь путем *социально-политического и экономического развития всех сфер жизни общества и государства в целом.*

Список литературы

1. "Конституция Российской Федерации" (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) // СПС Консультант Плюс;

2. Федеральный закон от 06.03.2006 № 35-ФЗ (ред. от 26.05.2021) «О противодействии терроризму», // Консультант Плюс [Электронный ресурс]: справочно-правовая система / СПС Консультант Плюс;

3. Федеральный закон от 29 декабря 2010 г. № 436-ФЗ (ред. от 18.12.2018) «О защите детей от информации, причиняющей вред их здоровью и развитию» // СПС Консультант Плюс;

4. Концепция противодействия терроризму в Российской Федерации (утв. Президентом Российской Федерации 5 октября 2009 г.) // СПС Консультант Плюс;

5. Постановление Правительства РФ от 30.12.2015 N 1493 (ред. от 30.03.2020) "О государственной программе "Патриотическое воспитание граждан Российской Федерации на 2016 - 2020 годы" // СПС Консультант Плюс;

6. Состояние преступности в России за январь-декабрь 2020 г.: статистический сборник. - Москва: ФКУ «ГИАЦ» МВД России, 2020. [Электронный ресурс] // Официальный сайт «МВД РФ» - Режим доступа: <https://мвд.рф/reports/item/27024130/>;

7. Состояние преступности в России за январь - июль 2021 г. [Электронный ресурс] // Официальный сайт «Генеральной прокуратуры» - Режим доступа: <https://genproc.gov.ru/>

8. Состояние преступности в России за январь-июль 2019 гг.: статистический сборник. - Москва: ФКУ «ГИАЦ» МВД России, 2019. [Электронный ресурс] // Официальный сайт «МВД РФ» - Режим доступа: <https://мвд.рф/reports/item/22678184/>;

9. Адлер М. Шесть великих идей. М. : МИФ, 2015;

10. Быков А. К. Патриотизм в контексте гражданско-нравственного становления школьников // Образование в современной школе. 2012. № 4. С. 12–15.;

11. Доклады министра народного просвещения С.С. Уварова императору Николаю I // Уваров С.С. Избранные труды. - М., 2010. - С. 53-54.

12. Крестина Е. А. Экстремизм и терроризм: концепты, законодательство, проблемы противодействия: учеб. пособие для вузов. Ставрополь, 2017

13. Патриотизм в США [Электронный ресурс] // Режим доступа: <http://www.us-visa.ru/info/life/patriotism.htm>;

14. Се Илин, Коврижных О. А. Об опытах патриотического воспитания студентов в Китае // Нижний Новгород: НОО «Профессиональная наука», 2016. С. 73-75.;

15. Энгельс Ф. Принципы коммунизма // Маркс К., Энгельс Ф. Соч. 2-е изд. М., 1955. Т. 4.

Барсукова А.П.,
Юридический институт,
АлтГУ, г. Барнаул.

Научный руководитель: Стародубцева М. А.
преподаватель кафедры уголовного права и криминологии
Юридический институт АлтГУ, г. Барнаул

Барсукова А.П. АНАЛИЗ ВЛИЯНИЯ НА МОЛОДЁЖЬ НЕПРИЕМЛЕМОГО КОНТЕНТА В СОЦИАЛЬНОЙ СЕТИ ТИК ТОК В 2021 ГОДУ

Как известно, в наше время социальные сети являются незаменимой частью жизни молодого поколения. С одной стороны, молодёжь за короткое время потребляет огромное количество информации, что является неотъемлемым достоинством, а с другой - именно подростки и молодежь является самой незащищённой группой населения от этого же самого контента. Ведь социальные сети также несут в себе огромное количество негативно влияющей на человека информации. Для того чтобы суметь защитить себя от подобного рода сведений, необходимо знать, какая негативная информация присутствует в социальных сетях и на что она может повлиять [3].

В январе 2019 года экспертами ВЦИОМ был проведён опрос среди взрослых и подростков (14–17 лет) на тему влияния социальных сетей на их поведение. В основном респонденты утверждали, что находили в Сети положительный контент. Однако 28% подростков сообщили, что видели сцены насилия, 16% – пропаганду наркотиков, 19% – призывы к самоубийствам [5].

Указанные статистические данные породили интерес для проведения собственного исследования и анализа сложившейся ситуации.

В проведённом мной исследовании приняли участие 44 респондента в возрасте от 14 до 30 лет. Респонденты являются учащимися колледжей или ВУЗов, либо уже имеют среднее специальное, либо высшее образование.

Доля мужчин, принявших участие в исследовании составила 34,9 %, доля принявших участие в исследовании женщин- 65,1%.

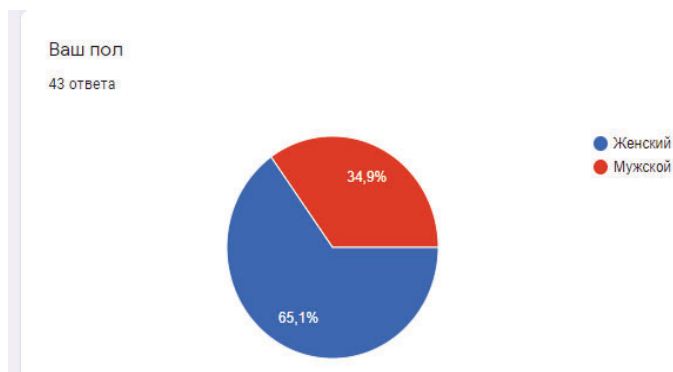


Рис 1. Половой состав участников исследования

Далее, нами был проанализирован возрастной состав участников исследования, а также степень осведомлённости аудитории исследования с существованием такой социальной сетью как Тик Ток.

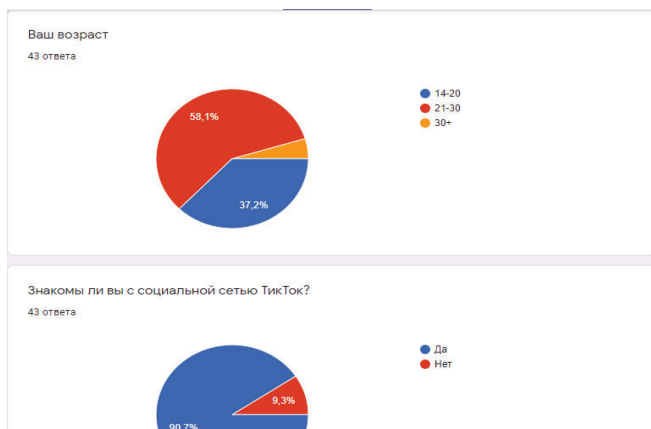


Рис 2. Возрастной состав участников исследования и степень узнаваемости социальной сети Тик Ток.

Комментируя данную диаграмму, можно прийти к выводу, что подавляющее большинство респондентов – молодёжь в возрасте от 14 до 30 лет. Именно данная возрастная категория непосредственно знакома с такой социальной сетью как Тик Ток. Подавляющее большинство опрошенных (более 90%) ответили, что знают, что такая интернет-площадка существует.

С учётом указанного, рационально утверждать, что в жизни молодёжи роль данной социальной сети – значительна.

Для подтверждения данной позиции, приведём следующую диаграмму, которая наглядно иллюстрирует, сколько часов в день респонденты проводят в социальной сети Тик Ток в день.



Рис. 3. Время, проводимое респондентами в социальной сети Тик Ток (в день).

Согласно данным диаграммы, 65 % пользователей уделяют менее 1 часа в день на просмотр ленты Тик Ток, 25% проводят в социальной сети 2-3 часа, 10% опрошенных более 4 часов в день уделяют просмотру видео на данной интернет-платформе.

В неделю, каждый из приведённых групп опрошенных человек будет проводить 7, 21, 28 часов в данной социальной сети соответственно.

По данным исследования RMIT University было выяснено, что многие люди зарегистрированы в подобных социальных сетях для того, чтобы вписаться в какую-то группу и быть «в тренде», что означает то же самое, что «идти в ногу со временем» или оставаться в курсе самых последних новинок в

определенной области. При этом участники не думают о последствиях, так как их мысли заняты погоней за популярностью. Часто индивид так стремится произвести впечатление и вписаться в определенную группу, что жертвует критическим мышлением и способен на неразумные поступки.

Очевидно, что такое поведение наиболее актуально для молодежи и лиц подросткового возраста, стремящихся к самоопределению, самовыражению и признанию окружающих [2].

Благодаря таким характерным для большинства индивидов психологическим особенностям в сети интернет распространяется множество трендов, способов самовыражения и образцов поведения. Чаще всего это позитивные или безобидные тенденции, направленные на развлечение пользователей, но, как мы убедились, иногда могут появляться явно деструктивные примеры, провоцирующие других пользователей на опасные, аморальные и противоправные действия, совершаемые не в виртуальном пространстве, а в реальном мире (расстрелы в учебных заведениях в России в 2020-2021 гг.).

Таким образом социальные сети в качестве инструмента воздействия на поступки и поведение человека достаточно эффективны. Спровоцировать молодого человека на подобные действия достаточно просто, многие сами будут готовы принять любой брошенный вызов, если это добавит им популярности.

Неприемлемый контент определяется в качестве грубого, либо нецензурного контента. В сети интернет, под неприемлемым контентом понимают контент, связанный с насилием. Контент, который касается событий или тем деликатного характера (таких как смерть, стихийные бедствия, техногенные катастрофы, нападение с применением насилия, общественные беспорядки и т. д.) и содержит какие-либо из следующих элементов: личные выпады, присвоение хэштегов, продажа товаров или услуг, политическая пропаганда, предложения или просьбы об увеличении количества читателей или другое неприемлемое содержимое [4].

Подавляющее большинство опрошенных хотя бы однажды встречало неприемлемый контент в социальных сетях, согласно рис. 4.

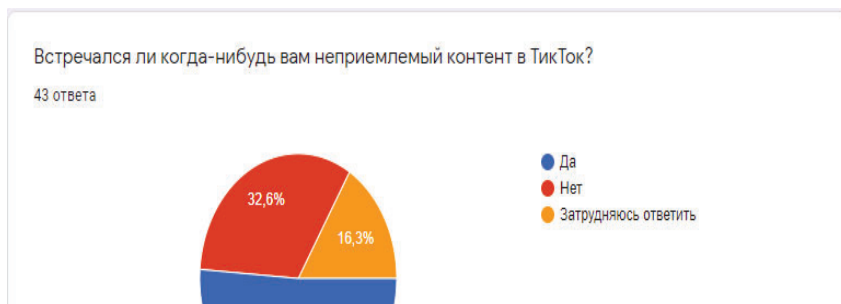


Рис. 4. Уровень осведомлённости пользователей о наличии неприемлемого контента в Тик Ток.

Далее, рационально будет проанализировать, какой неприемлемый контент, воздействующий на психику, встречался пользователям.

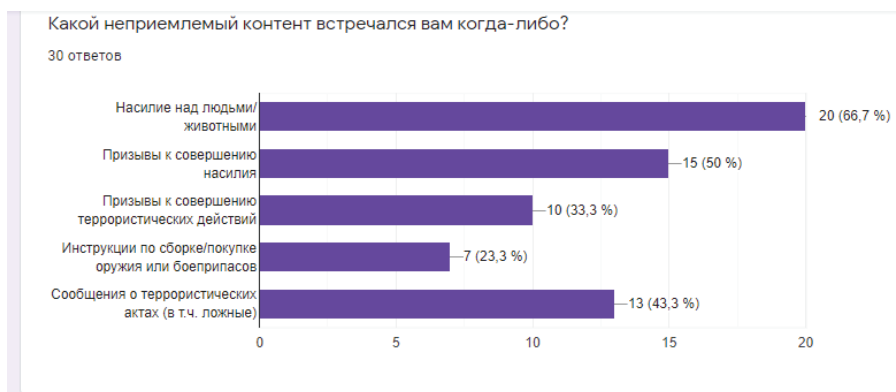


Рис. 5. Виды неприемлемого контента в Тик Ток.

Как видно из рис. 5., наибольшую долю неприемлемого контента занимает насилие над людьми или животными, либо призывы к совершению такого насилия.

На втором месте-сообщения о террористических актах-в том числе-ложные. Исследование проводилось в октябре 2021 года, во время обсуждения теракта, совершенного в одном из учебных заведений России, что и объясняет распространённость такого контента.

Реже пользователи встречались с призывами к совершению террористических действий, демонстрацией оружия, боеприпасов.

Далее, рационально рассмотреть реакцию пользователей на появление в их поле зрения такого контента.



Рис. 6. Реакция пользователей на неприемлемый контент

Как видно, 59% пользователей были обеспокоены либо встревожены появлением такого контента.

Естественно, если происходит террористический акт или другая вылазка террористов, в социальных сетях непременно сообщается об этой новости. Но, это играет на руку террористам, задача которых состоит в доведении до сведения общества информации о своих насильственных действиях, об угрозе их повторения для того, чтобы посеять страх у населения. Кроме того, само объявление о подобных событиях обостряет эмоциональный шок и ужас в обществе.

В действительности современные социальные сети характеризуются невероятной скоростью предоставления информации. В течение нескольких минут они способны представить зрителям любое событие, которое только что произошло в любом конце планеты. Выполняя свою работу, социальные сети передают и неожиданность, и тот шок, на который рассчитывают террористы [2].

С другой стороны, демонстрация указанного контента оказывает непосредственное влияние на криминогенную обстановку. Постоянная демонстрация такого контента порождает в сознании мысль о том, что насилие, угрозы и иное противоправное поведение-вполне нормально и приемлемо. Данная мысль популяризируется в современных социальных сетях.

Для неокрепшей психики молодёжи, которая не склонна к критическому мышлению, это может позиционироваться как прямой призыв к действиям.

В завершении опроса, респондентам было предложено оценить уровень организации проверки контента Тик Ток на приемлемость.

Считаете ли вы достаточным уровень организации проверки контента ТикТок на приемлемость?

42 ответа

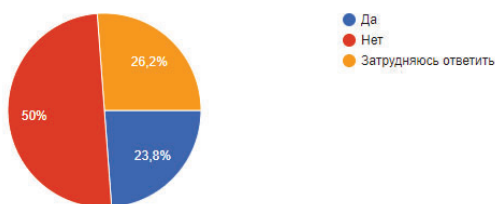


Рис. 7. Оценка уровня организации проверки контента в Тик Ток на приемлемость.

Как видно из рис. 7., лишь 23,8% пользователей довольны организацией процесса проверки контента, 50% считают, что меры, применяемые к проверке

контента недостаточны. Остальные опрошенные затруднились дать однозначный ответ.

Таким образом, можно подвести следующие итоги исследования:

1. Социальные сети оказывают огромное влияние на психику и сознание современного молодого человека;
2. Молодые люди проводят как минимум 1 час в день в социальных сетях;
3. На сегодняшний день существует реальная проблема воздействия вредоносного контента на психику молодёжи, что вызывает у них тревогу, страх и беспокойство;
4. Модераторы социальных сетей не создали действенной системы защиты от вредоносного контента;
5. Вредоносный контент непосредственно влияет на криминогенную обстановку.

Список литературы

1. Крок Луи Психологическое воздействие терроризма // Национальные интересы: приоритеты и безопасность. 2007. №9. URL: <https://cyberleninka.ru/article/n/psihologicheskoe-vozddeystvie-terrorizma> (дата обращения: 03.12.2021).
2. Медиакратия: современные теории и практики / Под ред. А.С. Пууо и С.С. Бодруновой. СПб: Изд-во С.- Петерб. ун-та, 2013.
3. Овчинникова Евгения Викторовна, Морозова Анна Анатольевна. Особенности негативного влияния контента социальных сетей на молодежную аудиторию (на примере «ВКонтакте») // Медиасреда. 2016. №11. URL: <https://cyberleninka.ru/article/n/osobennosti-negativnogo-vliyaniya-kontenta-sotsialnyh-setey-na-molodezhnyu-auditoriyu-na-primere-vkontakte> (дата обращения: 03.12.2021).

4. <https://business.twitter.com/ru/help/ads-policies/ads-content-policies/inappropriate-content.html>
5. <https://www.cism-ms.ru/poleznye-materialy/kakoe-vliyanie-negativnyy-kontent-okazyvaet-na-psikhiku-podrostkov/>

Юлин М.А., магистрант Юридического
института АлтГУ, г. Барнаул

Научный руководитель: Мазуров В.А., кандидат юридических наук,
доцент кафедры уголовного права и криминологии АлтГУ

Юлин М.А. КОНТРОПАГАНДА ИДЕОЛОГИИ ТЕРРОРИЗМА И ЭКСТРЕМИЗМА

За последние годы в России проблемы экстремизма и терроризма набирают серьезные обороты. Согласно статистическим данным Главного информационно-аналитического центра Министерства внутренних дел РФ, количество зарегистрированных преступлений экстремистской направленности в 2020 году составило 833, преступлений террористического характера - 2342. В 2019 году данное количество составляло 585 преступлений экстремистской направленности и 1806 преступлений террористического характера, т.е. по сравнению с 2019 годом, в 2020 году количество преступлений экстремистской направленности выросло на 42,4%, а террористического характера на 29,7% [1]. Данные виды преступлений представляют большую угрозу, т.к. они являются одним из наиболее опасных явлений, угрожающих как мировому сообществу, так и Российской Федерации в частности, и как правило они направлены на разрушение общепризнанных норм, устоев и ценностей в различных сферах общественной жизни, как политической, экономической, так социальной и духовной.

В данный момент времени наблюдается активность зарубежных спецслужб, которые занимаются идеологической обработкой граждан. Для достижения своих результатов, они активно используют социальные сети, средства массовой информации, видеоплощадки для пропаганды экстремистских взглядов. Информация в Интернете не фильтруется и не блокируется должным образом, доступ к ней имеют практически все. Интернет на данный момент основное и очень мощное оружие по информационному

воздействию на человека, которое активно используется спецслужбами. Под его воздействием развращается и обезличивается молодежь, утрачивает свою самобытность, национальную веру и идеалы. В тоже время разжигается ненависть между разными слоями общества, различными национальностями, религиями и т.п. Сейчас пропаганда спецслужб сконцентрирована на указание на социальное положение граждан в нашей стране, указывая на низкий уровень жизни в сравнении с другими, более развитыми. Это толкает людей на совершение противоправных действий, в том числе уголовно наказуемых. Люди выходят на незаконные митинги и шествия, нарушая общественный порядок, совершают насильственные действия в отношении представителей власти и других граждан, повреждают чужое имущество. Людей в прямом смысле стравливают друг с другом и заставляют идти на крайние меры в борьбе друг с другом, властями, правительством. Также с действиями иностранных спецслужб связывают появление такого вида преступления как скулшутинги, то есть массовые, беспорядочные убийства в образовательных учреждениях, ранее неизвестные в российской действительности. Повышена активность в сфере пропаганды суицида.

В Российском законодательстве, а именно в статье 3 Федерального закона от 06.03.2006 N 35-ФЗ (в редакции от 26.05.2021) «О противодействии терроризму», терроризм определяется как идеология насилия и практика воздействия на принятие решений органами государственной власти, органами местного самоуправления или международными организациями, связанные с устрашением населения и (или) иными формами противоправных насильственных действий. Терроризм по своей сути, есть крайняя форма проявления экстремизма, является отражением экстремистской идеологии. Термин «экстремизм» происходит от латинского слова *extremus* - крайний. В справочной литературе под экстремизмом традиционно принято понимать «приверженность к крайним взглядам и мерам». Легально данный термин закреплен в пункте 1 статьи 1 Федерального закона от 25 июля 2002 г. N 114-ФЗ «О противодействии экстремистской деятельности». Согласно данной

статье, экстремистская деятельность (экстремизм) – составное определение, которое включает в себя 13 действий. Из них можно сделать краткое определение, что основой экстремизма являются радикальные высказывания и действия на основе человеческого недовольства в отношении правительства, конституционного строя, каких-либо политических движений, общественных организаций, а также радикальной нетерпимости в отношении других членов общества, которые имеют религиозное, идеологическое, социальное, политическое, национальное, языковое или расовое отличие, в том числе культивация и пропаганда таких взглядов [4].

В России до сих пор не отработаны четкие методы противодействия идеологии экстремизма и терроризма. Для борьбы с идеологией терроризма и экстремизма может оказаться действенным средством разработка и утверждение государственной идеологии. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) в статье 13 указывает на то, что в Российской Федерации признается идеологическое многообразие; никакая идеология не может устанавливаться в качестве государственной или обязательной, а так же запрещается создание и деятельность общественных объединений, цели или действия которых направлены на насильственное изменение основ конституционного строя и нарушение целостности Российской Федерации, подрыв безопасности государства, создание вооруженных формирований, разжигание социальной, расовой, национальной и религиозной розни. Также, в пункте 2 статьи 29 Конституции не допускаются пропаганда или агитация, возбуждающие социальную, расовую, национальную или религиозную ненависть и вражду. Запрещается пропаганда социального, расового, национального, религиозного или языкового превосходства. Соответственно в Российской Федерации разрешена любая идеология, кроме той, которая направлена на возбуждение социальной, расовой, национальной или религиозной ненависти и вражды, пропаганды социального, расового, национального, религиозного или языкового превосходства; идеологии,

направленные на насильственное изменение основ конституционного строя и нарушение целостности Российской Федерации, подрыв безопасности государства, создание вооруженных формирований.

На сегодняшний день, в научном сообществе идет активная дискуссия о том, требует ли изменения ч. 2 ст. 13 Конституции РФ, запрещающая установление государственной идеологии. Некоторые авторы считают, что государство и идеология не должны смешиваться, а должны идти параллельными курсами. По мнению И.Н. Глебова, «идеология — это работа не отдельных выдающихся партийцев, и не экспертный продукт маститых умников, но тщательное понимание властью существа и нюансов российской общественной жизни. Идеология определяет общий смысл власти, позволяет людям с разным достатком и достоинством чувствовать себя единым народом». Для В.В. Семенович и К.А. Попова справедливой видится критика данной конституционной нормы. А.П. Погорелов утверждает, что «государственная идеология» и «обязательная идеология», запрещенные Конституцией РФ – категории не синонимичные. Государственная идеология должна предполагать систему взглядов и ценностей, в качестве ориентиров развития всего общества, однако, это не должно означать, что не допускается наличие иных концепций и воззрений на государственную действительность и перспективы государственного развития [3].

Идеология существовала на всех этапах развития Российского государства. Для большего понимания, на основе чего необходимо строить идеологию, необходимо обратиться к истории России, а именно к идеологиям СССР и Российской Империи.

Основой идеологии царской России была так называемая триединая формула. Данная триединая формула основ образования – православие, самодержавие, народность, высказанная Уваровым в 1832 г., вскоре начала распространяться на все сферы культурной жизни России. Понятие православие в этой формуле трактовалось не только как церковный догмат, но и как беспрекословное гражданское повиновение государственной власти,

освященной религией. Православие, объединявшее в себе основные общечеловеческие ценности, не противоречило взглядам верующих других конфессий, широко представленных в стране. По существу, это означало политику веротерпимости [2]. То есть во главе государства был царь самодержец и все выполняли его волю через призму православия, которое учило борьбе с человеческими пороками и грехом, а также в первую очередь исполнения таких добродетелей, как любовь, терпимость и самопожертвование в отношении ближнего, в том числе, если он другой веры и национальности, а также постоянному труду на благо Отечества и во славу Божью.

Основой идеологии в СССР было достижение общего блага, всеобщее взаимоуважение, почтение старших, своей истории и т.п. Одной из самых важных ценностей была семья, ведь именно семья была важной ячейкой советского общества. Также нельзя не упомянуть моральный кодекс строителя коммунизма, текст которого был прописан в уставе КПСС, принятом на XXII съезде КПСС в 1961 году. В моральном кодексе содержались положения о любви к социалистической Родине, к странам социализма; добросовестном труде на благо общества; нетерпимости к нарушениям общественных интересов; товарищеской взаимопомощи; взаимном уважении между людьми, нравственной чистоте; простоте и скромности в общественной и личной жизни; взаимном уважении в семье, заботе о воспитании детей; непримиримости к несправедливости, туеядству, нечестности; нетерпимости к национальной и расовой неприязни.

Соответственно, для противодействия идеологии терроризма, считаю необходимым разработать идеологию, направленную на контрпропаганду идеологии терроризма и экстремизма, которая будет основываться на идеологиях СССР и Российской Империи, а именно, на народности (единство государства и народа), уважении и взаимопомощи к окружающим людям, воспитании высокой нравственности и культуры, стремлении к саморазвитию, нетерпимости к правонарушениям, религиозной и национальной неприязни.

Идеология способна повлиять на повышение уровня нравственности населения, его правосознание и правовую культуру, что положительно скажется на контрпропаганде терроризма и экстремизма. На повышение уровня нравственности и правосознания населения также может оказать влияние углубленное изучение истории России в школах и институтах, текста Конституции РФ, расширенное использование государственных символов Российской Федерации, например ежедневное поднятие флага РФ, проигрывание Государственного гимна по радио.

Для борьбы с пропагандой экстремизма и терроризма в долгосрочной перспективе важно развитие правового самосознания и нравственности, воспитание молодого поколения в духе патриотизма и веротерпимости, что необходимо для обеспечения безопасности общества в целом. В данный момент времени, необходимо проведение следующих мероприятий:

- Выявление в социальных сетях, средствах массовой информации, видеоплощадках экстремистских материалов, фиксация данной информации, определение ее источника и блокирование;
- Активное информационное противодействие экстремизму и терроризму в сети Интернет, например, организация тематических групп, форумов, опросов общественного мнения и других мер;
- Просвещение граждан о негативном влиянии экстремизма и терроризма на общество и государство. Формировать у них активную гражданскую позицию, призывать к равнодушию в желании устранить подобные настроения;
- Возможность использования лидеров мнений для контрпропаганды идеологии терроризма и экстремизма (распространение ими профилактических материалов, которые будут вписываться в тематику, привычную для его аудитории, тем самым влияя на ее настроения).

Угроза терроризма будет сохраняться до тех пор, пока существуют источники и каналы распространения экстремистской идеологии.

Противодействие идеологии терроризма и экстремизма в РФ – это одна из наиболее важных задач обеспечения безопасности на государственном уровне.

Список литературы

1. Зайцев А.В. Анализ статистических показаний и выявление причин совершения преступлений в сфере экстремистской деятельности в Российской Федерации // Евразийское Научное Объединение. 2020. № 10-5 (68). С. 357-359.

2. Леванов Б.В. «История России XIX-XX вв.»: учебное пособие по дисциплине ГСЭ.Ф.03 «Отечественная история» для студентов вузов неисторических специальностей. / Б.В. Леванов, В.А. Корнилов, В.В. Рябов. – М.: Владос, 2008. 605 с.

3. Семенова В.В., Попов К.А. Проблемы формирования идеологии в современной России // Тенденции развития науки и образования. - 2021. - №70-6.

4. Слисаренко А.А., Мигущенко О.Н. Идеологическое противодействие экстремизму в современной России // Современная наука в условиях модернизационных процессов: проблемы, реалии, перспективы. - Уфа: Общество с ограниченной ответственностью "Научно-издательский центр "Вестник науки", 2021.

Зеленко А.Б.,

Юридический институт,

АлтГУ, г. Барнаул.

Научный руководитель: Стародубцева М. А.

преподаватель кафедры уголовного права и криминологии

Юридический институт АлтГУ, г. Барнаул

Зеленко А.Б. ПРОБЛЕМА ОСВЕДОМЛЕННОСТИ ГРАЖДАН ОТНОСИТЕЛЬНО ЦИФРОВЫХ АСПЕКТОВ ТЕРРОРИЗМА

Чтобы выявить сущность проблемы терроризма в современном мире, следует выяснить, что означает данный термин. Под словом «терроризм» подразумевают один из вариантов политической борьбы, связанный с идеологически мотивированным насилием. Его суть состоит в насилии для устрашения населения. Как правило, теракты подготавливают отдельные лица либо организации. Их целью становится власть в лице отдельных чиновников или общество в лице гражданского населения. Также террористы могут нанести удар по частному или государственному имуществу, по важным инфраструктурам и системам жизнеобеспечения. Цель преступников – добиться желаемого для них развития событий, как правило, это дестабилизация обстановки в стране, разжигание революции, объявление войны, обретение независимости некоторой территории, получение уступок от действующей власти и другое.

Хотя терроризм – глобальная проблема современного мира, законодатели разных стран не пришли к единому мнению в его определении. В большинстве государств терроризмом считаются деяния, которые опасны для общества. При этом совершены они с целью устрашения населения или его социальных групп. Цель террориста состоит в том, чтобы привлечь к преступлению как можно больше внимания. При этом он хочет воздействовать на какое-либо решение, ранее принятое властями страны. Терроризм тесно связан с более общим

понятием – террор, который является одним из способов управления народным мнением посредством устрашения. К такому способу воздействия прибегают как государства, так и различные организации, которые таким путем пытаются решить политические вопросы.

Чтобы выяснить, какие существуют проблемы терроризма в современном мире, кратко необходимо описать цели преступников, которые они преследуют при совершении акта насилия. Они заключаются в следующем:

1. Демонстрация бессилия власти. В том месте, где произошло преступление, власть утратила свою силу. В этом месте были нарушены законы и мораль, установилась альтернатива действующему управлению.

2. Пропаганда действием. Произведенный акт насилия заставляет некоторых членов общества сочувствовать террористам, а также присоединяться к их рядам.

3. Возникновение антиправительственных настроений, активизация работы оппозиционных сил, поскольку теракт трактуется как признак слабости государственного строя. Все эти действия толкают власть к уступкам.

4. Преступление отрицательно сказывается на экономике страны, где произошел инцидент. Ухудшается имидж города, снижается поток туристов.

5. Террористы подталкивают страну к смене политического курса. Часто цель бандитов заключается в переходе власти к авторитарной форме правления.

Указанные данные породили интерес для проведения собственного исследования и анализа сложившейся ситуации.

В проведённом мной исследовании приняли участие 10 респондентов в возрасте от 18 до 30 лет. Респонденты являются учащимися Алтайского Государственного университета.

Доля женщин, принявших участие в исследовании составила 50%, доля принявших участие в исследовании мужчин - 50%.

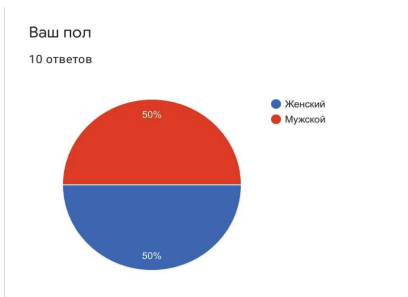


Рис 1. Половой состав участников исследования

Далее, мной был проанализирован возрастной состав участников исследования, а также степень осведомлённости аудитории исследования о понятии терроризма.

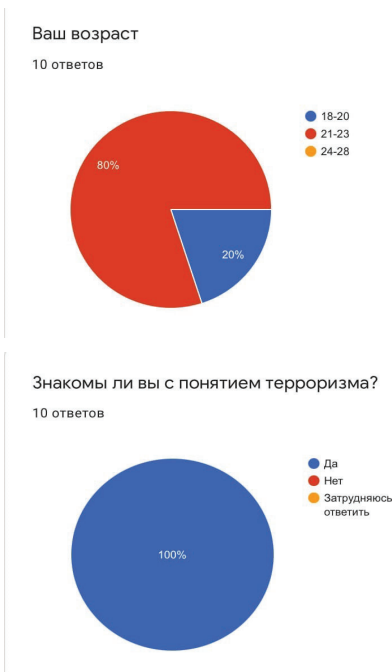


Рис 2. Возрастной состав участников исследования, а также степень осведомлённости аудитории исследования о понятии терроризма

Комментируя данную диаграмму, можно прийти к выводу, что большинство респондентов – молодёжь в возрасте от 21 до 23 лет, среди которых абсолютно все имеют представление и знания о понятии терроризма.

Далее был вопрос на предмет того, сталкивались ли участники опроса с проявлением терроризма в той или иной степени, большинство опрошиваемых видели, либо же слышали из различных источников, читали в новостях, в общем в той или иной степени наблюдали/были свидетелями данного явления.

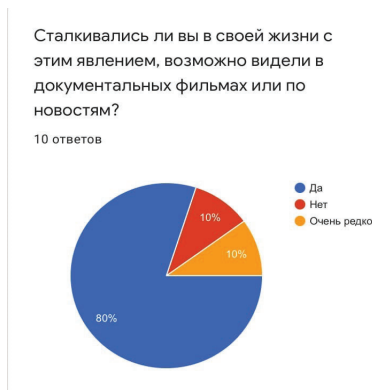


Рис 3. Наблюдение терроризма в повседневной жизни

Эти результаты говорят нам о том, что в повседневной жизни, будь то прочтение книги, просмотр фильма, прямое наблюдение и т.д., те или иные формы терроризма часто официруются и имеют своё место в глазах народа. Но тем не менее, 1 из 10 опрошиваемых не сталкивался с формами проявления терроризма за рамками юриспруденции.

Затем респондентам был задан вопрос касательно участников террористических действий.

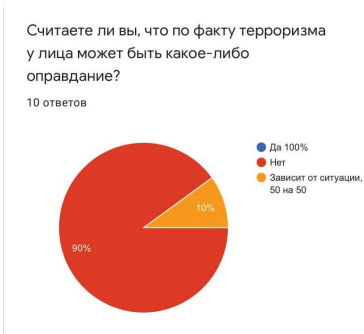


Рис 4. Существование оправдательного факта.

И вновь ответ практически однозначен. Подавляющее большинство опрошиваемых не находят для себя никаких оправданий действиям террористов.

Далее респондентам был задан вопрос, отражающий их отношение и оценку работы государства в рамках борьбы с терроризмом.

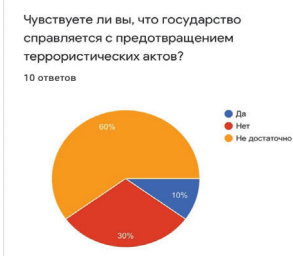


Рис 5. Оценка работы государства

В данном вопросе опрошиваемые вновь были схожи во мнении и 90% из них в той или иной степени не довольны осуществляемой в нашей стране работой по предотвращению и устранению терроризма.

Последним вопросом хотелось убедиться в том, какой инструмент влияния в терроризме наиболее сложен к устранению.

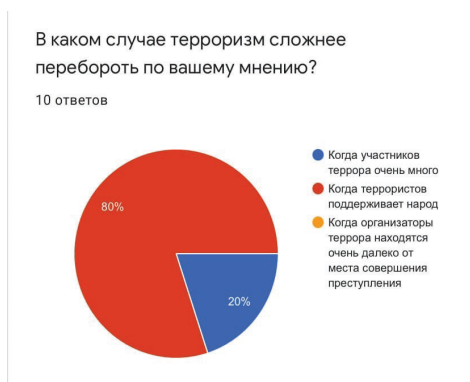


Рис 6. Сложность в устранении террористического акта и проявления терроризма.

8 из 10 опрошиваемых среди предложенных вариантов выбрали пункт, указывающий на поддержку терроризма народом как самый тяжело устранимый для государства.

И действительно, не смотря на то, сколько участников террористических действий и независимо от места их нахождения, главным признаком стихийности и, соответственно, сложности в предотвращении таких действий является поддержка народа, что свидетельствует уже об определённых настроениях в обществе и в таком ключе проблема становится более глобальной.

Подводя итог и говоря о методах противодействия терроризму отметим, что правовая основа антитеррора – Конституция РФ, нормы международного права, федеральные законы, отдельные правовые акты Президента и Правительства РФ, Уголовный Кодекс РФ. Также разработана стратегия и комплексный план противодействия идеологии терроризма.

Важная составляющая антитеррора – перекрытие источников финансирования группировок. А их немало: нелегальная продажа нефти, предметов старины, наркоторговля, ограбление банков и частных лиц, рэкет, торговля заложниками, пожертвования от пособников.

Террористам необходима поддержка среди населения. Поэтому борьба с этим явлением предполагает не только изоляцию его идеологов и практиков. Такие меры эффективны, но недостаточны.

Если используются только силовые методы – это борьба не с терроризмом, а с его проявлениями. Поэтому противодействие терроризму обязательно включает профилактику.

Важно сделать так, чтобы подобные идеи не пользовались популярностью у населения, привить «иммунитет» к попыткам вовлечения в эту разрушительную деятельность.

Здесь потребуется:

1. внедрение в общественное сознание установки толерантности и уважения многообразия культур, бесперспективности устрашающего насилия под любыми лозунгами;

2. разъяснение подросткам и молодежи разрушительной сути этого явления;

3. информирование населения о неотвратимости наказания за причастность к террористической деятельности (лучше – на конкретных примерах);

4. создание положительного имиджа властных органов и сотрудников спецслужб – для укрепления мотивации у населения помогать в деле антитеррора;

5. разоблачение мифов, в которых экстремисты и террористы предстают героями и борцами за справедливость, развенчание их лозунгов и пропагандистских приемов.

Еще один важный момент, составляющий систему противодействия терроризму – устранение последствий подобных проявлений. Это аварийно-спасательные работы, медицинская помощь, восстановление разрушенного, компенсация вреда пострадавшим. Действия властей в данном случае основываются на недопущении людских потерь, на приоритете жизни и здоровья человека.

Террористов необходимо обезвреживать и наказывать, но искоренить это явление только полицейскими методами не получится.

Победа возможна при условии создания атмосферы неприятия терроризма и осознания его разрушительной сути. Борьба с террористами – прерогатива государства, но победить их может только общество.

Список литературы

1. Скребец Е.С., Краснодарский университет МВД России / Борьба с терроризмом в Российской Федерации: концепция и методология.

2. Магомедова, Э. А. Причины развития современного терроризма // Молодой ученый. — 2018. — № 43 (229). — С. 127-129.

3. Шегаев И.С. «Терроризм: история и причины возникновения» // Молодой ученый. — 2013.

Бойцова А.А.,

Юридический институт,

АлтГУ, г. Барнаул.

Научный руководитель: Стародубцева М. А.

преподаватель кафедры уголовного права и криминологии

Юридический институт АлтГУ, г. Барнаул

Бойцова А.А. ОТРИЦАТЕЛЬНОЕ ВЛИЯНИЕ ДОРАМЫ «ИГРА В КАЛЬМАРА» НА ЗРИТЕЛЕЙ. МИФ ИЛИ РЕАЛЬНОСТЬ?

В середине октября "Лига безопасного интернета" попросила психологов проверить сериал «Игра в кальмара» на предмет опасности для детей и подростков и дать свою оценку.

"Лига безопасного интернета" получила несколько обращений от родителей в связи с выходом на Netflix "Игры в кальмара". Многие в нашей стране и за ее пределами обеспокоены сериалом. Они считают, что у некоторых зрителей, особенно у молодежи, может возникнуть соблазн повторить сцены из "Игры в кальмара", - написала директор организации Екатерина Мизулина в своем Telegram-канале.

По словам Мизулиной, тревогу вызывает то, что "все убийства в фильме поданы настолько легко и непринужденно, что любой молодой человек подумает, насколько легко можно организовать и реализовать такое преступление".

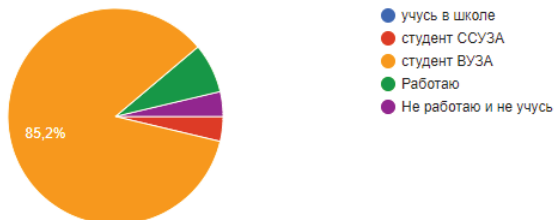
Моё исследование основано на социальном опросе молодёжи, как одной из потенциальных групп риска, и позволит узнать объективность вышеуказанных опасений общественности.

Исследование:

Вопрос 1 позволил определить категорию лиц, проходящих опрос и объективность их восприятия (учащиеся школы более восприимчивы к транслируемой жестокости, чем студенты ССУЗов и ВУЗов и т.д.)

Выберите тип Вашей занятости?

54 ответа



Учатся в школе – 0

Студенты ССУЗа - 2

Студенты ВУЗа - 46

Работаю - 4

Не работают и не учатся – 2

Вопрос 2 позволил отсеять тех, кто не понимал суть рассматриваемой проблемы и чьи ответы, соответственно, не могли быть объективными. Для резидентов ответивших «нет» опрос завершался.

Смотрели ли вы дораму "Игра в кальмара"?

54 ответа



Да – 28

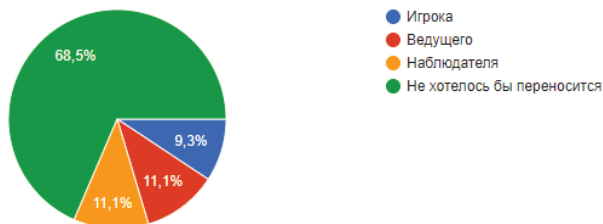
Видел частично по новостям в соц. сетях/ рассказывали друзья - 18

Нет – 8

Вопрос 3 позволил определить заинтересованность процессом игры, отражаемой в сериале, и готовностью стать её участником. (Игроки – преследуют чувство наживы, имеют чётко выраженную «готовность на всё» ради достижения собственных целей, попустительское отношение к моральным ценностям; Ведущие – абсолютное безразличие к моральным ценностям, азарт, проецируемый на смертельные игры, склонность к садизму; Наблюдатели – безразличное отношение к моральным ценностям, люди высокого положения, не привыкшие получать отказы, уверенность в своей безнаказанности, получают удовлетворение при садизме)

Если бы Вы могли перенестись в дораму, какую роль бы заняли?

54 ответа



Игрока – 5

Ведущего - 6

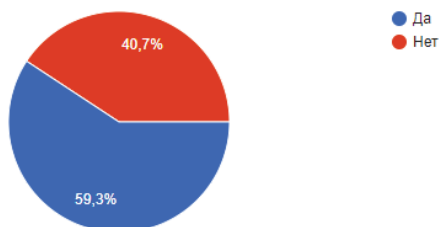
Наблюдателя – 6

Не хотелось бы переноситься - 37

Вопрос 4 позволил определить отношение к жестокости, проецируемой в сериале

Считаете ли Вы жестокими концепт игр, показываемых в сериале?

54 ответа



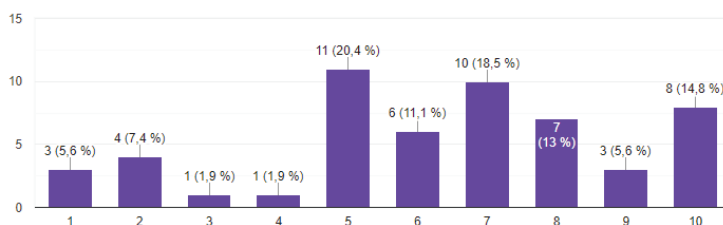
Да – 32

Нет - 22

Вопрос 5 предметно показал отношение молодёжи к жестокости в сериале (исходим из логики: чем выше человек оценил жестокость, тем сильнее будет в нём сопротивление при совершении преступления. Условно: «10» - не пойдут на совершение преступления, связанного с жестокостью, «1» - скорее всего совершат/ совершили преступление, связанное с жестокостью)

Оцените жестокость, описанную в драме?

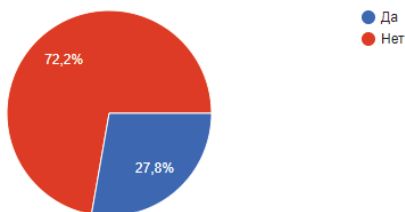
54 ответа



Вопрос 6 носил статистический характер о личном мнении каждого резидента о дурном влиянии «Игры в кальмара» на зрителей (своеобразное доказательство актуальности исследования)

Как Вы считаете, может ли эта дорама побудить к жестокости зрителей?

54 ответа



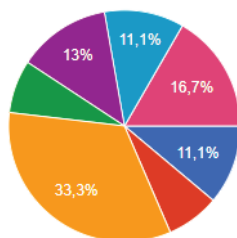
Да – 15

Нет - 39

Вопрос 7 позволил изучить отношение резидентов к аморальным ценностям, проецируемым в каждом раунде игры («Стой или беги», «сахарные соты» - стартовые раунд, не дающие чёткого понимания того или иного отношения к аморальным ценностям; «судная ночь» - предоставление людей самим себе, нагнетание обстановки для осознания что выживет только один – готовность идти по головам, маниакальные наклонности, поощрение преступного поведения, которое привело к раскрытию потенциала убийцы, склонность к самосуду; «перетягивание каната» - формирование группировок, проецирование идеи «выживает сильнейший», отсеивание слабых групп; «стеклянные шарик» - своеобразный крайний моральный барьер, выражающийся в убийстве близкого/ родного человека своими руками, окончательное разделение игроков, доведение их до границы беспощадности к окружающему для достижения своих целей; «закалённое стекло» - давление и угнетение обществом, смертельный риск, желание выжить любой ценой; «в игре нет жестоких раундов» - низкая моральная просвещенность, отрицание общепринятых норм поведения, скрытая безжалостность к окружающим)

Самый жестокий раунд в игре по Вашему мнению?

54 ответа



- Стой или беги
- Сахарные соты
- Судная ночь
- Перетягивание каната
- Стекланные шарики
- Закалённое стекло
- В игре нет жестоких раундов

Стой или беги – 6

Сахарные соты - 4

Судная ночь – 18

Перетягивание каната - 4

Стекланные шарики – 7

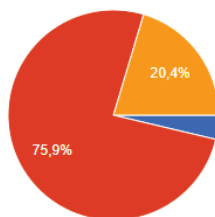
Закаленное стекло - 6

В игре нет жестоких раундов – 9

Вопрос 8: носил статистический характер о личном мнении каждого резидента по вопросу запрета дорамы «Игра в кальмара» на территории РФ (зрительская осознанность и проведение параллели с аналогичным по жестокости кинопроектом)

Нужно ли запретить показ этой дорамы на территории РФ, так же как показ аниме "Тетрадь смерти"?

54 ответа



- Конечно!
- Нет необходимости вводить запрет
- Не смотрел аниме "Тетрадь смерти"

Конечно! - 2

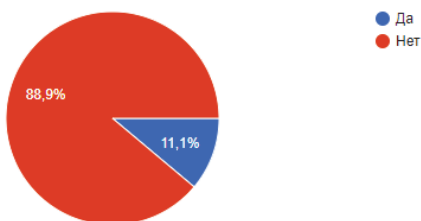
Нет необходимости вводить запрет – 41

Не смотрел аниме «Тетрадь смерти» - 11

Вопрос 9 позволил углубиться в уровень аморальности резидентов («да» - потенциальные садисты)

Решились бы Вы убить/ причинять тяжкий вред человеку, если бы об этом никто не узнал?

54 ответа



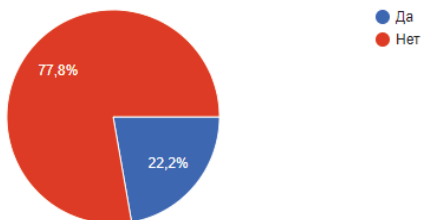
Да – 6

Нет – 48

Вопрос 10 дал понимание границы «не совершения» преступления. 100 млн. руб. было взято как условная сумма, позволяющая улучшить качество жизни в области проживания и иных социальных нужд (в сравнение с предыдущим вопросом число потенциальных садистов/ преступников выросло в двое)

Согласились бы Вы убить человека, если бы могли выиграть 100 млн. руб. ?

54 ответа



Да – 12

Нет – 42.

Хоть при подведении итогов и были обнаружены недочёты в проведённых исследованиях, те результаты, которые были получены, всё равно оказались впечатляющими.

Если бы со 100% уверенностью можно было сказать, что ответы резидентов были правдивыми, то можно ужаснуться количеству потенциальных маньяков/убийц в своём окружении.

Более того большинство вопросов показало заниженные моральные ценности, потому что резиденты ставили в приоритет жестокости варианты, где речь идёт о жизни чужих людей, чем вариант, где речь шла о жизни людей близких/родных.

По вопросу запрета данной драмы можно сказать следующее: «он нелогичен». Вместо этого стоит повышать культурную просвещённость молодёжи и прививание моральных ценностей, а также уважительное отношения к институту семьи.

Помимо этого, стоит отметить, что необходимо проработать создание условий, при которых станет невозможным расклад событий, приближенных к показанным.

Вдовинков С.С.,

Юридический институт,

АлтГУ, г. Барнаул.

Научный руководитель: Стародубцева М. А.

преподаватель кафедры уголовного права и криминологии

Юридический институт АлтГУ, г. Барнаул

**Вдовинков С.С. ПСИХОЛОГИЧЕСКИЕ АСПЕКТЫ
КИБЕРТЕРРОРИЗМА**

Жизнь современного человеческого общества все больше перетекает в виртуальное пространство, которое представляет собой «пространство, созданное компьютерной системой, как обозначение всего диапазона информационных ресурсов, доступных через компьютерные сети». В настоящее время Интернет – это постоянно растущее и видоизменяющееся информационное пространство: сайтов-новостей разных тематик и мнений, сайтов государств и отдельных личностей, госучреждений и частных компаний, социальных сетей, платежных систем и банков, «облачных» онлайн-хранилищ, вмещающих терабайты информации: от мультимедийных файлов до секретной информации. Повсеместное использование интернета в деловых и личных целях ведет к тому, что многие сферы современной жизни прочно основываются в виртуальном пространстве, которое становится местом повышенной опасности для его пользователей.

Целью данной статьи является определение основных причин, способствующих развитию и росту преступлений в виртуальном пространстве, а также выделение особенностей личности, предрасположенной к киберпреступлениям.

Согласно Акопову Г.Л., «кибертерроризм – несанкционированное вмешательство в работу компонентов компьютерных сетей общего пользования, вызывающее дезорганизацию работы элементов инфраструктуры

политически значимых институтов общества, причинение морального и материального ущерба, а также иные социально опасные последствия»

Автор определяет киберпреступника как пользователя компьютера, нарушившего законодательство с использованием сети общего пользования.

Учитывая своеобразие киберпространства, для психологической характеристики личности киберпреступника необходимо изучение следующих направлений:

- 1) общих особенностей интернет-среды;
- 2) психологии отдельных категорий преступников.

Развитие и рост информационных технологий позволяет кибертеррористам извлекать прибыль при низком риске, использовать информационные ресурсы для финансовых и организационных вопросов, обеспечивать связи, планировать и организовать акты терроризма, осуществляя всеохватывающий контроль над их проведением. Последние события показывают, что виртуальное информационное пространство становится «пристанищем» национальных террористических организаций, где они имеют возможность изучить весь контингент пользователей, провести пропаганду и сбор, минуя контроль государственных органов. Многочисленные социальные сети, чаты и форумы идеально приспособлены для создания анонимных переписок и передачи зашифрованных посланий, технологии позволяют распознавать карты и фотографии, что способствует легкой организации мест для теракта. Тем самым интернет является недорогим средством осуществления своей деятельности, а также сложным для выявления самих террористов.

Выделим несколько особенностей преступлений в виртуальном пространстве в дополнение к вышеприведенным.

- 1) Среда, образованная электронным устройством и сетями – меняется психологическое содержание взаимосвязей «преступник – электронное устройство (сеть) – потерпевший», что способствует устранению социального взаимодействия и материальной составляющей.

2) Анонимность – предполагает предоставление ложной информации, скрытность, защиту, ощущение безнаказанности, отсутствие механизмов порицания. Анонимность позволяет создавать разные образы личности, отличающиеся от реальности, что может вызвать у преступников различные расстройства типичных пользователей интернета: интернет-зависимость, тревожные расстройства, диссоциативные расстройства личности.

3) Психологические процессы – совершение киберпреступлений не требует присутствия непосредственно на месте, т.е. преступник может находиться дома в комфортной обстановке, отчего исчезает чувство дискомфорта, страха быть обнаруженным и задержанным. Киберпреступники не имеют возможности в полной мере оценить ущерб, увидеть реакцию жертвы, отчего не чувствуют раскаяние, а, наоборот, при удачно спланированном преступлении, удовлетворении своим результатом закрепляют образ акта преступного поведения.

4) Минимизация власти – чувство равенства в виртуальном пространстве, что возникает из-за опосредованного восприятия составляющих высокого социального статуса и положения. По мнению Макса Килгера, кибертеррористы имеют несколько мотивов для своей деятельности: жажда славы, легкий способ разбогатеть, политические разногласия, розыгрыш. На первое место он поставил деньги и легкий способ заработка: отмечено, что убытки, связанные с киберпреступлениями, увеличиваются каждый год, а любителей внести сбой в компьютерной системе становится гораздо больше – доступ к интернету и компьютеру имеется у подавляющей части общества.

На наш взгляд наиболее точная типология личности представлена А.Н. Косенковым, Г.А. Черным. Авторы выделили 7 типов личности, имеющих склонность к совершению киберпреступлений:

- 1) корыстный тип;
- 2) насильственный тип;
- 3) сексуальный тип;
- 4) социально-дезорганизирующий тип;

- 5) идеологически или политически мотивированный тип;
- 6) статусный тип;
- 7) исследовательский тип.

1) Корыстный тип – получение финансовых средств или специфических предметов, имеющих ценность в виртуальном пространстве, как с целью продажи, так и для личного пользования и коллекционирования.

2) Насильственный тип – доведение до самоубийства, угрозы, запугивания посредством электронных сетей и устройств.

3) Сексуальный тип – незаконное распространение порнографических материалов, принуждение к действиям сексуального характера.

4) Социально-дезорганизирующий тип – нарушение социальных норм и оказанием деструктивного влияния на общество и отношения.

5) Идеологически или политически мотивированный тип – форма протеста, идеологической или политической борьбы (в преддверии выборов).

6) Статусный тип – получение высокого неформального статуса в сообществах киберсоциума.

7) Исследовательский тип – изучение программных и аппаратных составляющих устройств и сетей, поиск уязвимостей, возможности дальнейшего использования или устранения.

Данная типология позволяет на основе личностных особенностей выделить предрасположенность к киберпреступлениям у определённых лиц, а также составить примерный психологический портрет преступника.

Исходя из данных проведенного опроса большая масса людей согласилась с тем, что общедоступная информация о способах совершения преступлений оказывает давление (66.7%) и лишь немногие (33.3%) возразили данному утверждению.

Также благодаря данному опросу удалось узнать, что в обществе знакомы с понятием кибертерроризм.

По нашему мнению, самым эффективным подходом к противодействию угрозе кибертерроризма является гибридный подход, включающий проведение

исследований с применением методов для сбора и анализа данных в онлайн- и офлайн-среде, расширяющий возможности изучения факторов риска и создание и внедрение в образовательных учреждениях единой процедуры оценки угроз.

Список литературы

1. Акопов Г.Л. Хактивизм в процессе информационно-политических конфликтов // *Вестник Национальной безопасности*. – 2014. – № 1. – С. 24-32.

2. Ахмадеева Е.В. Виртуальное пространство как угроза психологической безопасности семьи // *Вестник Башкирского университета*. – 2014. – Т.19. – №1. – С. 242-247.

3. Кибертерроризм и особенности его проявления [Электронный ресурс] // «Kursak.NET». – 2015. – Режим доступа: <http://kursak.net/kiberterrorizm-i-osobennosti-ego-proyavleniya/>

4. Косенков А.Н., Черный Г.А. Общая характеристика психологии киберпреступника // *Криминологический журнал ОГУЭП*. – 2012. – № 3(21). – С. 87-94.

5. Целевые атак» [Электронный ресурс] / Лаборатория Касперского. – 2015.

Ненашев Е.Д.,

Колледж АлтГУ, г. Барнаул

Научный руководитель: Стародубцева М.А., преподаватель кафедры
уголовного права и криминологии АлтГУ

Ненашев Е.Д. СПОСОБЫ ПРОТИВОДЕЙСТВИЯ КИБЕРТЕРРОРИЗМУ

Актуальность данной темы обусловлена тем, что с появлением и развитием компьютерных технологий, а также развития сети "Интернет", что способствовало тому, что люди стали больше времени проводить в Интернете для осуществления своих различных целей, поэтому террористам приходится выходить на новый "информационный" уровень для совершения противоправных деяний и вербовке новых "бойцов" в террористические организации.

Одной из разновидностей терроризма является кибертерроризм, под этим понимаются действия по дезорганизации информационных систем, создающие опасность гибели людей, причинения значительного имущественного ущерба либо иных общественно опасных последствий, совершенные со специальной целью нарушить общественную безопасность, устрашить население путем создания условий для аварий и катастроф техногенного характера либо оказать воздействие на органы власти с целью принятия ими решений, выгодных террористам[1].

Основной формой кибертерроризма является политически мотивированная атака на компьютерную информацию, вычислительные системы, аппаратуру передачи данных, иные составляющие информационной инфраструктуры, совершаемая группами или отдельными лицами. Она позволяет проникать в атакуемую систему, перехватывать управление или подавлять средства сетевого информационного обмена, осуществлять иные деструктивные воздействия.

Информационному терроризму способствует простота и дешевизна осуществления доступа к соответствующей инфраструктуре, рост объемов информации, передаваемой по открытым каналам связи, а также уязвимость в электронных сетях информации, содержащей государственную и служебную тайну. Ее утечка, искажение, уничтожение, подделка или блокирование может вызвать либо увеличить масштабы чрезвычайных ситуаций, дезорганизовать систему управления всей страной, опасно трансформировать индивидуальное и общественное сознание, психику людей, а также вызвать вооруженные конфликты, террористические акции и другие нежелательные последствия.

Информационные сети помогают экстремистским группировкам в реализации задуманных планов, которые перетекают в кибертерроризм как реальную угрозу деятельности для отдельных стран и всего мирового сообщества. Высокотехнологичные теракты способны сегодня продуцировать мировой системный кризис.

Рассмотрим причины развития кибертерроризма:

Безусловно первой причиной развития кибертерроризма является неограниченная возможность их финансирования со стороны лиц, имеющих политический, корыстный или иной интерес в достижении данных преступлений. Также с развитием интернета стало сложнее отследить данные финансовые операции, что делает такие операции анонимными. Конечно кибертерроризм требует значительно меньше финансовых затрат, это не отменяет того факта, что акты информационного терроризма финансируются заинтересованным лицом (чаще всего по политическим или финансовым мотивам) [2].

Кибертеррористы осознают факт зависимости современных государственных инфраструктур от информационно-телекоммуникационных сетей и активно используют в своих целях. Так например в статье Мохаммеда бен Ахмада ас-Салима "39 способов служить и участвовать в джихаде", вводится понятие "электронный джихад", который рассматривается как один из способов дестабилизации западных государств.

Вторая причина связана с тем, что информационный терроризм обходится дешевле "традиционного", поскольку нет необходимости покупать дорогостоящее оборудование, специальную технику, оружие и взрывчатые вещества, необходим лишь доступ к персональному компьютеру, сам компьютер, доступ к интернету и соблюдение осторожности.

Третьей причиной выступает то, что совершая противоправные деяния, киберпреступнику не составляет труда остаться в тени, то есть анонимным. Используя способы по скрытию своего местоположения, киберпреступник почти неуловим, по крайней мере в течении некоторого времени, в любом случае это затрудняет работу правоохранительных органов, поскольку нужно время, чтобы обнаружить условного преступника.

Четвертая причина заключается в многообразии целей, которые возможно достигнуть методами кибертерроризма. Кибертеррористы могут осуществлять атаки на компьютеры и информационные сервера правительств, государственных органов, частных лиц, коммунальных служб, инфраструктурных объектов, имеющих стратегическое значение. Так, например в июне 2010 года в компьютерной системе иранского центра по обогащению урана был обнаружен вирус, получивший название "Стакснет", изменивший скорости вращения центрифуг, что привело к их выходу из строя. Именно этот инцидент вынудил многие развитые страны пойти на укрепление защиты своих жизненно важных промышленных объектов, в частности, в энергетике и водоснабжении.

Объектами информационного терроризма, в зависимости от преследуемых целей и задач, могут быть: информационные ресурсы; системы формирования, распространения и использования информационных ресурсов; информационная инфраструктура вооруженных сил, правоохранительных органов и центров управления АЭС, транспортными структурами и высокотехнологичными производствами; корпоративные группы людей и институты государства, а также сам человек.

Для достижения поставленных целей в киберпространстве могут быть использованы различные приемы совершения теракта:

- хищение или уничтожение информационных, программных и технических ресурсов, имеющих стратегическую значимость, путем преодоления систем защиты, внедрения вирусов, программных закладок;

- нанесение ущерба отдельным физическим элементам, например разрушение сетей электропитания, временное выведение из строя отдельных сайтов, наведение на них помех, использование специальных программ, стимулирующих разрушение аппаратных средств, а также биологических и химических средств для уничтожения элементной базы;\

- воздействие на программное обеспечение и информацию с целью их искажения или модификации в информационных системах и системах управления;

- уничтожение либо активное подавление линий связи, ошибочное адресование, искусственная перегрузка узлов коммутации и др.;

- раскрытие и угроза опубликования закрытой информации о функционировании информационной инфраструктуры государства, общественно значимых и военных информационных систем, кодов шифрования, принципов работы систем шифрования;

- захват каналов телекоммуникационного вещания с целью распространения дезинформации, слухов, демонстрации мощи террористической организации и объявления своих требований;

- воздействие на операторов, разработчиков, эксплуатационников информационных и телекоммуникационных систем с целью совершения ими ошибочных действий;

- ложная угроза акта кибертерроризма, влекущая за собой серьезные экономические последствия.

Террористам важно, чтобы теракт имел опасные последствия, стал широко известен населению и получил большой общественный резонанс. При этом политический и экономический аспекты кибертерроризма тесно

переплетены, и невозможно однозначно сказать, какой из них имеет большее значение. По некоторым оценкам, кибертерроризм по степени угрозы человечеству сравним с ядерным, бактериологическим и химическим оружием и его опасность будет возрастать по мере развития и распространения информационно-телекоммуникационных технологий [3].

Приведу недавние примеры киберпреступлений:

Активный перевод сотрудников на удаленную работу и вывод внутренних сервисов компаний на сетевой периметр, обусловленные пандемией COVID-19, повлияли на ландшафт киберугроз во всем мире. Лишь немногие компании, которые и так практиковали работу в режиме «удаленки», были готовы справиться со всеми сложностями в обеспечении безопасности, остальные столкнулись с нехваткой времени на продумывание и реализацию всех необходимых мер защиты.

Злоумышленники без промедления приступили к поиску уязвимостей в сервисах на периметрах компаний, в том числе в решениях, используемых для организации удаленной работы, проверяя их на прочность.

В 2020 году количество атак на медицинские организации по сравнению с 2019 годом выросло на 91%. Доля атак на медицину составила 9% от общего числа инцидентов. На фоне пандемии COVID-19 и повышенной нагрузки на лечебные учреждения хакеры подливали масло в огонь, нарушая доступность медицинских информационных систем своими многочисленными атаками. Эту проблему признают во всем мире, к примеру Франция выделит 1 млрд евро на укрепление кибербезопасности после серии атак на больницы: в этой стране доля атак на медучреждения в 2020 году составила 11% от общего количества зафиксированных инцидентов.

Последствия от реализации атак с этим типом ВПО колоссальные. К примеру, общий ущерб в 2020 году от атак шифровальщиков на американские медучреждения оценивается в 20,8 млрд долл. Но для этой отрасли более опасны не финансовые последствия, а сложности с оказанием медицинской помощи людям. Такая ситуация произошла, к примеру, в сети больниц

Universal Health Services и в медицинском центре Университета Вермонта. Сотрудники больниц UHS не могли получить доступ к результатам анализов пациентов и ранее сделанным назначениям, получить данные с диагностических приборов и оказать неотложную медицинскую помощь, поскольку все необходимые данные хранились в электронном виде и оказались зашифрованы в результате атаки. А в медицинском центре в Вермонте сотрудникам пришлось восстанавливать по памяти протоколы химиотерапии, так как на восстановление системы требовалось время, которым пациенты не располагали. Подобные ситуации, когда медучреждение не может оказать неотложную помощь, а пациентов в срочном порядке приходится переводить в другие клиники, могут привести к трагическим последствиям, как, например, случай в больнице Дюссельдорфа.

BlueLeaks — самая громкая утечка данных из госорганов

Хакеры из группировки Anonymous получили доступ к 269 Гб секретных данных правоохранительных органов и спецслужб США в виде более 1 млн файлов: видеоролики, электронные письма, аудиофайлы, а также документы по планированию и разведке за последние десять лет — включая те, что подтверждают слежку за активистами Black Lives Matter. Файлы передали группе хакеров-активистов DDoSecrets, которая опубликовала полученную информацию.

13 марта сайт посольства России в Израиле подвергся атаке хакеров, которая нарушила его работу. При открытии сайта russianembassy.org.il появлялся текст на английском языке, содержащий антиизраильские лозунги, призыв оказать поддержку палестинскому народу и звучал антиизраильский рэп также на английском языке.

Эти примеры хорошо показывают, что государственные системы и системы компаний гигантов могут быть взломаны и использованы киберпереступниками в своих целях, а также это показывает то, что обычный пользователь интернета становится еще более уязвимой целью для хакера (сбор

личной информации, фишинг, вербовка в террористические организации и так далее).

В последнее время, как показывает практика, террористы все чаще используют Интернет для организации связи и управления в среде своих последователей. Так, экстремистские группировки для призывов к осуществлению террористической деятельности, демонстрации своей мощи, распространения, пропаганды и оправдания своих идей, дезинформации населения, а также для вербовки в свои ряды граждан, особенно молодежи, постоянно создают и обновляют свои многочисленные веб-сайты. Это позволило ИГИЛ довести численность своей организации в Сирии и Ираке до 30 тыс. боевиков, прибывших из 100 государств.

Путем использования интернета в качестве средства психологического воздействия террористы стремятся привлечь внимание к совершенным терактам, посеять среди граждан страх, панику, ввести их в заблуждение, распространить в обществе необходимые слухи, дезинформацию, оказывать влияние на общественное мнение, тем самым подрывая доверие населения к правительственным органам.

В связи с этим стоит вопрос о том, как противостоять кибертерроризму.

В данный момент в РФ любому проявлению терроризма, включая кибертерроризм, противостоят органы государственной власти и силовых структур различного уровня. Введен в действие Федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», создан орган ГосСОПКА и другие различные структуры. Государство пытается максимально обезопасить критически важные объекты инфраструктуры и граждан от любых проявлений терроризма. В Российской Федерации до сих пор нет "легального" закрепления определения кибертерроризма, и по моему мнению, необходимо закрепить в законодательстве определение кибертерроризма, для того, чтобы более точно классифицировать противоправные деяния в сети интернет. Также для того чтобы обеспечить информационную безопасность РФ 15 января

2013 года Указом Президента РФ No 31-с на ФСБ РФ были возложены полномочия по созданию государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ.

Основными направлениями противодействия мирового сообщества кибертерроризму могут быть:

- развитие и укрепление сотрудничества между государствами, правоохранительными органами, специальными службами, международными организациями в сфере обеспечения информационной безопасности от возможных угроз кибертерроризма и транснациональной компьютерной преступности;

- создание национальных подразделений по борьбе с кибертерроризмом, образование международного контактного пункта по оказанию помощи при реагировании на транснациональные компьютерные инциденты;

установление и расширение обмена информацией об угрозах совершения компьютерных атак, о признаках, фактах, методах и средствах использования ГИС в террористических целях;

- обмен опытом и лучшими практиками мониторинга информационных ресурсов Интернета, поиска и отслеживания содержимого сайтов террористической направленности, проведения криминалистических компьютерных экспертиз в этой сфере;

- повышение эффективности сотрудничества органов и структур государств, деятельность которых, в частности, связана с противодействием терроризму, с обеспечением безопасности информационно-телекоммуникационных сетей, с обеспечением внутренней информационной безопасности;

- доведение и разъяснение политики государств и мирового сообщества в области глобальной борьбы с терроризмом, недопустимости двойных стандартов.

Список литературы

1. Паненков А.А. Система преступлений в сфере компьютерной информации, входящих в структуру террористической деятельности (кибертерроризм) как реальная угроза внешнему и внутреннему контурам национальной безопасности России. // Военно-юридический журнал.

2. Чернов С.А., Шунаев А.М. Угрозы экономической безопасности РФ в информационной среде.

3. Ищенко Е.П. Виртуальный криминал.

ФОТОАРХИВ КОНФЕРЕНЦИИ



Президиум пленарного заседания



Аудитория пленарного заседания



Секция 1. Организационно-правовые формы противодействия терроризму
в образовательных организациях



Секция 1. Организационно-правовые формы противодействия терроризму
в образовательных организациях



Секция 2. Научно-правовые проблемы терроризму в цифровую эпоху:
взгляд студентов



Секция 2. Научно-правовые проблемы терроризму в цифровую эпоху:
взгляд студентов



Выставка «Мы против терроризма»



Место проведения конференции

Научное издание

**ОРГАНИЗАЦИОННО-ПРАВОВЫЕ МЕРЫ
ПРОТИВОДЕЙСТВИЯ ТЕРРОРИЗМУ
В ЦИФРОВУЮ ЭПОХУ**

Сборник статей по итогам всероссийской конференции

Издание публикуется в авторской редакции
Дизайн обложки — Ю.В.Луценко

Издательская лицензия ЛР 020261 от 14.01.1997.

Подписано в печать 04.02.2022.
Формат 60x84 ¹/₁₆. Бумага офсетная.
Усл.-печ. л. 14,0. Тираж 100. Заказ 32.

Типография Алтайского государственного университета:
656049, Барнаул, ул. Димитрова, 66