

Министерство науки и высшего образования Российской Федерации
Министерство внутренних дел Российской Федерации

Московский университет Министерства внутренних дел
Российской Федерации имени В.Я. Кикотя

ПРОТИВОДЕЙСТВИЕ ТЕРРОРИЗМУ И ЭКСТРЕМИЗМУ В ИНФОРМАЦИОННЫХ СФЕРАХ

**Всероссийская конференция
(26 апреля 2022 г.)**

Сборник научных статей

1 электронный оптический диск (CD-R)
Текстовое электронное издание

Научное электронное издание

Москва
2022

© Московский университет МВД России
имени В.Я. Кикотя, 2022
ISBN 978-5-9694-1194-1

УДК 004.9
ББК 16.3
И 74

Рецензенты:

Заместитель начальника Управления защиты информации ДИТСиЗИ
МВД России **С. С. Пименов**; начальник Центра информационных технологий,
связи и защиты информации ГУ МВД России по г. Москве **А. Ф. Прокопчук**

Составитель И. С. Мельцева

И 74 **Противодействие терроризму и экстремизму в информационных сферах:** Всероссийская конференция, 26 апреля 2022 г. : сборник научных статей / [сост. И. С. Мельцева]. – М. : Московский университет МВД России имени В.Я. Кикотя, 2021. – 251 с. – 1 электронный оптический диск (CD-R). – Системные требования: CUP 1,5 ГГц ; RAM 512 Мб ; Windows XP SP3 ; 1 Гб свободного места на жестком диске.
ISBN 978-5-9694-1194-1

В сборнике публикуются статьи авторов – участников Всероссийской конференции «Противодействие терроризму и экстремизму в информационной сфере», прошедшей в Московском университете МВД России имени В.Я. Кикотя 26 апреля 2022 г.

В статьях авторов рассматриваются основные аспекты распространения терроризма и экстремизма по всему миру, их негативное влияние на внутригосударственные и международные процессы, характеризуется идеологическая основа экстремизма и терроризма и приводятся правовые пути борьбы с ними. В работах отражены проблемные вопросы и перспективные направления по борьбе с экстремизмом и терроризмом в условиях цифровизации общества.

Сборник предназначен для научных и практических работников, участвующих в борьбе с преступностью.

Научное электронное издание

Минимальные системные требования: CPU 1,5 ГГц; RAM 512 Мб;
Windows XP SP3; 1 Гб свободного места на жестком диске

© Московский университет
МВД России имени В.Я. Кикотя,
2022

Издание подготовлено
с помощью программного обеспечения Microsoft Word

Редактор *Горбунова Т. С.*

Подписано к изданию 28.09.2022
Объем издания: 4,39 Мб
1 электронный оптический диск (CD-R)

ISBN 978-5-9694-1194-4



Московский университет МВД России имени В.Я. Кикотя
117997, г. Москва, ул. Академика Волгина, д. 12
<http://www.mosu.mvd.ru>; e-mail: support_mosu@mvd.ru

СОДЕРЖАНИЕ

Овчинский А. С.

Деструктивные идеологии как угроза информационным
сферам современного общества 10

Минаев В. А.

Как найти следы экстремизма в социальных медиа 15

Дош Н. А.

Платежная инфраструктура как инструмент кибертерроризма..... 20

Гурина О. Д.

Изучение ксенофобских установок у пользователей сети Интернет 25

Дорошенко Е. И.

Идеологическая адаптация ИГ в условиях пандемии COVID-19..... 28

Гончар В. В.

Основные проблемы противодействия информационно-психологическому
воздействию преступников..... 34

Ходикова Н. А.

Информационная грамотность как условие успешности
профилактики экстремизма 38

Рахмонбердиев Б. Б. угли, Куриленко Ю. А.

Уровни угроз атаки rootkit и методы борьбы с ними..... 43

Чихирева А. А., Халилова Р. Р., Шевко Н. Р.

Кибертерроризм как угроза национальной безопасности 46

Белоусов А. И., Шевко Н. Р.

Новеллы российского законодательства в области обеспечения
информационной безопасности по противодействию экстремизму и
терроризму..... 49

Цимбал В. Н.

Информационный терроризм в современных геополитических условиях 52

Пакляченко М. Ю.

К вопросу применения технологий искусственного интеллекта
в террористических целях..... 55

Галиев Д. В.

Осмотр средств вычислительной техники по делам экстремистской
направленности 58

Худяков В. В.

Проблемы кибербезопасности в деятельности сотрудников органов
внутренних дел при работе с ИСОД МВД России..... 62

Борзунов К. К.

Правовая основа Модельного закона ОДКБ «Об информационном
противоборстве терроризму и экстремизму» 66

Лустин В. И.

Вопросы разграничения преступлений экстремистской направленности
и бандитизма 70

Клочкова Е. Н.

Выявление интернет-страниц несовершеннолетних, потенциально
подверженных проявлению экстремизма 73

Ковригин В. С.

Приведение в негодность объектов жизнеобеспечения, совершенное
с использованием IT-технологий 76

Картика А. Г., Лемайкина С. В.

Актуальные вопросы защиты компьютерных сетей в условиях
скоординированных атак 80

Гасимова С. А., Шевко Н. Р.

Терроризм и экстремизм в киберпространстве: состояние и вопросы
противодействия 84

Гречков В. А., Гончар В. В.

IT-технологии борьбы с фейковыми новостями в сети Интернет..... 87

Дворянова Н. Е., Клочкова Е. Н.

Профилактика идей терроризма и экстремизма в молодежной среде с использованием возможностей сети Интернет 95

Иванов А. А., Лустин В. И.

Повышение защищенности объекта информатизации от утечки информации по оптико-электронному каналу 100

Изюмский Д. И., Гончар В. В.

К вопросу о медиатерроризме, как угрозе медиабезопасности 103

Филимонова Ю. В., Галиев Д. В.

Использование сетевых уязвимостей для получения оперативно-значимой информации 106

Куксов В. А., Мурадян С. В.

К вопросу о вовлечении несовершеннолетних в экстремистскую деятельность с помощью информационно-телекоммуникационных технологий 110

Макаров Р. Е., Дворянкин О. А.

Принуждение к совершению террористических актов с использованием сети Интернет 115

Макарова Е. А., Лустин В. И.

Использование специальных ключевых слов для получения оперативно-значимой информации из социальных сетей 120

Миляев Г. А., Лустин В. И.

Применение компьютерной экспертизы при противодействии терроризму 128

Гизатуллин М. Г., Копеина А. В.

Некоторые аспекты в области реализации направления профайлинга поведения субъектов на режимных объектах 131

Очилов А. И., Плотников Г. Г.

О проблеме финансирования терроризма в социальных сетях 136

Рыжак В. А.

Отдельные аспекты правового регулирования в рамках Содружества
Независимых Государств по противодействию терроризму
и экстремизму в информационном пространстве 139

Серов И. С., Ключкова Е. Н.

Проблемы противодействия религиозному терроризму в сети Интернет 144

Ситников А. А., Ключкова Е. Н.

Информационно-психологическое проявление экстремистской
деятельности в социальных сетях 148

Скворцов П. Д., Ключкова Е. Н.

Методика поиска информации террористической и экстремистской
направленности в сети Интернет 153

Бегларян М. Е., Спирина В. Ю.

Компьютерные и правовые технологии борьбы с терроризмом в
информационном пространстве Рунета..... 157

Золоторев Д. В., Дворянкин О. А.

Незаконный оборот наркотиков и его взаимосвязь с терроризмом
в сети Интернет 162

Боровиков В. Б., Боровикова В. В.

Проблемы уголовно-правового противодействия преступлениям
террористической и экстремистской направленности
в информационной сфере..... 166

Гунина К. Е., Шевко Н. Р.

Кибертерроризм как форма терроризма..... 170

Заманова А. Н., Зарифуллина А. Р., Шевко Н. Р.

Профилактика экстремистских и террористических проявлений среди
молодежи в информационной сети Интернет..... 173

Новиков А. В., Гончар В. В.

Современное состояние экстремизма и терроризма в условиях
развития цифровых технологий 176

Маклаков Е. Д., Овчинский А. С.

Цифровые платформы оперативно-разыскной аналитики
в противодействии терроризму и экстремизму 180

Осипова А. А., Клочкова Е. Н.

Современные методы и технологии борьбы с экстремистскими
проявлениями в сети Интернет 183

Полянская Е. П.

Некоторые проблемы доказывания, возникающие по уголовным делам
о преступлениях, совершенных по мотивам расовой, национальной,
религиозной ненависти или вражды 188

Шмарион П. В.

Современный терроризм: особенности, тенденции,
меры противодействия 193

Терехов М. Г., Шаронов С. А.

Значимость становления правового режима цифровых активов
в обеспечении национальной безопасности (по линии
противодействия терроризму и экстремизму) 197

Наумов Е. Е., Пименова О. В.

Анализ метаданных как способ идентификации преступника 204

Трухачев А. А., Гончар В. В.

Связь незаконного оборота наркотиков с терроризмом
в современных условиях 208

Фарахiev Д. М., Минзянова Д. Ф.

Инновационные технологии противодействия терроризму в процессе
глобализации 211

Филимонова Ю. В., Клочкова Е. Н.

Особенности профилактики и борьбы с проявлениями экстремизма и
терроризма среди молодежи в сети Интернет 216

Хаярова Э. А., Эркаева С. А., Шевко Н. Р.

Проблемы противодействия терроризму в молодежной среде 221

Черкесова Д. А., Клочкова Е. Н.

Интернет, как платформа для пропаганды экстремизма и терроризма 225

Чурин Р. А., Ращупкина В. А.

Современное состояние компьютерной судебной экспертизы
в экспертно-криминалистических подразделениях МВД России 229

Лукина Е. В., Аматыч Э. Р., Шевко Н. Р.

Проблемы противодействия пропаганде экстремизма и терроризма
в социальных сетях 233

Рафикова Р. Р., Шевко Н. Р.

Кибертерроризм – конвергенция терроризма и киберпространства..... 235

Андреянова Ю. М., Шевко Н. Р.

Особенности противодействия кибертерроризму
в современных условиях 238

Шаруха И. А.

Практика применения законодательства об ответственности
за преступления, посягающие на свободу совести и вероисповедания..... 241

Гринберг С. А.

Криминологически значимые особенности превентивного
воздействия на организованные формы
профессиональной преступности..... 248

Овчинский А. С.¹,
профессор кафедры информационной безопасности
учебно-научного комплекса информационных технологий
Московского университета МВД России имени В.Я. Кикотя,
доктор технических наук, профессор, академик РАЕН

ДЕСТРУКТИВНЫЕ ИДЕОЛОГИИ КАК УГРОЗА ИНФОРМАЦИОННЫМ СФЕРАМ СОВРЕМЕННОГО ОБЩЕСТВА

Среди угроз современному обществу, отношениям на мировой арене, да и всей нашей цивилизации на первый план неумолимо выдвигаются угрозы идеологические. об этих угрозах в последнее время стали говорить все чаще, но ситуация уже во многом упущена.

В данной статье обращу внимание на то, что идеологию в мире цифровых коммуникаций необходимо рассматривать в единой связке с информацией. И сколько бы ни писали об информационном взрыве, о больших данных, о сингулярном их накоплении, вопрос о том, что собой представляют килобайты, мегабайты и зеттабайты данных и сведений, сообщений и сигналов, остается открытым.

Западные социологи и разнообразные эксперты после многочисленных дискуссий сходятся на том, что «чтобы существовать, информация не нуждается в том, чтобы ее воспринимали, не нуждается в том, чтобы ее понимали, она не требует умственных усилий для своей интерпретации, ей не требуется иметь смысл, чтобы существовать».

В такой позиции сфокусирована практически вся ложь современного мира. Из этой лжи вырастают двойные стандарты в политике, в праве, в морали. Она в дипломатических переговорах «слепого с глухим», как отметил Министр иностранных дел Российской Федерации С. В. Лавров после одной из встреч с западными коллегами. Ложь все глубже поражает историческую память. Она является питательным бульоном для формирования и распространения мировой деструкции, идеологий экстремизма и терроризма, человеконенавистнических идей и расизма, идеологии нацизма. Под ложью принято понимать умышленно искаженную информацию. Но является ли она собственно информацией?

На самом деле информация – это то, что позволяет адекватно реагировать на воздействия на всех уровнях организации живой природы. Информация – это то, что возникает в сознании человека как функция целевой интерпретации получаемых сообщений. Информация позволяет понимать смысл происходящих событий, оценивать прошлое, заглядывать в будущее. Именно из блоков информации в сознании складываются модели мира, она формирует наше отношение к окружающей реальности, обоснование права на те или иные действия и поступки.

Информация, которая является ложью, противоестественна. Так, ошибки в распознавании угроз приводят к сбою в функционировании систем на всех уровнях жизни. Неадекватные реакции влекут гибель объектов живой природы. Но

¹ © Овчинский А. С., 2022.

злонамеренная ложь может захватывать сознание человека. В результате заданной извне интерпретации событий и получаемых сообщений она может заражать его вирусами деструктивных идеологий.

Под идеологией принято понимать систему взглядов и идей, которые отражают наше отношение к окружающей действительности. Идеология может объединять людей или разъединять на враждующие лагеря. Она может оформляться в программных документах. Главное же, идеология, оказывая влияние на личностные качества человека, образует в сознании, можно сказать, некую глобальную матрицу обоснования права на определенные действия и поступки, на образ жизни, на отношение к прошлому, настоящему и будущему.

На разных исторических этапах мир не раз сталкивался с угрозами таких деструктивных идеологий как расизм и терроризм. В русле нацистской идеологии были методично уничтожены миллионы людей, признанных представителями «неполноценных» народов или просто мешавших установлению «мирового порядка». К сожалению, самые мрачные страницы истории оказались далеко не до конца осознаны человечеством.

Можно по-разному подходить к раскрытию сущности информации, но вполне очевидно, что сегодня она вышла на мировую арену как инструмент воздействия на сознание людей и народов, как рычаг управления социально-политическими процессами и культурно-духовными сферами.

Однако наряду с информацией все более эффективным средством воздействия и управления становится целенаправленная, изопренная ложь. Если относительно недавно можно было говорить о борьбе идей, спорить о привлекательности той или иной идеологии, о культурных кодах и духовных ценностях, то блокада коммуникаций в условиях разгорающейся мировой информационной войны лишает миллионы людей, население стран и регионов доступа к правде, возможности объективной оценки происходящих событий, их адекватного осмысления.

Ложь, целенаправленно генерируемая в огромных объемах, которая захватывает и поражает сознание людей, населяющих страны западного мира, неизбежно приводит к деформации и последующей убийственной деградации социума. Это комплексное явление обозначим таким новым понятием как антиформация.

Формация (от лат. «formation» – образование, вид) в экономике, социологии, истории – это стадия общественного и социального развития (общественно-экономическая формация).

Если общественные отношения в истории человечества складывались, условно говоря, естественным образом, отражая в той или иной мере технологический уровень развития производительных сил, то антиформации противоестественны. В наше время они возникают и развиваются в значительной степени благодаря возможностям информационно-коммуникационных технологий.

Антиформация подобно информации отражает окружающую реальность, но отражает в «кривом зеркале» матрицы деструктивных идей. Антиформацию порождают неадекватные реакции массового сознания, пропитанного, скажем, идеологией нацизма, терроризма или религиозного экстремизма.

Идеологию было принято считать некой «надстройкой» над «базисом», т. е. над производительными силами и производственными отношениями. Однако события новейшей истории убедительно показывают, что именно идеология все чаще задает основной вектор как общественных, так и антиобщественных устремлений.

В полной мере представляя огромный комплекс самых разнообразных факторов, определяющих исторические процессы, невозможно отрицать, что возникновение фашистских государств, террористических анклавов, нацистских режимов, милитаристских устремлений происходило и происходит как реализация деструктивных идеологий. Именно деструктивные идеи, например, о превосходстве одних народов над другими, внедряемые в сознание людей, лежат в основе образования и развития антиформаций.

«Ложное информационное поле, которое все более плотно окутывает человечество, является сегодня одной из основных угроз нашей цивилизации», как заметил президент Российской академии наук А. М. Сергеев в одном из своих интервью.

Вообще ложь между людьми, сообществами, народами присутствовала всегда. Но начало нашего века было ознаменовано провозглашением информационного общества. И с развитием глобальных сетей ложь стала принимать глобальный характер. На фоне триумфа информационных технологий всемирная паутина Интернета все чаще становилась не только средой, формирующей и генерирующей огромные объемы самых разнообразных деструктивных идей, но и фактором образования и развития очагов антиформаций в виде уже сетевых или пока виртуальных сообществ, нацеленных на экстремистскую и террористическую деятельность.

Вышедшая на арену цифровизация стала стремительно захватывать и, образно говоря, перемалывать в своих электронных жерновах все сферы жизни и деятельности людей. Об угрозах цифровизации уже немало сказано. Не исключено, что последствия цифровой трансформации, особенно в сфере образования, потребуют масштабных мер по дедебилизации населения стран и регионов.

Впереди же нас ожидает еще один, небезопасный для сознания людей переход – массовое погружение в виртуальные миры. Это технологии, например, дополненной реальности, виртуальной реальности или уже так называемая «мета вселенная», а именно, конвергенция физической, виртуальной и дополненной реальности в общем онлайн-пространстве.

Масштабные акции информационной войны против России сейчас строятся на дипфейках, т. е. уже целенаправленной «глубокой» лжи – на создании компрометирующих нереальных событий. Фабрики фейков, организованная деятельность сотен «специалистов информационной войны», тысяч «любителей», подрабатывающих на войне, создают такой информационный фон, лавины таких

сообщений, которые порождают в сознании людей не столько собственно информацию, сколько ее противоположность.

Противоположность информации – это информационные вирусы лжи и вражды в отношениях между людьми и народами. Так, на фоне углубляющегося мирового кризиса сегодня на передний план вышла русофобия с так называемой «культурой отмены» всего русского. Формируется уже глобальная антиформация, охватывающая страны и регионы.

Антиформации, построенные на лжи и деструкции, противоестественны, но зачастую они имеют мощнейшие исторические корни. По аналогии с названием известной в свое время работы В. И. Ленина можно выделить «три источника и три составные части нацизма». Это колониализм, т. е. подъем Западной цивилизации за счет ограбления и эксплуатации народов Африки, Азии и латинской Америки. Это западноевропейская философия, которая провозгласила могущество человека, поставив его на место бога. Это языческие культы, поклонение идолам, человеческие жертвоприношения, переходящие в сатанизм. Все это сегодня прорастает иррациональным стремлением к мировому доминированию, новыми волнами шовинизма с пренебрежением жизнью людей и народов, не входящих в «круг избранных», терроризмом с невиданной ранее показной жестокостью.

Информационные вирусы деструкции могут проникать в то сознание, в котором образуется идеологический вакуум или идеологический хаос. В современном мире этот хаос обусловлен глубочайшим кризисом либеральной идеологии. Она успешно выполняла свою функцию обоснования прав обогащаться и потреблять на этапах становления и развития капитализма. Но на его закате стала проявлять все более деструктивный характер, оправдывая экспансию, агрессию в борьбе за мировое доминирование и настойчиво пропагандируя самые низменные человеческие пороки. Более того, именно в русле деградирующего либерализма набирает силу современный нацизм.

Информационные антитела, защищающие иммунную систему сознания от деструкции, могут вырабатываться с консервативной идеологией. Обосновывая право на защиту традиционных ценностей, она, однако, представлялась неким тормозом на пути прогресса. Но относительно недавно Президент Российской Федерации В. В. Путин, выступая на Валдайском форуме 2021 г., процитировал русского философа Н. Бердяева о том, что умеренный консерватизм – это не препятствие движению вперед и вверх, а защита от отката назад, от падения вниз, от деградации и хаоса.

Но только защищаясь, сложно рассчитывать на большие успехи в борьбе с социальной деструкцией, на победу в неутихающей мировой информационной войне, на оздоровление отравленного ложью сознания огромных масс людей и целых народов, населяющих страны и континенты.

В пространстве основных мировых идеологий нельзя не выделить и социалистическую с приоритетом справедливости в отношениях между людьми и народами, а в перспективе и коммунистическую с обоснованием права на борьбу со

всем, что угнетает человечество, мешает движению вперед к «светлому будущему».

Нельзя не отметить, что, если для либерализма идеалом был человек-потребитель, консерватизму требовался человек-защитник, то идеология, которая являлась государственной в Советском Союзе, была направлена на формирование, на воспитание человека-творца. Так и было обозначено в программных документах коммунистической партии, и сложно отрицать что творческий потенциал этой идеологии не находил реализацию в весьма эффективной системе образования, подготовке высококвалифицированных специалистов, в достижениях советских ученых.

Эпоха перемен сегодня – это не просто слова, это не только отражение стремительных изменений на мировой арене, это неуклонное втягивание в смертельную схватку за будущее нашей страны и всего человечества. В этой схватке мир как никогда поляризован. Парламенты так называемых недружественных стран в едином порыве сегодня рукоплещут нацизму. Как бы не было сложно задачи по демилитаризации, по денацификации Украины, да и Европы будут решены. Главный вопрос современности: что мы, наше государство, наша цивилизация сможем предложить миру? Какое будущее, какую идеологию?

Но начинать надо с себя, с принятия ясной государственной идеологии. Именно государственная идеология должна, в первую очередь, дать обоснование права на бескомпромиссную борьбу за независимость и суверенитет России, на защиту русского мира. Также, как герб, гимн, флаг, конституция, идеология будет необходимым атрибутом государства. Наша государственная идеология должна быть понятной и привлекательной для мирового сообщества.

*Минаев В. А.¹,
профессор кафедры специальных информационных
технологий учебно-научного комплекса
информационных технологий Московского университета
МВД России имени В. Я. Кикотя,
доктор технических наук, профессор*

КАК НАЙТИ СЛЕДЫ ЭКСТРЕМИЗМА В СОЦИАЛЬНЫХ МЕДИА

На современном этапе развития российского общества наблюдается существенное возрастание угроз кибербезопасности, в числе ключевых из которых в Доктрине информационной безопасности Российской Федерации названы информационно-психологические воздействия (ИПВ) на индивидуальное, групповое и общественное сознание.

Отмечается рост распространения контента экстремистского характера, к которому относятся материалы с прославлением нацизма, содержащие призывы радикальных исламистов, обращения, направленные на развитие расизма и криминальной культуры в обществе, насильственный захват власти и активизацию противоправной деятельности. Особенно опасно, что такой контент, в первую очередь, направлен на подростков и молодежь, которые активно используют современные информационные системы и коммуникационные сети, заражаясь через них экстремистскими идеями.

Соответствующие подразделения МВД России, применяя современные программно-технологические возможности, все активнее противодействуют распространению деструктивного контента среди населения, особенно среди его подростковых и молодежных групп.

Перспективные модели интеллектуальной классификации

Современный этап развития правоохранительной системы России характеризуется ускоряющимся использованием информационно-аналитических систем в управлении социальными процессами, включая перспективные технологии искусственного интеллекта. Для целей выявления и идентификации контента экстремистского характера в социальных медиа (далее – СМ) могут быть эффективно использованы математические методы анализа, имеющие высокий уровень устойчивости к шумовым эффектам при классификации текстового материала. Такие работы активно ведутся как российскими [1–4], так и зарубежными [5–7] учеными.

Автором осуществлен анализ не менее десятка моделей интеллектуальной классификации применительно к деструктивному контенту. Среди них выбраны три наиболее перспективные: алгоритм машинного обучения – метод опорных векторов (SVM – Support Vector Machines) [8], классификатор на основе рекуррентной нейронной сети (GRU – Gated Recurrent Units) [9], а также классификатор текста на основе искусственных нейронных сетей (трансформер BERT –

¹ © Минаев В. А., 2022.

Bidirectional Encoder Representations from Transformers) [10]. Оценены их свойства и влияние шумовых факторов на качество классификации экстремистского контента.

Сегодня выявление деструктивного контента в СМ осуществляется как с использованием автоматизированных систем (далее – АС), так и в результате обычных экспертных процедур.

Поскольку ежемесячно создается более миллиарда новых текстовых публикаций, ключевое направление поиска социально опасного контента в СМ связано с автоматизацией, так как проводить качественный анализ такого объема материалов с привлечением человека-эксперта невозможно.

При применении автоматизированных систем необходимо учитывать точность их работы, связанную с шумостойкостью. Именно так формулируются задачи, стоящие перед специалистами подразделений МВД России, занимающихся выявлением и идентификацией деструктивного контента в СМ.

Формальная постановка задач заключалась в том, чтобы с достаточным уровнем точности отделить текст деструктивного характера от допустимого контента, похожего синтаксически, но отличающегося семантически (так называемого шумового контента).

В настоящей статье анализировался смешанный контент, состоящий из двух примерно равных частей – из текстов Федерального списка экстремистских материалов [11] и из материалов СМ, включая известные социальные сети ВКонтакте, Одноклассники и др., а также системы обмена мгновенными сообщениями Telegram, WhatsApp и т. п.

Корпуса текстовых массивов состояли каждый примерно из трехсот тысяч предложений экстремистской направленности со средним количеством слов в них, равном 14, а также шумового корпуса из СМ (материалы, не являющиеся экстремистскими). Характеристики корпусов экстремистского характера приведены в таблице 1.

Таблица 1

Объем исследованных текстовых массивов экстремистской направленности

Характер текстового деструктивного массива	Количество предложений, тыс.
Антисемитизм	268
Реабилитация нацизма	284
Радикальный ислам	310

Эксперименты по выявлению экстремистского контента

Проведены компьютерные эксперименты с указанным выше объемом текстового материала для поиска наиболее точного метода искусственного интеллекта по идентификации контента экстремистского характера. При этом для обучения нейронных сетей выявлению экстремистского контента использовался Федеральный список экстремистских материалов [11].

На рисунке 1 показаны основные этапы выявления контента экстремистской направленности в СМ.

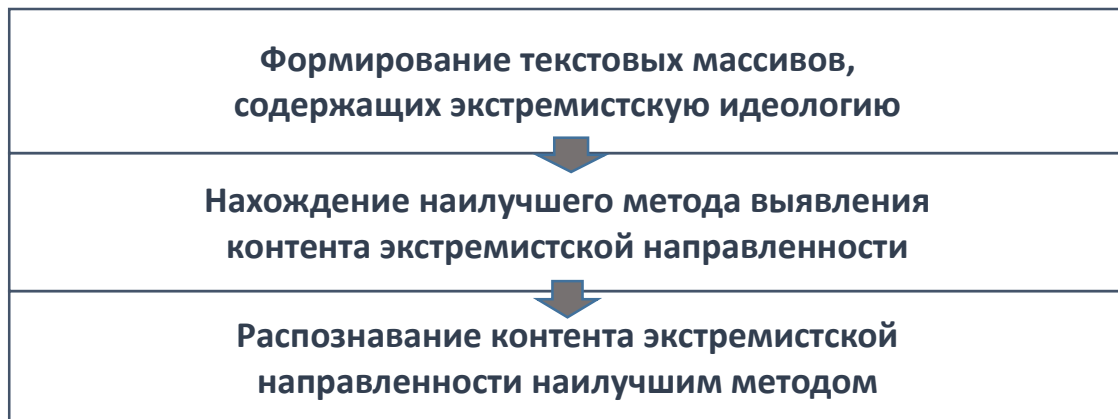


Рис. 1. Этапы выявления контента экстремистской направленности в социальных медиа

Как видно из таблицы 2, все реализованные в статье методы искусственного интеллекта показывают достаточно высокое качество выявления экстремистского контента при учете шумовых эффектов (не менее 82 %). При этом наиболее результативной является модель BERT (92 %).

Таблица 2

**Точность методов искусственного интеллекта
по выявлению контента экстремистской направленности**

Метод искусственного интеллекта	Точность выявления, %
Метод опорных векторов (SVM)	82
Рекуррентная нейронная сеть (GRU)	82
Трансформер BERT	95

Из таблицы 3 очевидна очень высокая точность распознавания текстовых массивов экстремистской направленности, если использовать автоматизированную систему анализа контента.

Таблица 3

**Точность распознавания текстовых массивов
экстремистской направленности**

Характер текстового деструктивного массива	Точность распознавания, %
Антисемитизм	91
Реабилитация нацизма	93
Радикальный ислам	95

Отметим, что в сложных случаях, когда с помощью АС не удастся идентифицировать деструктивность текстов, составляющих 5–9 %, как это следует из таблицы 3, следует привлекать профессионалов-экспертов (рис. 2).

Таким образом, в статье предложена и практически реализована методика выявления и идентификации контента экстремистской направленности в социальных медиа, базирующаяся на применении нейронных сетей как перспективного направления искусственного интеллекта.

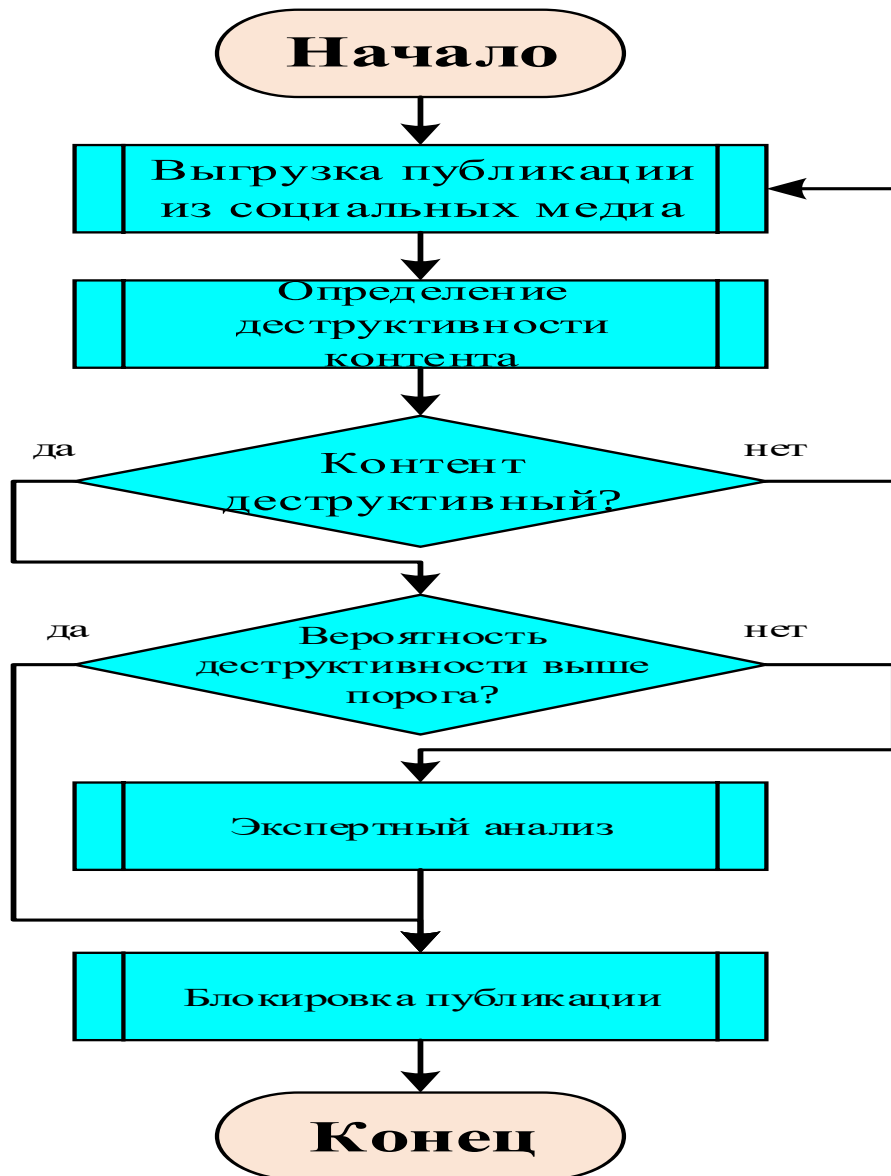


Рис. 2. Алгоритм распознавания и блокировки контента экстремистской направленности с привлечением экспертов

Высокая точность распознавания деструктивности текстов позволяет использовать полученные результаты для практического совершенствования работы подразделений органов внутренних дел по противодействию распространению идеологии терроризма и экстремизма в социальных медиа.

Кроме того, указанные результаты могут быть полезными при разработке и модернизации прикладного математического обеспечения автоматизированных систем правоохранительных структур, в частности – МВД России, для поиска контента террористической и экстремистской направленности в социальных медиа.

Ценность полученных научных результатов заключается в новых возможностях методического обеспечения аналитической деятельности, связанной с обработкой и анализом больших данных (Big Data), как правило, зашумленных искусственно генерируемыми «текстовками».

Следует также отметить, что высокоточное определение деструктивного контента необходимо для принятия своевременных и эффективных мер по противодействию и иным деструктивным воздействиям в социальных медиа. Так, результаты проведенного исследования целесообразно учитывать при выявлении информационных воздействий на молодое поколение при склонении к суицидальному поведению, вовлечении в различные опасные сообщества.

Список литературы

1. Минаев В. А., Поликарпов Е. С., Симонов А. В. Применение глубинных нейронных сетей для выявления деструктивного контента в социальных медиа // Информация и безопасность. 2021. Т. 24. № 3. С. 361–372.
2. Минаев В. А., Симонов А. В. Количественная оценка деструктивности больших текстовых массивов в социальных медиа // Информация и безопасность. 2021. Т. 24. Вып. 2. С. 267–280.
3. Минаев В. А., Реброва А. Д., Симонов А. В. Выявление деструктивного контента в социальных медиа на основе моделей машинного обучения // Информация и безопасность. 2021. № 1. Т. 24. С. 7–20.
4. Kuratov Y., Arkhipov M. Adaptation of deep bidirectional multilingual transformers for Russian language // arXiv preprint arXiv:1905.07213. 2019. P. 1–7.
5. Van Aken B. et al. Challenges for toxic comment classification: An in-depth error analysis // Proceedings of the 2nd Workshop on Abusive Language Online (ALW2). 2018. P. 33–42.
6. Wang X. et al. Drifted Twitter spam classification using multiscale detection test on KL divergence // IEEE Access. 2019. Vol. 7. P. 108384–108394.
7. Vaswani A. et al. Attention is all you need // Advances in neural information processing systems. 2017. Vol. 30. P. 1–15.
8. Scheinberg K. An efficient implementation of an active set method for svms // J. Mach. Learn. Res. 2006. Vol. 7. P. 2237–2257.
9. Будыльский Д. В. GRU и LSTM: современные рекуррентные нейронные сети // Молодой ученый. 2015. № 1 (95). С. 51–54.
10. Sun C. et al. How to fine-tune BERT for text classification? // China National Conference on Chinese Computational Linguistics. Springer, Cham, 2019. P. 194–206.
11. Экстремистские материалы : Министерство юстиции Российской Федерации (minjust.gov.ru) (дата обращения: 18.05.2022).

Дош Н. А.¹,

директор по рискам Ассоциации участников Мастеркард

ПЛАТЕЖНАЯ ИНФРАСТРУКТУРА КАК ИНСТРУМЕНТ КИБЕРТЕРРОРИЗМА

В настоящее время правонарушители активно осваивают современные технологии и направляют их в криминальное русло. В настоящее время преступники умеют многое – они достаточно качественно подделывают сайты государственных органов, организаций здравоохранения, благотворительных организаций и фондов, интернет-магазинов и банков. Благодаря слитым в сеть персональным данным мошенники получили возможность связываться с потенциальными жертвами – убеждать, запугивать и угрожать.

В условиях специальной военной операции и продолжения распространения коронавирусной инфекции в мире преступники разработали и используют множество новых либо хорошо забытых старых схем, направленных на получение выгоды от их совершения.

Один из негативных зарубежных трендов, который фиксируется на сегодняшний день, – это подрыв банкоматов с помощью газа или взрывчатки. Данный вид атаки характеризуется огромными сопутствующими разрушениями и периодической гибелью как самих преступников, пытающихся подорвать банкомат, так и случайных прохожих, оказавшихся неподалеку от места взрыва. Для понимания масштабов проблемы на примере Германии стоит отметить, что за 2021 г. на территории этой страны зафиксировано около 450 подрывов банкоматов. Такого рода цифра демонстрирует нам еще одну большую проблему в Европе, связанную с достаточно свободным доступом криминальных элементов к взрывчатым веществам и их использованием в людных местах. Это тем более опасно, учитывая последствия подрывов банкоматов на территории европейских стран.

Рассмотрим суть данных проблем наглядно.



АТАКИ НА БАНКОМАТЫ

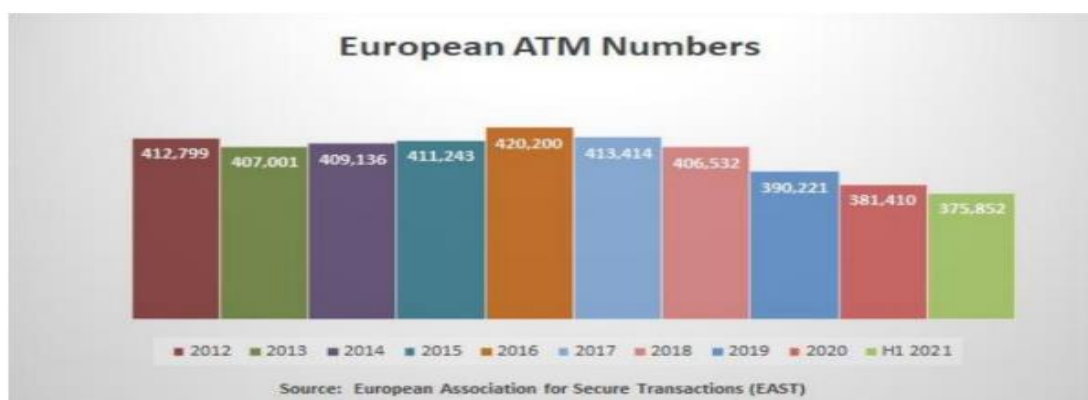


Рис.1. Количество атак на банкоматы

¹ © Дош Н. А., 2022.

АТАКИ НА БАНКОМАТЫ

Current trends

Key findings

- Phenomenon increasingly reported to Europol since 2016
- 27 countries affected. UK and DE = main affected countries
- Less ATM attacks reported to Europol this year compared to same period last year
- Decrease during covid-19 where a lockdown was decided
- Side effect of the border controls (DE – BE – NL)
- Increase again during the second half of 2020.
- Situation in North Rhine-Westphalia (DE) - ATM explosions have more than doubled in 2020

Рис.2. Общая информация об атаках на банкоматы

АТАКИ НА БАНКОМАТЫ

Recent attacks- few examples

Germany

- September 29th : ATM Attack Löhne, North Rhine-Westphalia. Complete bank was destroyed by explosion
- October 4th: ATM Dortmund, Northrhine-Westphalia. Two explosions were noticed by witnesses

Switzerland

- September 28th : ATM Attack Rikon, Tösstal. Unknown suspects managed to attack an ATM by the use of explosives and steal 100,000 Franken

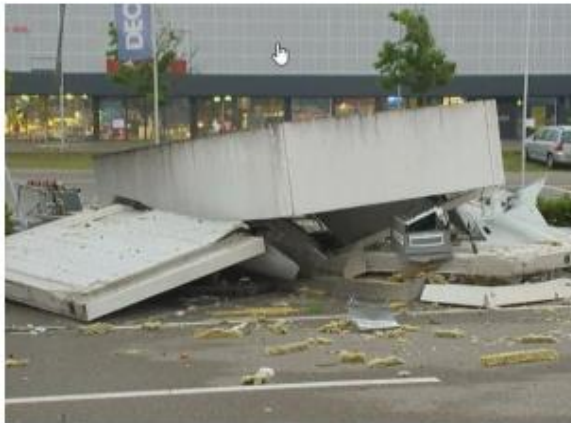
Netherlands

- September 24th: ATM Attack Alkmar. ATM attack committed by the use of explosives. Two perpetrators managed to escape by a the use of a scooter



Рис.3. Примеры последствий атак на банкоматы

АТАКИ НА БАНКОМАТЫ



Швейцария



Рис. 4. Примеры последствий атак на банкоматы

АТАКИ НА БАНКОМАТЫ

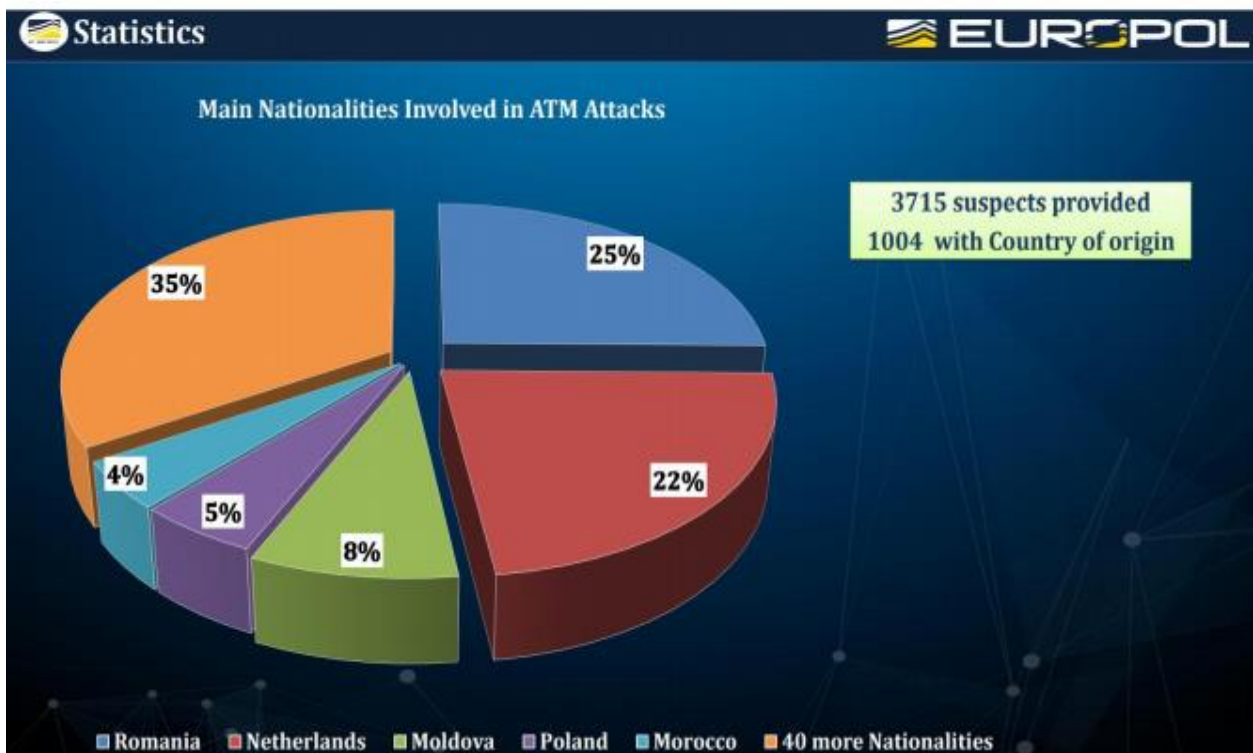


Рис. 5. Общая статистика



ДИСТАНЦИОННЫЙ ФРОД

INVESTMENT SCAMS

INVESTMENT SCAMS	H1 2018	H2 2018	H1 2019	H2 2019	H1 2020	H2 2020	H1 2021	H1 vs H1 CHANGE	H1 vs H2 CHANGE
Number of cases	1,359	2,026	3,425	3,364	3,723	5,235	6,864	84%	31%
Number of payments	3,675	4,261	7,126	7,097	9,492	13,761	20,152	112%	46%
Total value of losses	£20.8m	£29.3m	£43.4m	£51.9m	£55.2m	£79.9m	£107.7m	95%	35%
Total subsequently returned to the customer	£1.4m	£2.5m	£2.9m	£9.4m	£15.1m	£33.9m	£44.3m	193%	31%

PURCHASE SCAMS

PURCHASE SCAMS	H1 2018	H2 2018	H1 2019	H2 2019	H1 2020	H2 2020	H1 2021	H1 vs H1 CHANGE	H1 vs H2 CHANGE
Number of cases	21,483	31,138	35,472	37,864	37,516	41,204	52,348	40%	27%
Number of payments	27,011	39,685	44,252	48,868	47,768	54,834	68,763	44%	25%
Total value of losses	£19.4m	£26.9m	£27.9m	£31.1m	£27.1m	£30.0m	£37.7m	39%	26%
Total subsequently returned to the customer	£1.6m	£2.6m	£2.7m	£6.9m	£6.8m	£9.6m	£11.0m	63%	15%

Рис. 6. Информация о дистанционных атаках



ДИСТАНЦИОННЫЙ ФРОД

IMPERSONATION: POLICE/BANK STAFF

IMPERSONATION: POLICE/BANK	H1 2018	H2 2018	H1 2019	H2 2019	H1 2020	H2 2020	H1 2021	H1 vs H1 CHANGE	H1 vs H2 CHANGE
Number of cases	1,947	3,512	4,242	6,846	8,222	13,245	18,816	129%	42%
Number of payments	3,196	5,507	10,056	12,204	14,478	27,510	39,246	171%	43%
Total value of losses	£22.2m	£34.3m	£35.4m	£48.7m	£36.7m	£59.9m	£84.7m	131%	41%
Total subsequently returned to the customer	£6.9m	£12.9m	£11.2m	£26.1m	£23.4m	£36.1m	£48.7m	108%	35%

CEO FRAUD

CEO	H1 2018	H2 2018	H1 2019	H2 2019	H1 2020	H2 2020	H1 2021	H1 vs H1 CHANGE	H1 vs H2 CHANGE
Number of cases	347	256	340	336	241	596	207	-14%	-65%
Number of payments	478	353	487	475	361	770	310	-14%	-60%
Total value of losses	£8.0m	£6.8m	£7.9m	£9.8m	£4.7m	£5.7m	£6.5m	37%	14%
Total subsequently returned to the customer	£2.2m	£2.1m	£2.1m	£1.7m	£2.2m	£1.7m	£3.0m	36%	72%

Рис. 7. Информация о дистанционных атаках



Рис. 8. Механизм атаки при помощи вирусного ПО

*Гурина О. Д.¹,
главный эксперт
отдела психологических экспертных исследований
ГБУ г. Москвы «МИЦ»,
кандидат психологических наук*

ИЗУЧЕНИЕ КСЕНОФОБСКИХ УСТАНОВОК У ПОЛЬЗОВАТЕЛЕЙ СЕТИ ИНТЕРНЕТ

Общественным вызовом сегодняшнего дня являются различные формы экстремистской деятельности. Особенно подвержены подобным радикальным формам поведения несовершеннолетние, подростки. Предупреждение и профилактика экстремизма представлены как одни из важнейших государственных задач, решение которых требует соответствующих инструментов. К таким инструментам могут быть отнесены правовые механизмы урегулирования экстремизма, деятельность общественных институтов, в том числе СМИ, способы регулирования общественных отношений на местном уровне (например, в общеобразовательных учреждениях), что также включает в себя разработку методик для оценки явлений, способствующих и/или препятствующих проявлению экстремизма.

В психологической науке существует ряд образований, которые непосредственно могут влиять на возникновение экстремистского поведения [4; 6]. К ним относятся ксенофобские установки, которые представлены как готовность действовать враждебно по отношению к какой-либо группе лиц.

Для измерения готовности к враждебному поведению могут быть использованы соответствующие методики, шкалы оценки, дающие возможность отследить, отобрать на первом этапе лиц, склонных к экстремистскому поведению.

Поведение пользователей в сети Интернет, в том числе несовершеннолетних, может отличаться от реального поведения, и эта особенность виртуального мира связана с такими его характеристиками как большая анонимность, сниженный уровень правового и социального контроля и др. [2].

Вопрос о том, насколько опасно может быть само проявление ксенофобии в сети Интернет, определяется, прежде всего, законодательно: например, запрещено возбуждение вражды, ненависти; побуждение к насильственным, дискриминационным действиям по отношению к какой-либо группе лиц и т. д. [1].

Для изучения ксенофобии в Интернете необходимо в первую очередь оценить коммуникативную ситуацию, в рамках которой размещена соответствующая информация. В целом такая оценка в рамках борьбы с экстремизмом проводится правоохранительными органами, в отдельных случаях с назначением необходимых судебных экспертиз [7, с. 5].

В соответствии с задачей определения ксенофобских установок у пользователей сети Интернет, в первую очередь у подростков (можно также использовать их и для оценки взрослой категории лиц), стоит обращать внимание на следующие обобщенные высказывания и оценки пользователей (в социальных сетях,

¹ © Гурина О. Д., 2022.

блог-платформах и др.): *следует запретить иностранцам селиться в одном месте; большинство иностранцев нарушают местные правила и нормы; следует применять к иностранцам более жесткие санкции и наказания, чем к местному населению, за совершение ими правонарушений; иностранцы часто страдают опасными заболеваниями; следует меньше общаться с иностранцами; достаточно часты случаи, когда иностранцы вели себя агрессивно по отношению к местному населению; тяжкие преступления (убийства, грабежи и т. д.) чаще всего совершают иностранцы; враждебное отношение (оскорбление, унижение и т. д.) к иностранцам оправдано; зачастую иностранцы работают там, где могли бы работать местные жители; местные жители чаще всего враждебно настроены к иностранцам.*

Перечисленные высказывания были разработаны в рамках составления шкалы оценки ксенофобских установок у подростков. Шкала включает в себя 20 утверждений, степень согласия с которыми определяют выраженность и характер установки по отношению к иностранцам. Утверждения содержат различного рода представления о взаимоотношениях между местным населением и приезжими, чужими (иностранцами, мигрантами). Надежность шкалы была оценена с помощью процедуры теста-ретеста, анализа согласованности отдельных пунктов шкалы, определения уровня пригодности (α Кронбаха = 0,764). Для оценки валидности использовалась шкала-опросник «Индекс толерантности» [5, с. 46]. Коэффициент ранговой корреляции Спирмена составил $r = 0,851$ при $p < 0,001$. Полученные результаты свидетельствуют о достаточной надежности и валидности шкалы [3, с. 12].

Указанную шкалу можно внедрить для экспресс-оценки установок пользователей, использующих те или иные Интернет-ресурсы. Например, в общеобразовательных учреждениях для выявления лиц, склонных к враждебному поведению не только онлайн, но и в реальном мире. Это может быть организовано при получении доступа к сети, как предварительное тестирование. Полученные результаты могут быть в дальнейшем использованы для соответствующей оценки установок пользователей в рамках предупреждения и профилактики экстремизма.

Список литературы

1. Федеральный закон от 25 июля 2002 г. № 114-ФЗ «О противодействии экстремистской деятельности» (с изменениями от 27 июля 2006 г., 10 мая 2007 г., 24 июля 2007 г., 29 апреля 2008 г.).
2. Бовина И. Б. Поведение онлайн и офлайн: к вопросу о возможности прогноза / И. Б. Бовина, Н. В. Дворянчиков // Культурно-историческая психология. 2020. Том 16. № 4. С. 98–108.
3. Гурина О. Д. Ксенофобские установки и личностные особенности у подростков с противоправным поведением: автореф. дис. ... канд. психол. наук: 19.00.06 / Гурина Оксана Дмитриевна. М., 2020.

4. Дозорцева Е. Г. Ксенофобия и молодежный экстремизм: истоки и взаимосвязи [Электронный ресурс] / Е. Г. Дозорцева, О. Д. Маланцева // Психологическая наука и образование. 2012. № 2. Режим доступа: http://psyjournals.ru/psyedu_ru/2012/n2/53445_full.shtml.

5. Психодиагностика толерантности личности / Г. У. Солдатова, Л. А. Шайгерова. М. : Смысл, 2008.

6. Солдатова Г. У. Мониторинг толерантности, ксенофобии и социального доверия / Г. У. Солдатова, А. Н. Кричевец, Е. Филиеева. М. : Центр СМИ МГУ им. М. В. Ломоносова, 2004.

7. Теоретические и методические основы производства судебной психолого-лингвистической экспертизы текстов по делам, связанным с противодействием экстремизму / О. В. Кукушкина, Ю. А. Сафонова, Т. Н. Секераж. М. : ГУ РФЦСЭ при Минюсте России, 2014.

*Дорошенко Е. И.¹,
выпускающий редактор
отдела общественно-политических проектов
Дирекции государственных проектов
МИА «Россия сегодня»,
кандидат филологических наук*

ИДЕОЛОГИЧЕСКАЯ АДАПТАЦИЯ ИГ² В УСЛОВИЯХ ПАНДЕМИИ COVID-19

Затрагивая тему актуальности угрозы, исходящей со стороны так называемого «Исламского государства», нужно отметить, что сегодня эта организация как будто отошла не то, что на второй, – на третий план. Этому способствовали три наиболее заметных фактора: потеря псевдохалифата как квази-административного образования, существовавшего на территории Сирии и Ирака в период между 2014 и 2019 гг., ликвидация Абу Бакра аль-Багдади в октябре 2019 г., а затем и нового лидера Абу Ибрагима аль-Хашими аль-Курайши в начале февраля 2022 г. и, наконец, долговременные, последовательные и эффективные действия России в Сирии.

Однако не будем забывать, что в условиях пандемии COVID-19 и текущего конфликта на Украине, когда внимание общественности и ресурсы государства сосредоточены на других проблемах, ИГ получило возможность перегруппироваться и в какой-то степени восстановиться. В подтверждение приведем некоторые тезисы из публикации в британской *The Times* от 18 апреля 2022 г. [1]. В статье сообщается о том, что ИГ объявило о начале нового «общемирового наступления», первыми целями которого должны стать Европа и Израиль, в ответ на ликвидацию Абу Ибрагима аль-Хашими аль-Курайши. Также приводятся цитаты из аудиообращения нового пресс-секретаря группировки Абу-Омара аль-Мухаджира. В частности, через него ИГ призывает своих сторонников воспользоваться тем, что внимание Запада сегодня сосредоточено на военных действиях на Украине, т. е. совершать теракты, пока «крестоносцы сражаются друг с другом».

Аль-Мухаджир подчеркивает, что сложившаяся ситуация является «возможностью» для группировки, в то время как немусульманские государства «заняты» конфликтом.

Другими словами, **ИГ не только воспринимает и осознает сложившиеся обстоятельства как «возможность», но и призывает своих сторонников ее не упускать.**

Важно также отметить, что эти заявления последовали в контексте двух терактов, совершенных в конце марта 2022 года сторонниками ИГ в израильских городах Беэр-Шева и Хадера. Аль-Мухаджир призывает членов группировки

¹ © Дорошенко Е. И., 2022.

² Здесь и далее имеется в виду «Исламское государство», запрещенная в Российской Федерации террористическая организация.

«вооружаться и совершать новые [атаки]». Он также добавил, что Иерусалим может быть освобожден только при условии возвращения так называемого «халифата». Это говорит о том, что ИГ по-прежнему преследует цель восстановления своего псевдогосударства, а значит, потенциал для нападений сохраняется.

На территории нашей страны также наблюдается активизация исламистских группировок: к такому выводу можно прийти, отследив хронологию новостных сообщений о предотвращенных терактах. Так, в Ставрополе 25 апреля 2022 г. была «...вскрыта и пресечена деятельность сторонника запрещенной в России международной террористической организации „Исламское государство“, планировавшего **по указанию зарубежных эмиссаров МТО совершение теракта** на одном из объектов транспортной инфраструктуры региона. Подозреваемый задержан» [2].

Аналогичное сообщение поступило 21 апреля 2022 г.: был предотвращен теракт, который ИГ готовило на железной дороге в Республике Крым, причем в этом случае исполнитель получал указание от главарей крымско-татарского формирования, которое участвует в боях против российских военных на Украине [3]. Соответственно, если здесь пока нет оснований говорить о сращении неонацистской и исламистской идеологии, то по крайней мере очевидно то самое **стремление воспользоваться моментом**. Это означает, что деятельность ИГ действительно разворачивается уже в контексте текущих событий.

Прочие инциденты, указывающие на активизацию исламистских группировок: 13 апреля 2022 г. ФСБ России пресекла в Республике Крым деятельность подозреваемого в пропаганде запрещенной в Российской Федерации организации «Хизбут-Тахрир» [4], а 1 апреля в России была ликвидирована крупная ячейка пособников сирийских террористов «Хайат Тахрир аш-Шам», действовавших в Башкирии, Дагестане, Ингушетии, Краснодарском крае, а также в Астраханской, Тульской, Новосибирской и Тюменской областях [5].

Одно из условий устойчивости, слаженности и выживаемости террористических организаций – это **их способность к адаптации, прежде всего, в плане идеологии**.

С одной стороны, это важный фактор создания и поддержания нужного верушке видения среди членов и сторонников, а с другой – решение задачи по привлечению и вербовке новых кадров.

Одновременно с этим, для самой организации – это развитие базовых установок в зависимости от изменения внешних условий. Наконец, толкование текущих событий в терминах идеологии указывает и направление дальнейшей деятельности группировки.

В связи с этим обратимся к тому, как ИГ подает себя в информационном пространстве, т. е. приведем его основной нарратив.



Рис. 1. Основные смысловые элементы идеологии ИГ

Эти базовые установки составляют идеологическое ядро группировки и не будут изменяться в зависимости от внешнего воздействия, пока организация существует, т. е. останутся актуальными в течение всей ее жизни. Даже сегодня потеря реального квазигосударства компенсируется идеей о «виртуальном халифате», которая присутствует в информационном пространстве как минимум с 2018 г.



Рис. 2. Идея «виртуального халифата», проиллюстрированная в агитационном материале

Для членов и сторонников группировки это, конечно, не означает, что на этом и следует остановиться, как раз наоборот: нужно воссоздать «потерянный рай», раз он уже однажды существовал, и призыв к этому был уже упомянут выше: восстановление псевдохалифата как условие «освобождения» Иерусалима.

Сегмент «условий конца света» в нарративе ИГ до недавнего времени был одним из самых слабых и труднодоказуемых смысловых элементов, который

требовал от последователей именно *веры*, поскольку апокалипсис все не наступает, несмотря на упорные заявления идеологов ИГ. Теперь же благодаря коронавирусу и соответствующим интерпретациям, он неожиданно приобрел некоторое развитие и даже подтверждение. Соответственно, именно в рамках данного сегмента можно проиллюстрировать механизмы идеологической адаптации и проследить развитие идеи «избранности», «праведности» и «правоверности» в условиях пандемии COVID-19.

Вполне закономерно, что появление и взрывное распространение коронавируса вызвало почти мгновенную реакцию со стороны всех крупных салафитоджихадистских организаций. Спикеры «Аль-Каиды», ИГ, а также представители радикально настроенного мусульманского духовенства, выступили с соответствующими заявлениями. Их послания содержали указания для правоверных (причем требующие беспрекословного и точного выполнения) о том, как защититься от болезни.

И все это помещалось в контекст исполнения заповеди о спасении жизней, увещеваний о возврате к исламу и призывов **продолжать борьбу, несмотря на потрясения, связанные с утратой территориального псевдохалифата.**

В понимании джихадистов **через COVID-19 проходит линия фронта в борьбе против не мусульман и тех мусульман, которых считают «приспешниками [неверных] или же слишком пассивными»** – в противоположность тем, кто полностью проникся идеей вечной войны через джихад.

Мысль о «состоянии бесконечного конфликта» прослеживается также в специфическом объяснении причин эпидемии: COVID-19 поразил Китай и Европу, будучи «проклятием Всевышнего». При этом Китай, согласно этим теориям, пострадал особенно сильно из-за массовых репрессий против мусульманского уйгурского населения.

На эти установки накладывается контекст более широкого геополитического плана: это продолжающаяся **«апокалиптическая» битва с «разлагающимся Западом».**

В такой интерпретации **коронавирус представлен как знак приближающейся победы над культурой, погрязшей в материализме и [основанной] на «гибельной», по мнению джихадистов, вере в силу самостоятельной личности, а не в Бога.** То есть вместо того, чтобы доверить свое будущее, защиту и спасение Всевышнему, западные потребители запасаются туалетной бумагой. Они покупают продукты вместо того, чтобы верить, что Всевышний даст им пищу, **пока не настанет время решающей битвы против безбожного Запада** – в данном случае, объединения стран, материальные ценности которых бросают вызов упрощенному мировосприятию исламистов. А оно, в свою очередь, предписывает трудиться исключительно ради загробной жизни и не пытаться повлиять на реальный ход событий.

Как и конспирологические теории, эти установки не лишены привлекательности: они предлагают логичное объяснение текущим событиям, дают ответ на вызванные пандемией бессилие и уязвимость, а также, несмотря на

весь свой нигилизм, открывают перспективу дальнейшего развития событий. Так, в разгар пандемии на YouTube наблюдался всплеск [популярности] джихадистских видео о «конце света», «крестоносцах» и «Махди» – мессии, который должен прийти накануне Судного дня и очистить мир от зла. Все это сопровождалось пространными рассуждениями о том, почему COVID-19 – это, с одной стороны, наказание, ниспосланное Аллахом, а с другой – «воин Аллаха». В частности, ИГ даже призывало своих приверженцев не «ступать на земли эпидемии».

Таким образом, реакцией джихадистов на возникший в западных странах глубокий кризис стали воззвания к мусульманам «наказать „неверных“», злорадство, а также призывы воспользоваться слабостью Запада и нестабильностью текущей ситуации для совершения нападений.

Несмотря на военное поражение ИГ, происходящее было представлено как «проявление могущества Всевышнего и раскрытие слабости врагов ислама» и, соответственно, общее содержание обращений сводится к тому, что победа обеспечена.

Более того, хотя членам и сторонникам ИГ также угрожает коронавирус, сокращение военного присутствия стран антииГИЛовской коалиции в регионе, по мнению джихадистов, может помочь «правоверным» реорганизоваться и подготовиться к борьбе с «врагами ислама».

Таким образом, COVID-19 интерпретируется как признак «последних дней» и как указание на приближающуюся «финальную битву», а также как кара небесная, призванная помочь джихадистам в борьбе с «неверными». Более того, это еще одно основание продолжать борьбу.

В общем плане актуальность исламистской идеологии также поддерживается, в частности, приходом к власти талибов в Афганистане: это *эмират* – т. е. *государство* – которое, в отличие от псевдохалифата ИГ, сегодня существует в реальности, что можно считать «историей успеха». Однако и здесь присутствуют те же смысловые элементы, что и у ИГ: возможно, только за исключением «конца света».

Некоторый парадокс состоит в том, что движение «Талибан», «Аль-Каида» и ИГ фактически являются противниками на геополитическом уровне и борются за влияние, но при этом во многом совместимы с точки зрения идеологии – если не повторяют друг друга. То есть, независимо от внутренних связей, взаимоотношений и того, как они интерпретируют приход талибов к власти, «Аль-Каида» приветствует создание «эмирата», ИГ, наоборот, говорит о том, что это была не победа, а «сговор» с американцами – идеологические основы всех трех организаций близки.

Соответственно, те, кто недоволен политикой талибов, может с легкостью перейти в ИГ-Хорасан, которое уже несколько раз заявляло о своих претензиях на власть, совершив громкие теракты. С точки зрения борьбы с террористической угрозой это усложняет ситуацию, поскольку способствует укреплению ИГ – в том или ином виде, как на уровне «регионального» отделения, так и организации в целом.

Наконец, возвращаясь к способности ИГ адаптироваться, пока сложно сказать, насколько вероятно слияние джихадистской идеологии с нацистской. Как это проявится и проявится ли – вопрос будущего. Однако как ни странно, потенциал имеется: это то, что прослеживается на примере формирования идеологии «Братьев-мусульман» в Египте в 1928 г. Как известно, лидер движения Хассан аль-Банна был поклонником Гитлера и по его распоряжению книга «Mein Kampf» была переведена на арабский язык под названием «Мой джихад» [6].

Список литературы

1. *Vochra A.* Isis urges jihadists to strike Europe and Israel while West is distracted by Ukraine // The Times, 18.04.2022. URL: <https://www.thetimes.co.uk/article/isis-urges-jihadists-to-strike-europe-and-israel-while-west-is-distracted-by-ukraine-bz0sfpf0t> (дата обращения: 29.04.2022). Режим доступа: для зарегистрир. пользователей. Текст: электронный.
2. ФСБ предотвратила теракт на Ставрополье: «РИА Новости» – 25.04.2022. URL: <https://ria.ru/20220425/terrorist-1785251955.html> (дата обращения: 29.04.2022). Текст: электронный.
3. ФСБ сообщила о пресечении теракта на железной дороге в Крыму: ТАСС – 21.04.2022. URL: <https://tass.ru/proisshestviya/14433249> (дата обращения: 29.04.2022). Текст: электронный.
4. В Крыму задержан приверженец Хизб-ут Тахрир: «РИА Новости» – 13.04.2022. URL: <https://crimea.ria.ru/20220413/v-krymu-zaderzhan-priverzhenets-khizb-ut-takhrir-1122932772.html> (дата обращения: 29.04.2022). Текст: электронный.
5. Сотрудники ФСБ опубликовали видео задержания пособников террористической организации: ФАН – 01.04.2022. URL: https://riafan.ru/22648858-sotrudniki_fsb_opublikovali_video_zaderzhaniya_posobnikov_terroristicheskoi_organizatsii (дата обращения: 29.04.2022). Текст: электронный.
6. *Duheume T.* Analysis: The Nazi roots of Muslim Brotherhood // Al-Arabiya News, 27.06.2018. URL: <https://english.alarabiya.net/features/2018/06/27/ANALYSIS-The-Nazi-roots-of-Muslim-Brotherhood> (дата обращения: 29.04.2022). Текст: электронный.

Гончар В. В.¹,
*начальник кафедры информационной
безопасности учебно-информационного комплекса
информационных технологий Московского
университета МВД России имени В.Я. Кикотя,
кандидат юридических наук, доцент*

ОСНОВНЫЕ ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОМУ ВОЗДЕЙСТВИЮ ПРЕСТУПНИКОВ

В настоящее время Интернет следует отнести к одному из основных каналов массовой информации, оказывающих наиболее эффективное воздействие на общество и особенно на молодую его часть, неопределившихся в своих мировоззренческих приоритетах, чьи взгляды на жизнь и смысловые установки еще не сформированы, а их жизненные пути развития могут сложиться как в сторону принимаемых обществом правил поведения, так и в сторону антисоциальных действий и совершения правонарушений, в том числе в сфере IT.

В последние годы основной проблемой для правоохранительных органов стали так называемые «дистанционные преступления», т. е. хищения, совершаемые дистанционным способом с использованием методов социальной инженерии. Особенности преступлений в данной сфере являются:

1. Преступное сообщество пополняет свои ряды за счет вовлечения информационно подкованных молодых людей, а также лиц, освободившихся из мест лишения свободы, которые могут изменить преступную специализацию благодаря освоению информационных технологий с последующим использованием их для противоправных действий. Вместе с приобретаемым новым криминальным опытом в сфере информационных технологий у таких представителей криминальной среды остается прошлый, которым они могут воспользоваться в определенной ситуации.

2. Лица, совершающие преступления с применением информационных технологий, это, как правило, люди зрелого возраста, реже – несовершеннолетние и пожилые (чаще мужчины). Зрелость означает сформированность личности преступника (он знает, что хочет; умеет и знает, как разговаривать с жертвой и как оказывать на нее воздействие, получает удовольствие от успешных преступных действий и т. д.). В силу специфики совершаемых киберпреступлений и того, что есть возможность получить крупные преступные доходы, с большой вероятностью избежав при этом уголовной ответственности, эта категория преступников отличается хорошей информационной подготовленностью, предприимчивостью, авантюристичностью, рискованностью. По мере накопления криминального опыта они становятся более замотивированными на совершение киберпреступлений и внесение в них креативных изменений.

¹ © Гончар В. В., 2022.

3. Киберпреступники знают, изучают и используют психологию людей для манипулирования ими и получения собственной выгоды, отличаются прогностическими и коммуникативными способностями, думают на несколько шагов вперед, просчитывают свои действия, а также действия жертвы. Их преступно-манипулятивный и корыстный психологический опыт, умение завоевывать доверие наряду с общительностью и прогностическими способностями становятся основой для дальнейшей целенаправленной практической тренировки криминальных навыков. Усиливает их криминальное мастерство и материальное (денежное) подкрепление навыков, получаемое удовлетворение от процесса и результата преступления/преступлений, групповой характер преступных действий, анонимность и безнаказанность.

С началом специальной военной операции в феврале 2022 г. получили подтверждения сведения о том, что в отношении граждан Российской Федерации последние несколько лет велись организованные и хорошо спланированные акции в информационном поле с применением социальной инженерии [3]. По всей видимости, наряду с хищением денежных средств перед преступниками стояла еще одна не менее важная задача, а именно: дестабилизация обстановки внутри страны путем создания у людей впечатления недостаточности принимаемых государством мер по противодействию «дистанционным преступлениям». Преступники работали по специально созданным методическим рекомендациям, учитывающим психологию их жертвы.

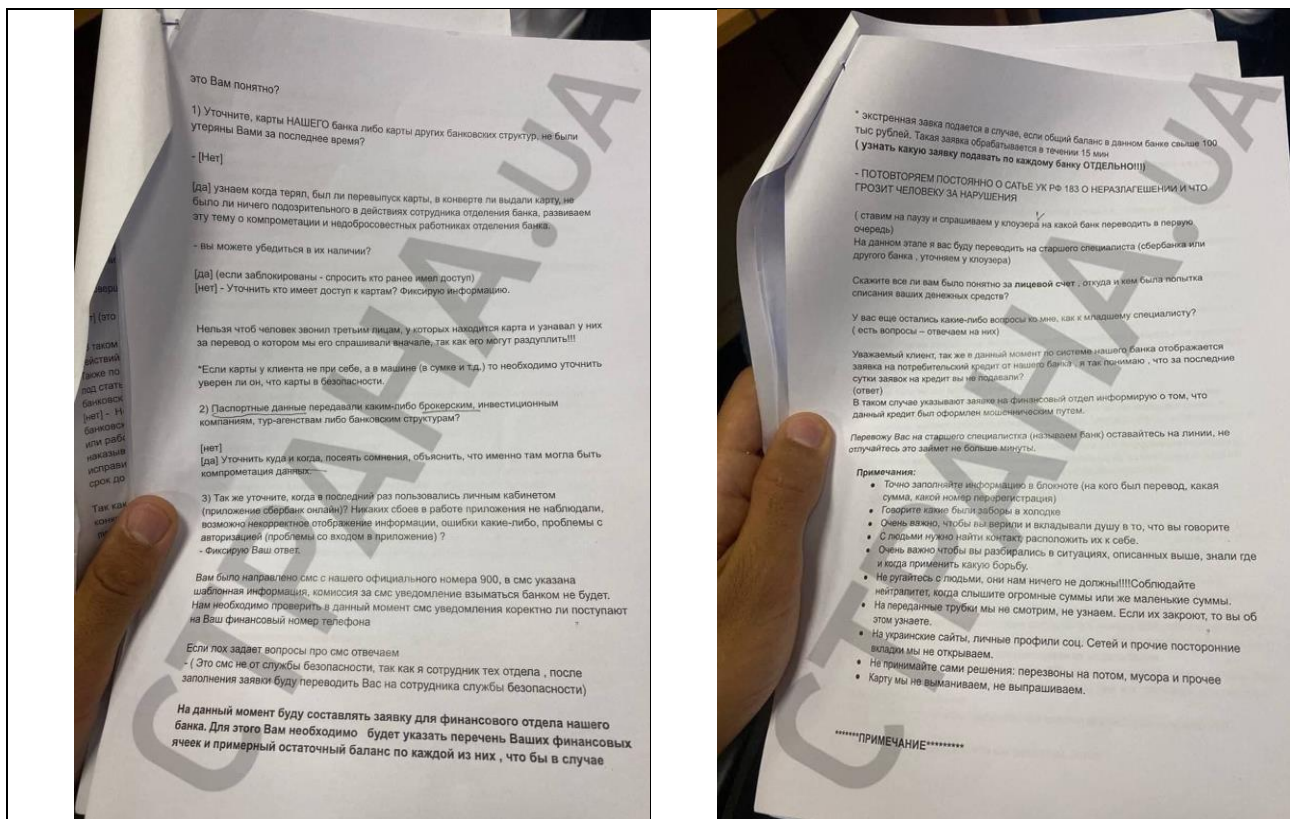


Рис. 1. Часть методических рекомендаций преступников

Анализируя типичные проблемы расследования таких преступлений, следует выделить основные:

1. Трансграничный характер преступлений. Преступники не редко находятся на территории другой страны (Украина, Литва, Латвия, Эстония, Армения), с которой у России затруднен обмен информацией.

2. Не сформирован действенный инструментарий быстрого получения от кредитных организаций, интернет-провайдеров, операторов связи, социальных сетей и интернет-сервисов информации, имеющей доказательственное значение по расследуемым преступлениям (сведений о лице, биллинге, движении денежных средств по лицевым счетам абонентских номеров и др.). Длительность получения ответов составляет от одного до нескольких месяцев.

3. Использование преступниками программного обеспечения, позволяющего избежать (или существенно затруднить) их идентификацию – VPN, TOR, SSL, а также технологий, позволяющих менять IP-адрес пользователя сети Интернет, создавать динамические или нераспознаваемые IP-адреса, применять технологии «подменных» абонентских номеров посредством IP-телефонии.

4. Недостаточная компьютерная грамотность населения. В 2020–2021 гг. участились случаи выдачи онлайн-кредитов при установке потерпевшими программ удаленного доступа к электронным устройствам и передаче прав управления преступникам. Преступники, используя методы социальной инженерии, убеждают лицо установить такие компьютерные программы как TeamViewer QuickSupport или аналогичные, после чего получают контроль над устройством потенциального потерпевшего и совершают хищения.

5. Необходимость увеличения числа государственных специалистов и экспертов, имеющих право проводить соответствующие исследования и компьютерные экспертизы. Сегодня практически отсутствуют ведомственные специалисты, способные идентифицировать компьютерную программу как вредоносную методом обратного реверс-инжиниринга. Кроме того, расследование IT преступлений усложняет длительность производства таких экспертиз и значительная их стоимость при проведении в негосударственных экспертных учреждениях (до нескольких сот тысяч рублей за одну экспертизу при причиненном в большинстве случаев ущербе в несколько тысяч рублей).

Решение данных проблем лежит в комплексе законодательных, организационных и научных мер. Кроме того, необходимо активное вовлечение представителей бизнес-сообщества в данную деятельность. Так как в настоящее время финансово-кредитные учреждения для увеличения прибыли всячески упрощают доступ к своим продуктам, нередко пренебрегая вопросами безопасности доступа к ним. Вся полнота ответственности за возможные хищения, например, в результате использования преступниками социальной инженерии возлагается на клиента, который обязан знать и уметь защищаться от всех угроз.

Необходимо принципиально изменить подход предоставления дистанционных продуктов от «Разрешено все, что не запретил клиент» к «Запрещено все, что не разрешил клиент».

Таким образом, при заключении договора банковского обслуживания клиенту автоматически подключается минимально необходимый, обозначенный им объем услуг. Рискованные услуги, например, возможность дистанционного

оформления кредита или подключение дополнительных абонентских номеров будут предоставляться только после идентификации клиента в офисе Банка или иным доверенным способом.

С началом специальной военной операции сотрудниками банковского сообщества был зафиксирован резкий спад количества «мошеннических» звонков с одновременным увеличением звонков семьям участников данной операции, что позволяет предположить о переориентации существующих колл-центров в соответствии с нуждами кураторов. Уверены, что поступательное развитие проводимой операции в дальнейшем приведет к уменьшению количества данных центров и сокращению соответствующих звонков.

Реализация данных предложений позволит существенно уменьшить количество дистанционных хищений денежных средств, поступления от которых могли идти на финансирование экстремистской и террористической деятельности.

Список литературы

1. Информационно-аналитические материалы следственных подразделений МВД России за 2020 и 2021 гг.
2. Противодействие преступлениям в сфере информационных технологий: учебник / [В. В. Гончар и др.]. М. : Московский университет МВД России имени В.Я. Кикотя, 2021.
3. <https://www.youtube.com/watch?v=YVJsLrl0oW4>.

*Ходикова Н. А.¹,
доцент кафедры философии
Академии Государственной противопожарной
службы МЧС России,
кандидат философских наук, доцент*

ИНФОРМАЦИОННАЯ ГРАМОТНОСТЬ КАК УСЛОВИЕ УСПЕШНОСТИ ПРОФИЛАКТИКИ ЭКСТРЕМИЗМА

Одним из ведущих факторов дестабилизации социально-политической ситуации, нарушения общественного спокойствия, возникновения чрезвычайных ситуаций социального характера сегодня является существование и распространение экстремизма и его крайней формы – терроризма. Экстремизм является серьезной угрозой для общественных интересов и жизни людей, поскольку он является причиной раскола в обществе, препятствует мирному сосуществованию разных национальных, религиозных и социальных групп, провоцирует преступления, зачастую очень жестокие. Что же такое экстремизм? Согласно Федеральному закону от 25 июля 2002 г. № 114-ФЗ «О противодействии экстремистской деятельности» в содержание понятия «экстремистская деятельность» включены, кроме прочих, следующие признаки:

- насильственное изменение основ конституционного строя и (или) нарушение территориальной целостности Российской Федерации;
- публичное оправдание терроризма и иная террористическая деятельность;
- возбуждение социальной, расовой, национальной или религиозной розни;
- пропаганда исключительности, превосходства либо неполноценности (нарушение прав, свобод и законных интересов) человека по признаку его социальной, расовой, национальной, религиозной или языковой принадлежности [1].

Обобщив эти признаки, можно сказать, что экстремизм – это распространение деструктивных идей и основанные на этих идеях насильственные действия, направленные на раскол общества и разрушение государства [2, с. 108].

Таким образом, одним из существенных признаков экстремистской деятельности является ее информационный характер. Не случайно в России под действие закона подпадают не только практические насильственные экстремистские действия, но и распространение экстремистской информации. Действительно, негативные последствия экстремистской пропаганды трудно переоценить. В условиях информационного хаоса (особенно на просторах интернета, который сегодня является самым доступным и удобным инструментом распространения экстремизма), который мы сегодня наблюдаем, очень легко стать жертвой заведомо ложной информации, намеренного искажения исторических, общественно-значимых данных. Особенную опасность как источник дезинформации приобрели сегодня так называемые «фейки» – специально сфабрикованные заведомо ложные провокационные «новости», распространяемые через средства массовой информации, прежде всего – через Интернет.

¹ © Ходикова Н. А., 2022.

Для молодежи особенно велика опасность поддаться ложной дезориентирующей информации, агрессивной пропаганде. Это связано с тем, что молодые люди сегодня большую часть информации получают из различных интернет-ресурсов, многие из которых содержат большой экстремистский контент. Действия государства по ограничению деятельности ресурсов, распространяющих экстремистские материалы, представляются вполне оправданными. Необходимо отметить, что молодежь сегодня очень уязвима для всевозможных манипуляций. Причин такой уязвимости несколько. Во-первых, молодые люди еще не имеют прочно устоявшихся нравственных ориентиров и системы ценностей, они психологически уязвимы, зачастую не уверены в себе, ищут тех, кто научит их жизни. Во-вторых, степень доверия к интернет-источникам в молодежной среде очень высок, ведь для многих большая часть жизни проходит в виртуальном пространстве. И именно такие молодые люди, не обладающие критическим мышлением, не находящие жизненных ориентиров и поддержки в реальной жизни (от родственников, друзей, школы), чаще всего становятся мишенью экстремистской информационно-деятельности.

Итак, экстремизм в своем основании имеет информационную природу – любому практическому действию насильственного характера, направленному против представителей определенной группы (основание деления может быть любым – национальным, религиозным, социальным), предшествует публичное распространение деструктивной информации, формирующей определенные установки. Поэтому одной из важных составляющих профилактики экстремизма является информационная деятельность тех субъектов, которые призваны противостоять распространению экстремистской идеологии. Эта деятельность должна быть направлена на предупреждение формирования экстремистского сознания, прежде всего, у молодежи [3, с. 109–110]. Направления такой информационной деятельности, очевидно, должны иметь целью смягчение потенциальных уязвимостей молодых людей, описанных выше. А именно: формирование нравственных ориентиров, системы ценностей, таких, которые несовместимы с ксенофобией, ненавистью, нетерпимостью, а также выработка навыков критического мышления, умения оценивать информацию, сопоставлять факты и их оценку, понимать различные точки зрения и т. д.

Можно выделить следующие уровни профилактики экстремизма по субъекту, целям и методам деятельности [4, с. 34–37].

1. Правовой уровень. На этом уровне государственно-правоохранительные органы выявляют фактически осуществляемую экстремистскую деятельность (как пропагандистскую, так и предметную) и борются с ней методами принуждения. Информационная составляющая здесь заключается в способности служб анализировать данные с целью выявления экстремистской деятельности.

2. Социальный уровень. На этом уровне социальные и психологические службы определяют круг тех, кто потенциально может иметь отношение к экстремизму, и проводят предупредительную работу посредством убеждения и разъяснения негативных последствий экстремистской деятельности. Этот этап является чисто информационным.

3. Социально-воспитательный уровень. Система просветительских, образовательных и воспитательных мер, предпринимаемых государственными и муниципальными органами власти и общественными организациями, направленных на формирование устойчивых позитивных установок, которые препятствуют проявлению экстремистских идей и экстремистского поведения. В отличие от двух других уровней, имеющих одностороннюю субъект-объектную структуру, здесь взаимодействие может быть осуществлено в форме диалога субъекта и объекта. Таким образом, информационная деятельность на этом этапе осуществляется обеими сторонами – как объектом, так и субъектом.

Важной подсистемой этого уровня является *социально-экспертная профилактика*. Этапы социально-экспертной профилактики (являющиеся, как не сложно заметить, чисто информационными):

1 этап. Выявление внешних условий и признаков потенциальной экстремистской активности (мониторинг контента, социальных сетей, СМИ, выявление факторов вовлеченности лиц в экстремистские и деструктивные группы, выявление мировоззренческих и социально-психологических установок экстремистской направленности).

2 этап. Работа с наиболее уязвимыми для экстремистской пропаганды социальными группами, она включает информационный и психологический аспекты:

- информирование о видах экстремистской деятельности, перечне экстремистских объединений;
- практические рекомендации по тому, как не быть завербованным в подобные объединения;
- информирование об ответственности за экстремистскую деятельность;
- формирование психологической невосприимчивости к деструктивному социальному влиянию, умения контролировать свою эмоциональную сферу;
- формирование толерантного отношения к представителям иных социальных, религиозных, национальных групп;
- развитие самостоятельного и критического мышления.

3 этап. Анализ и экспертное изложение причин экстремизма, разработка методологического инструментария для дальнейшей профилактической работы.

Авторы «Методических рекомендаций по профилактике экстремизма в России и странах Центральной Азии» [3, с. 37] считают особой и очень значимой мерой профилактики идеологии экстремизма развитие критического мышления. Как инструмент противостояния экстремистским влияниям критическое мышление позволяет разобраться в мотивах, которые побуждают экстремистов совершать преступления и особенно – вербовать новых последователей. Здесь важно понимать, что мотивы тех, кто вовлекает в экстремистскую деятельность, могут существенно отличаться от мотивов тех, кто поддается этому вовлечению. Люди, которые распространяют экстремистскую идеологию и вербуют новых сторонников, руководствуются стремлением к самоутверждению, жадностью власти, меркантильностью, стремлением к разрушению. Понять эти мотивы, увидеть их за провозглашаемыми лозунгами позволяет критическое мышление. Вообще критическое мышление является основой информационной грамотности, на которой

базируется способность человека осмысленно относиться к новостям, анализировать свои информационные потребности, выбирать информацию, оценивать ее релевантность, адекватно интерпретировать данные, выделять объективный и субъективно-политизированный контекст и т. д. [4, с. 11; 3, с. 39].

Другим важным аспектом профилактики экстремизма и других проявлений социальной агрессии является формирование у молодежи (например, в ходе изучения философии, политологии, социологии) политической культуры, элементарных навыков социального взаимодействия. Сегодня стало очевидным, что совершенно необходимо на всех этапах образования (от детского сада и до вуза) осуществлять патриотическое воспитание молодежи, включающее глубокое знакомство с историей страны, формирование уважения к ее традициям, понимания геополитических процессов в прошлом и настоящем. Кроме того, можно утверждать, что эффективным противоядием против принятия экстремистской идеологии является наличие у молодого человека сформированного комплекса навыков, которые принято называть «мягкими» или «гибкими» (soft-skills), к ним относятся, помимо критического мышления, умение работать в команде, способность мыслить творчески, нестандартно, умение понять мотивы другого человека и т. д. Патриотическое воспитание и формирование гибких навыков у обучающихся на всех уровнях является, прежде всего, задачей социально-гуманитарных дисциплин [5].

Итак, поскольку экстремизм в основе своей является, прежде всего, информационной деятельностью (основанной, например, на искажении и предвзятой трактовке общественных событий истории и современности), противодействие ему также во многом лежит в области обращения с информацией. Поэтому очень важными задачами являются формирование у молодежи (и вообще в обществе) как патриотизма, так и толерантного, терпимого отношения к «другим», развитие критического мышления, включающего, помимо прочего, способность объективно и всесторонне оценивать информацию, менять свою позицию при наличии достаточных для этого оснований, вести диалог, умение и желание находить общее в различных позициях.

Список литературы

1. Федеральный закон № 114-ФЗ «О противодействии экстремистской деятельности». URL: <https://base.garant.ru/12127578/1cafb24d049dcd1e7707a22d98e9858f/#friends> (дата обращения: 18.12.2021).
2. Старостин А. Н., Суслонов П. Е., Шиллер В. В. Профилактика экстремистских проявлений: теоретические основания и практические модели // Дискурс-Пи. 2019. № 2 (35). С. 107–117.
3. Мурзагалеев Р. И., Сулейманов А. Р. Методические рекомендации по профилактике экстремизма в России и странах Центральной Азии: выводы и мнения экспертов. Уфа : Издательство «Диалог». 2018.
4. Ходикова Н. А. Критическое мышление и информационная грамотность // Культура и безопасность. №3 (2021). С. 11–15.

5. Липский В. Н. Зачем техническому вузу научный социально-гуманитарный журнал? // Культура и безопасность. 2021. № 1. С. 5–7.

Рахмонбердиев Б. Б. угли¹,
слушатель факультета подготовки иностранных специалистов
Московского университета МВД России имени В.Я. Кикотя,
рядовой сотрудник МВД Республики Узбекистан

Куриленко Ю. А.²,
заместитель начальника кафедры информатики и математики
Московского университета МВД России имени В.Я. Кикотя,
кандидат юридических наук

УРОВНИ УГРОЗ АТАКИ ROOTKIT И МЕТОДЫ БОРЬБЫ С НИМИ

Человечество все больше сталкивается с цифровой реальностью. Люди стали применять компьютерные и мобильные технологии в качестве средства выхода в глобальную сеть Интернет в повседневной жизни. Это привело к росту числа злоумышленников, пытающихся намеренно завладеть персональными данными, в том числе при помощи ряда компьютерных атак, таких как DDoS, MiTM, Brute Force, SQL инъекции, а также rootkit. В данной статье будет рассматриваться вид наиболее сложной кибератаки rootkit, используемой для получения расширенных прав пользователя. Данная атака представляет сложный цифровой код, действующий скрытно в достаточно долгом промежутке времени, и позволяет удаленно контролировать компьютер пользователя.

Rootkit является наиболее сложным в обнаружении и удалении из разновидностей компьютерных вирусов. Находится данный вирус очень глубоко в недрах операционной системы (ОС) и специально написан таким образом, чтобы не быть замеченным антивирусными программами и другими средствами безопасности. Данный вид атаки может хранить свои и/или другие процессы, исполняемые годами, те или иные функции для каких-либо целей злоумышленника и никак не оказывать свое влияние на работоспособность компьютера.

В основном для создания данного вида атак применяются «инструменты», дистрибутивы операционных систем на базе семейства Linux. В обиходе данный вид атаки применяется для «майнинга» в целях обогащения. А именно при применении наиболее подходящих команд в терминале операционных систем Linux, предназначенных для сокрытия собственного присутствия. Роль майнера в данной команде будет играть часто применяемая программа XMRig с открытым исходным кодом [1]. В случае если злоумышленник удаленно запустит данную программу с помощью функций бэкдора, то обнаружить ее будет несложно, так как в самих процессах будет отображаться рост занимаемой данной программой ОЗУ памяти, затем администратор может закрыть процесс. Для того, чтобы атака была успешной злоумышленнику необходимо написать небольшой программный код на языке C# для пространства ядра операционной системы Linux, чтобы скрыть собственное присутствие вместе с тем процессом, который он запустил,

¹ © Рахмонбердиев Б. Б. угли, 2022.

² © Куриленко Ю. А., 2022.

а именно XMRig. Так, злоумышленник собирает исходный код и имплантирует его в ядро ОС, после чего программа самостоятельно скрывает свое наличие в системе, в которой находится. Далее, оставаясь незамеченным, злоумышленник запускает программу и сам «убивает» ее в древе процессов, успешно выполнив поставленные задачи. Таким образом, компьютер будет испытывать нагрузки, а владелец не сможет обнаружить запущенные процессы в древе открытых программ. Приведенный выше процесс «майнинга» можно обнаружить по другим косвенным признакам, например, таким как частый запуск охлаждающей системы, чрезмерное потребление энергии и т. д.

Также данные виды атаки могут быть применены в сети «Tor» или «I2P». Если задачей злоумышленника будет использование компьютера пользователя как прокси-сервера или IP-адреса данного компьютера для совершения противоправных действий или долгий промежуток времени следить за личной жизнью жертвы для сбора информации и применения ее в преступных целях, то проследить за этими процессами не получится. Обнаружить данную атаку практически нереально, если внедрить ее со стороны системы. Вредоносный код атаки может распространяться в сборке с малоизвестными дистрибутивами операционных систем, где исходный код никем не просматривался и не изучался. Также он может быть интегрирован в какую-либо программу, распространяемую под свободной лицензией. Таким образом, скачав и установив такую программу, компьютер будет инфицирован, о чем владелец даже не будет проинформирован антивирусной программой.

Данный вид атак распространен уже достаточно давно и под мобильные устройства с платформой Android, и под системы управления Windows. В ОС Windows все еще сложнее, чем на ОС Linux, так как исходный код является непрозрачным. Поэтому в качестве противодействия сами программисты компании Microsoft обеспечивают защиту и подписывают официальные драйвера с пройденной проверкой.

Основным методом борьбы с rootkit-атакой являются утилиты, направленные на поиск известных и неизвестных rootkit узкоспециальными методами, а также программы удаления, например, такие как Gmer, XueTr, Chkrootkit, Rkhunter, TDSSkiller [2]. Для менее вредоносных rootkit можно использовать некоторые антивирусные программы, такие как Kaspersky Internet Security [3]. Кроме того, профилактикой компьютерных систем будет являться использование дистрибутивов и программ, проверенных официальным сообществом. Возможно использование изолированных систем виртуализации, например, таких как изоляция программ в рамках ОС Qubes, в которой каждая программа запускается в отдельной изолированной виртуальной машине, если при каких-либо обстоятельствах программа инфицирована, то изоляция не позволит вирусу распространиться и заселить в недрах ОС [4].

Угрозы компьютерной безопасности, увеличивающиеся в разы за последние годы, требуют все новых способов защиты. Разработчики операционных систем, прикладных и антивирусных программ стремятся быть на голову выше злоумышленников, пытающихся взломать компьютерные программные продукты.

Но не стоит уповать лишь на данные средства защиты, в первую очередь необходимо соблюдать цифровую гигиену, устанавливать только лицензионные продукты, обеспечивая безопасность данных, хранящихся на персональных компьютерах.

Список литературы

1. Cryptoprofi : [сайт] / URL: <https://www.cryptoprofi.info/?p=7526> (дата обращения: 10.04.2022). Текст электронный.

2. Руткиты: проблемы безопасности и тенденции развития. URL: <https://habr.com/ru/company/xakep/blog/186072/> (дата обращения: 10.04.2022). Дата публикации: 12 июля 2013. Текст электронный.

3. Serge Malenkovich. Что такое руткит и как удалить его с компьютера. URL: <https://www.kaspersky.ru/blog/chto-takoe-rutkit-i-kak-udalit-ego-s-kompyutera/650/> (дата обращения: 10.04.2022). Дата публикации: 28 марта 2013. Текст электронный.

4. ИзLinux : [сайт] / URL: <https://blog.desdelinux.net/ru/что-вы-и-ваша-безопасность-в-изоляции/> (дата обращения: 10.04.2022). Текст электронный.

Чихирева А. А.¹,
студентка Казанского филиала ФГБОУВО
«Российский государственный университет правосудия»

Халилова Р. Р.²,
студентка Казанского филиала ФГБОУВО
«Российский государственный университет правосудия»

Научный руководитель:
Шевко Н. Р.,
доцент кафедры уголовно-правовых дисциплин
Казанского филиала ФГБОУВО «Российский
государственный университет правосудия»,
кандидат экономических наук, доцент

КИБЕРТЕРРОРИЗМ КАК УГРОЗА НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

Современный этап развития общества характеризуется повсеместным внедрением инновационных информационных технологий во все сферы жизнедеятельности. Особенно опасно использование высоких технологий в преступных целях [4]. В сложившейся ситуации особую угрозу национальной безопасности практически каждого государства, жизненно важным интересам как отдельно взятой личности, так и мирового сообщества в целом представляет информационный терроризм, как форма негативного воздействия на личность, общество и государство посредством использования всех видов информации. Посредством информационного воздействия на психику, на сознание людей с целью формирования целенаправленной реакции и поведенческого настроения кибертерроризм является наиболее изощренным преступным деянием.

Кибертерроризм является актуальной проблемой современности глобального характера, возрастающей с развитием и популяризацией информационных технологий. Как явление понятие кибертерроризма возникло не так давно. Однако за столь короткий промежуток времени он укрепил свои позиции в интернет-пространстве.

В связи с нынешней внешнеполитической ситуацией в Российской Федерации проблемы обеспечения безопасности, противодействия интернет-терроризму являются основополагающими. Статистические данные говорят сами за себя. Так, по официальным данным за последние десять лет наблюдается рост преступности террористического характера более, чем в два раза: за 2011 г. зарегистрировано 377 лиц, совершивших преступления террористического характера, в то время как за 2021 г. лиц, совершивших такие преступления, зарегистрировано 865 [1].

¹ © Чихирева А. А., 2022.

² © Халилова Р. Р., 2022.

Наиболее уязвимым и в то же время самым открытым явлением, воздействующим на национальную безопасность государства, является «банковская паника». Она заключается в многочисленном изъятии депозитов вкладчиками из-за утраты доверия к определенному банку или банковской системе в целом, опасением неплатежеспособности или банкротства банка, падением курса национальной валюты, усилением стагнации экономики, непостоянностью функционирования денежной системы страны. Последствия этого явления являются разрушительными для всей финансовой системы страны.

В качестве примера приведем ситуацию, которая сложилась во время спецоперации на Украине. Спрос населения на наличные 24 февраля 2022 г. подскочил до максимальных пределов с конца марта 2020 г. За день россияне сняли со счетов свыше 100 млрд руб. По официальным данным россияне в день начала специальной операции России в Украине сняли 111 млрд рублей наличных [2]. Отдельные авторы и «специалисты» еще больше нагнетают ситуацию сообщениями о том, что российские банки могут установить лимит на выдачу наличных средств или вообще приостановить обслуживание. Кто-то скажет, что деньги вообще конфискуют. Так как жители России за свою историю сталкивались с различными ситуациями, подобным высказываниям верят. Потом нервничают. Далее снимают деньги. Потом разочаровываются. В данной ситуации Сбербанк и ВТБ успокоили своих клиентов тем, что они готовы к любой ситуации, что отработали сценарии для защиты средств клиентов и для обеспечения работоспособности всех функций банка. Благодаря действиям Центробанка Российской Федерации для стабилизации рубля на фоне санкций, клиенты перестали массово снимать со счетов свои средства. А ведь это могло привести к ослаблению банковской системы, тем более речь шла о показателях в огромных масштабах. Но это только одно из направлений.

В данной связи немаловажными становятся и любые информационные сообщения через средства массовой информации (а в современном мире основным и пользующимся наибольшим спросом является сеть Интернет). Особенно пагубное влияние на население страны оказывает информация с веб-страниц, участвующих в распространении ложной информации, так называемых «фейковых» новостей. Большинство из «фейковых» веб-ресурсов были оперативно заблокированы, некоторые сами прекратили свое вещание на территории России после санкционных мероприятий в адрес Российской Федерации со стороны ряда зарубежных государств. Причинами для блокировки могут служить:

- призыв к насилию;
- публикация непроверенной или заведомо ложной информации.

Самой известной «фейковой» платформой была Meta Platforms, которой пользовалось большинство россиян. Однако по решению суда в России она названа экстремистской организацией, так как распространяла «информационные материалы, содержащие призывы к совершению насильственных действий в отношении граждан Российской Федерации, в том числе военнослужащих». Поэтому Роскомнадзор ограничил доступ к некоторым приложениям (таким как,

например, Instagram) из-за призывов экстремистского характера в отношении россиян [3].

Таким образом, эффективное взаимодействие госструктур в лице Роскомнадзора и правоохранительных органов оперативно позволило повысить уровень информационной защиты, остановить распространение информации, способствующей деятельности международных террористических организаций. Постоянное информационное воздействие на психику людей в условиях неопределенности, неуверенности в завтрашнем дне, отсутствие возможности сформировать свое собственное мнение и отношение ко всему происходящему способствуют нагнетанию обстановки. Противодействовать этому необходимо всесторонне. Необходимо прилагать усилия не только для открытой борьбы с терроризмом, но и для обеспечения постоянной бдительности, поскольку бездействие в условиях стабильности может привести к возникновению очагов опасности, вызванных пассивностью властей.

Список литературы

1. Портал правовой статистики Генеральной Прокуратуры Российской Федерации. URL: <http://crimestat.ru/> (дата обращения: 13.04.2022).
2. Официальный сайт РБК. URL: <https://www.rbc.ru/finances/25/02/2022/621899d69a7947901710e6f2> (дата обращения: 13.04.2022).
3. Официальный сайт Роскомнадзора. URL: <https://rkn.gov.ru/news/rsoc/news74176.htm> (дата обращения: 13.04.2022).
4. Шевко Н. Р. Актуальные проблемы обеспечения информационной безопасности современного общества / Н. Р. Шевко. Вестник Казанского юридического института МВД России. 2012. № 2 (8). С. 57–59.

Белоусов А. И.¹,
 студент Казанского филиала ФГБОУВО
 «Российский государственный
 университет правосудия»

Научный руководитель:
Шевко Н. Р.,
 доцент кафедры уголовно-правовых дисциплин
 КФ ФГБОУВО «Российский государственный
 университет правосудия»,
 кандидат экономических наук, доцент

НОВЕЛЛЫ РОССИЙСКОГО ЗАКОНОДАТЕЛЬСТВА В ОБЛАСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПО ПРОТИВОДЕЙСТВИЮ ЭКСТРЕМИЗМУ И ТЕРРОРИЗМУ

В 2022 г. в России обострилась внешнеполитическая обстановка и в связи с возникновением информационной войны против России были приняты законодательные и судебные механизмы противодействия новым формам экстремизма и терроризма.

В России экстремизмом признают деятельность лиц, направленную на уничтожение государственного строя, разбалансировка государственной территории, публичное оправдание терроризма, ношение нацистской атрибутики, публичные призывы к нарушению прав человека и др. [3].

В России стали появляться новые механизмы проявления экстремистской деятельности, такие как публичные призывы к различным формам борьбы с государством, а именно: разжигание ненависти граждан к государственной власти, дискредитация вооруженных сил и государственных органов, осуществляющих деятельность за рубежом, публичное опубликование значимой информации, являющейся заведомо ложной.

30 декабря 2021 г. в законодательство Российской Федерации было внесено понятие «иностранный агент». К одному из направлений деятельности признания лица иностранным агентом относится ведение политической деятельности в различных формах, а также в форме распространения мнений в информационных ресурсах о решениях государственных органов и о проводимой их политике, а также формирование через информационные сети отрицательных взглядов и убеждений, направленных против государственной власти [4]. Также за иностранными агентами ведется специализированный реестр, с помощью которого происходит контроль и надзор в целях недопущения ими экстремистской деятельности.

Так, например, 15 апреля 2022 г. Минюст России признал деятельность блогера-журналиста Юрия Дудь и политолога Екатерину Шульман подпадающих под действия иностранного агента. Признание данных деятелей иностранными

¹ © Белоусов А. И., 2022.

агентами вытекает из публикаций на видеохостинге YouTube о противоречивых политических взглядах и убеждениях в отношении нынешней политики России. Таким образом, введение института иностранного агента помогает обеспечить контроль и надзор за сохранением политической и правовой стабильности на информационных ресурсах, не допуская формирования экстремистской деятельности в информационном пространстве.

Следующий правовой механизм борьбы с экстремизмом – это ужесточение уголовной ответственности за ложность общественно значимой информации. В апреле 2021 г. были введены новые составы преступлений в области распространения ложной информации, выдавая ее за достоверную, которая направлена на нарушение прав человека, а также создающая угрозу безопасности государства [1].

Также в связи с действиями государственных органов и вооруженных сил России за рубежом были внесены дополнительно составы преступлений о ложной информации об их деятельности. В данном случае предполагаем, что данные механизмы законодательного регулирования помогают эффективно пресекать попытки внутреннего распространения экстремизма, которые пытаются ввести дестабилизацию внутри России, и, таким образом, введены ограничения и ответственность за распространение ложной информации в телекоммуникационных сетях.

Необходимо отметить, что в связи с участием российских вооруженных формирований за рубежом экстремистские силы пытаются дестабилизировать их деятельность, а также вызвать негативное отношение российского народа к своим вооруженным силам, тем самым были приняты решения о введении административной ответственности о дискредитации вооруженных сил. Под дискредитацией вооруженных сил принято понимать осознанные действия лиц, направленные на подрыв доверия, авторитета к деятельности вооруженных сил [2].

Необходимо отметить и применение мер борьбы с экстремизмом в информационном пространстве. Тверским районным судом от 28.03.2022 было вынесено решение по делу № 02-2473/2022 о признании экстремистской организацией компании Meta и ее информационные продукты Facebook и Instagram. В период с 2019 по 2022 гг. компания Meta нарушала российское законодательство в области противодействия экстремизму, Генеральной прокуратурой Российской Федерации были зафиксированы многочисленные публикации в Facebook и Instagram, в которых содержались материалы в оправдание нацизма, нацистской символики. После февраля 2022 г. Facebook и Instagram стали активно публиковать призывы к массовым беспорядкам в России, а также стали дискредитировать Вооруженные силы Российской Федерации в связи со специальной операцией по денацификации и демилитаризации Украины. И Facebook, и Instagram официально разрешили призывать к насилию российских граждан и лоббирование русофобских настроений в информационном пространстве.

Такие действия Генеральная прокуратура Российской Федерации расценила как публичные призывы к осуществлению экстремистской деятельности и

направила исковое заявление в суд о признании Meta, Facebook и Instagram субъектами, занимающимися экстремистской деятельностью. 28 марта 2022 г. Тверской районный суд г. Москвы вынес решение, в котором признал их продукты экстремистскими и запретил их деятельность на территории России. Таким образом, необходимо отметить, что на данный момент борьба с экстремизмом и терроризмом в информационной среде происходит через признание таких ресурсов экстремистской направленности и последующей их блокировкой.

На наш взгляд, данных механизмов недостаточно для эффективной борьбы с экстремизмом и терроризмом в информационном пространстве. Необходимо ввести дополнительные ограничения иностранных агентов путем внесения поправок в российское законодательство об ограничении иностранных агентов в пользовании информационными ресурсами, а именно – запретить им на информационных серверах социальных сетей размещать свои публикации, которые содержат экстремистские материалы или призывы к осуществлению экстремистской деятельности.

Список литературы

1. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 25.03.2022) // Собрание законодательства Российской Федерации. 1996. № 25. ст. 2954.
2. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ (ред. от 16.04.2022) (с изм. и доп., вступ. в силу с 27.04.2022) // Собрание законодательства Российской Федерации. 2002. № 1. (ч. 1), ст. 1.
3. Федеральный закон «О противодействии экстремистской деятельности» от 25.07.2002 № 114-ФЗ // СПС «КонсультантПлюс».
4. Федеральный закон от 28.12.2012 № 272-ФЗ (ред. от 14.03.2022) «О мерах воздействия на лиц, причастных к нарушениям основополагающих прав и свобод человека, прав и свобод граждан Российской Федерации» (с изм. и доп., вступ. в силу с 15.03.2022) // Собрание законодательства Российской Федерации. 2012. № 53 (ч. 1), ст. 7597.
5. Федеральный закон от 12.01.1996 № 7-ФЗ (ред. от 02.07.2021) «О некоммерческих организациях» (с изм. и доп., вступ. в силу с 01.01.2022) // Собрание законодательства Российской Федерации. 1996. № 3. ст. 145.
6. Шевко Н. Р. Актуальные проблемы обеспечения информационной безопасности современного общества / Н. Р. Шевко. Вестник Казанского юридического института МВД России. 2012. № 2 (8). С. 57–59.

Цимбал В. Н.¹,

заместитель начальника кафедры

информационной безопасности учебно-научного

комплекса информационных технологий

Московского университета МВД России имени В.Я. Кикотя,

кандидат юридических наук

ИНФОРМАЦИОННЫЙ ТЕРРОРИЗМ В СОВРЕМЕННЫХ ГЕОПОЛИТИЧЕСКИХ УСЛОВИЯХ

Происходящее на мировой арене: экономические проблемы, невозможность договориться по тем или иным вопросам и последующие после этого взаимные упреки государств, введение санкций и т. п. приводит к серьезным геополитическим проблемам, которые отражаются на различных сферах жизни как отдельно взятого человека, так и страны в целом.

Новшеством, в части их количества, последних месяцев 2022 г. стало развитие областей и массовый рост кибератак в сети Интернет. Данные действия направлены на инфраструктуру крупных IT-компаний, государственный сектор (в частности, на объекты критической инфраструктуры), ресурсы правоохранительных органов и иное. Так, к примеру, всего за два с небольшим месяца 2022 г. (с конца февраля по апрель) в Российской Федерации атаке подверглись ресурсы Министерства цифрового развития, связи и массовых коммуникаций [7], Министерства культуры [8], ОАО «РЖД» [9], крупнейших СМИ страны [10]. Официальных статистических данных на государственных ресурсах найти не удалось.

Результатами этих действий являются вывод из работоспособности атакованных ресурсов, кража данных, нарушение функционирования сетевой инфраструктуры организации и т. п.

Причем только атаками в киберпространстве все не ограничивается, так нарастают темпы информационно-психологического воздействия на население через распространение недостоверной информации, посредством СМИ, разнообразные ресурсы в сети Интернет и даже через официальные пресс-службы различных организаций, вплоть до государственных.

Классический терроризм, согласно действующему законодательству Российской Федерации, представляет собой «...идеологию насилия и практику воздействия на принятие решения органами государственной власти, органами местного самоуправления или международными организациями, связанные с устрашением населения и (или) иными формами противоправных насильственных действий» [11].

Его разновидностей, как известно, большое количество: политический, социальный, криминальный, экономический и другие. Помимо перечисленных выделяется и информационный.

Различные ученые (Л. А. Бураева, Ю. Н. Григорьев, Э. Б. Родюков, Е. А. Харич и др.) исследовали данное понятие: его значение, содержание, негативные последствия

¹ © Цимбал В. Н., 2022.

и меры противодействия. Мы же согласимся с В. И. Антюховым [и др.], которые под данным термином понимают «...процесс целенаправленного информационного воздействия на сознание людей с целью подавления их воли и дезорганизации деятельности, а также нанесения материального и морального ущерба идейным, политическим и экономическим конкурентам с применением современных телекоммуникационных и компьютерных средств».

Проблема данной разновидности террористической деятельности заключается в том, что при современных способах и средствах коммуникации, свободного обращения и распространения всевозможной информации, применении психологических методов воздействия на население целого государства либо конкретную группу людей противостоять негативным эффектам указанной противоправной деятельности довольно сложно, а иногда и вовсе невозможно.

Те действия, которые происходят сейчас в информационном пространстве сети Интернет на различных площадках, будь то СМИ, социальные сети, разнообразные сайты, форумы и иные ресурсы глобальной сети, направленные против населения Российской Федерации, являются серьезнейшей проблемой. Они не приводят к человеческим жертвам сразу, как например, при совершении террористического акта (взрыва, массового убийства и т. п.), в случае информационного терроризма этот результат отложенный, однако в дальнейшем через какой-то промежуток времени жертв может быть намного больше.

Обычный человек не всегда может разобраться в том, что ему демонстрируют и говорят, возможности его критического мышления не совершенны, а иногда оно попросту отсутствует. Объект воздействия не всегда может перепроверить получаемую информацию из иных источников, а также может и не знать, как это сделать. Но что самое страшное, в некоторых случаях – это принятие любых сведений и собственное нежелание разбираться в их точности, объективности, полноте и смысле. В итоге, он не понимает, что на него осуществляется воздействие различными изощренными информационно-психологическими способами и методами, в конечном счете он будет верить и воспринимать любую поступающую информацию, его мнением и мышлением возможно манипулировать и в дальнейшем побуждать к разнообразным действиям или бездействию.

Государственным органам необходимо со всей серьезностью и вниманием относиться к данной проблеме, не вызывает сомнения тот факт, что давление со стороны информационных противников будет только усиливаться и вряд ли в ближайшее время оно ослабнет. Как представляется, проведение разъяснительной работы, распространение объективной информации, противопоставление фактов демонстрируемым и распространяемым сведениям, повышение цифровой грамотности и осведомленности среди населения страны, т. е. активное противодействие негативному воздействию от информационных террористических акций и атак должно быть системным, своевременным и последовательным, что поможет минимизировать потенциальный разрушительный эффект.

Список литературы

1. Федеральный закон от 06.03.2006 № 35-ФЗ «О противодействии терроризму».
2. Лизунов В. В. Проблемы и виды современного терроризма // Национальные приоритеты России. 2011. № 1 (4). С. 34–42.
3. Бураева Л. А. Информационные войны и информационный терроризм в современном мире: методы и поле действия // Известия Кабардино-Балкарского научного центра РАН. 2014. № 1 (57). С. 7–11.
4. Григорьев Ю. Н., Родюков Э. Б. Информационный терроризм и безопасность общества // Наука. Культура. Общество. 2016. № 1. С. 120–129.
5. Харич Е. А. Информационный терроризм и эффективные методы обеспечения информационной безопасности // Электронный научный журнал. 2015. № 3 (3). С. 258–262. – DOI 10.18534/enj.2015.03.258.
6. Антюхов В. И., Кравчук О. В., Суходулов Р. Б. Формальный подход к информационному терроризму // Природные и техногенные риски (физико-математические и прикладные аспекты). 2012. № 3 (3). С. 62–71.
7. Минцифры сообщило об отражении атаки на сайты некоторых госорганов [статья]. URL: <https://tass.ru/obchestvo/14004657> (дата обращения: 20.04.2022).
8. Ударная волна: число DDoS-атак на российские компании выросло в 8 раз [статья]. URL: <https://iz.ru/1313624/natalia-ilina/udarnaia-volna-chislo-ddos-atak-na-rossiiskie-kompanii-vyroslo-v-8-raz> (дата обращения: 20.04.2022).
9. Официальный телеграмм-канал ОАО «РЖД». URL: <https://t.me/telerzd/1334> (дата обращения: 20.04.2022).
10. Хакеры взломали сайты ряда российских СМИ [статья]. URL: <https://www.m24.ru/news/tehnologii/28022022/435537> (дата обращения: 20.04.2022).
11. Статья 3 Федерального закона от 06.03.2006 № 35-ФЗ «О противодействии терроризму».

Пакляченко М. Ю.¹,

доцент кафедры специальных информационных технологий учебно-научного комплекса информационных технологий Московского университета МВД России имени В.Я. Кикотя, кандидат технических наук

К ВОПРОСУ ПРИМЕНЕНИЯ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ТЕРРОРИСТИЧЕСКИХ ЦЕЛЯХ

Технологии искусственного интеллекта (ИИ) открывают широкие перспективы, они не лишены риска, а некоторые вызывают существенное беспокойство как общественности, так и специалистов. Их можно использовать со злонамеренными целями, получать непредвиденные негативные последствия. Новые технологии и, в частности, ИИ могут быть чрезвычайно мощными инструментами, позволяющими добиться больших успехов в медицине, информационных и коммуникационных технологиях, маркетинге, транспорте и других областях деятельности общества и государства. Однако они также могут быть использованы в злонамеренных целях при попадании в руки преступников. В этой связи актуально формирование должного понимания потенциального риска попадания ИИ в руки преступников, главным образом, террористов, а также разработки соответствующий мер реагирования общества и государства в лице правоохранительных органов и иных силовых структур.

Хотя террористические организации в определенной степени традиционно склонны использовать различные формы «низко-технологичного» терроризма посредством таких средств, как: огнестрельное оружие, пропаганда, транспортные средства и др., терроризм в своей сущности не является застойной угрозой. Как только ИИ приобретет широкое распространение, барьеры для входа будут снижены за счет сокращения навыков и технических знаний, необходимых для его использования. Таким образом, важно ответить на следующие вопросы: когда ИИ станет инструментом в арсенале терроризма; как международное сообщество сможет подготовиться и должным образом отреагировать на это.

Хотя тактика терроризма варьируется от группы к группе и от индивидуума к отдельному человеку, можно сказать, что определенные террористические организации, как правило, не склонны к изменению своих преступных техник, отдают предпочтение испытанной эффективности оружия, такого как пистолеты и бомбы. Тем не менее терроризм не является нестатичной в своем содержании и исполнении угрозой.

Террористические группировки и отдельные преступники показали, что они могут очень хорошо адаптироваться к современным реалиям, значительно эволюционировали за десятилетия. Они продемонстрировали потенциал для инноваций, например, в своей организационной структуре посредством Интернета, став децен-

¹ © Пакляченко М. Ю., 2022.

трализованной, франчайзинговой и глобальной организацией. Они также значительно изменились с точки зрения тактики, перейдя от нерегулярной партизанской войны к деятельности в форме таргетированных (избирательных) атак.

С технологической точки зрения эта тенденция к инновациям особенно ярко проявляется в Интернете и социальных сетях, которые оказались чрезвычайно ценными для террористов. Интернет и социальные сети, другие технические и виртуализированные экосистемы, игровые онлайн-платформы стали для террористических групп мощными инструментами радикализации, подстрекательства к насилию. Благодаря указанному инструментарию преступники с легкостью могут расширять свои ряды, покупать и передавать оружие, создавать учебные пособия или инструменты, находящиеся в легкой доступности для своих членов.

Злоупотребление Интернетом и социальными сетями также является областью, в которой способность террористических групп адаптироваться, в частности, к вызовам совершенно очевидна. В ответ на усилия платформ социальных сетей и правоохранительных органов удалить террористический контент в Интернете, преступники внесли изменения в способы их использования, применив методы шифрования сообщений. Действительно, развертывание сквозного шифрования (E2EE) в свое время вызвало серьезную озабоченность у государственных служащих и специалистов по борьбе с терроризмом, поскольку оно максимально эффективно позволяло террористам быть анонимными в сети и безопасно общаться друг с другом.

Хотя технологии, безусловно, не были единственной причиной значительной эволюции терроризма, они сыграли в ней важную роль. Новейшая история изобилует примерами, демонстрирующими все более изощренное использование разнообразных технологий террористическими и воинствующими экстремистскими группировками. Террористы, как и каждый человек, в конце концов, являются «детьми своего времени». Как коллектив они полагаются на инструменты, которые им доступны, и используют их, как и любой штатный пользователь. Сущность современных технологий, аналоговых и цифровых, развита до такой степени, что злоумышленники могут с легкостью применять их без глубоких знаний и навыков с целью совершения преступлений.

Таким образом, с каждым днем передовые технологии, когда-то ограниченные специализированными сообществами, становятся все более доступными для широких масс. Ярким примером является, например, тот факт, что, если десять лет назад угроза террористической деятельности в части маневрирования флотом или «роем» дронов, несущих взрывоопасную нагрузку, была бы сочтена неосуществимой, сегодня подобный сценарий представляет собой гарантированную реальность.

Технологическое расширение функционала терроризма, новаторство в деятельности террористических групп и отдельных лиц, определяют новые и непредвиденные способы и средства совершения преступлений, которые базируются на использовании доступных коммерческих технологий в злонамеренных целях. Учитывая указанные факты, размышляя о последних тенденциях, разработках и потенциале в области ИИ, включая компьютерное зрение, нелинейное программирование и пр., возникает вопрос о том, станет ли или, корректнее, когда ИИ станет еще одним инструментом в арсенале терроризма.

Список литературы

1. Чернов С. Б. Политика противодействия финансированию терроризма: определение и угрозы в условиях развития рынка искусственного интеллекта / С. Б. Чернов // Экономические науки. 2019. № 176. С. 85–91.
2. Научная электронная библиотека «eLIBRARY.RU». URL: <http://elibrary.ru>.
3. Новостной портал «NEWSru.com». URL: <https://www.newsru.com>.
4. Электронный фонд правовой и нормативно-технической документации. URL: <http://docs.cntd.ru>.

Галиев Д. В.¹,

*преподаватель кафедры информационной
безопасности учебно-научного комплекса
информационных технологий*

Московского университета МВД России имени В.Я. Кикотя

ОСМОТР СРЕДСТВ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ ПО ДЕЛАМ ЭКСТРЕМИСТСКОЙ НАПРАВЛЕННОСТИ

В эпоху развития информационных технологий все больше следов совершения преступлений остаются лишь в виде материальных отображений действий пользователя в информационной среде. Так, например, при использовании компьютера множество действий, совершаемых с учетной записи, журналируется средствами операционной системы.

Вместе с тем многие цифровые следы являются весьма динамичной структурой. В связи с этим наиболее правильным вариантом получения доказательственной информации в полном объеме является проведение осмотра, так как в данном следственном действии отсутствуют ограничения по области исследования информации, ведь очень многие следы остаются в интернет-пространстве, доступ к которому можно получить с использованием конкретного устройства. Методами и способами получения такой информации занимается цифровая криминалистика.

Существует большое количество определений цифровой форензики и цифровой криминалистики. Цифровая криминалистика предназначена для исследования устройств, на которых зафиксирован инцидент. В этом случае цифровое устройство либо было использовано для непосредственного совершения преступления, либо оно породило цифровое событие.

Цифровое исследование или цифровая форензика – это процесс, направленный на разработку и проверку гипотез, которые отвечают на вопросы о цифровых событиях. Это становится возможным с применением научного метода, когда разрабатывается гипотеза с помощью полученных фактов, а затем эта гипотеза проверяется с использованием дополнительных доказательств, которые извлекаются из цифровых артефактов.

Цифровые артефакты – это цифровые объекты, которые содержат достоверную информацию, которая поддерживает или опровергает гипотезу.

В большем числе случаев исследования не ограничиваются одним, конкретным видом экспертизы, а применяют комплексный подход. Любые исследования компьютерных систем так или иначе подразумевают исследование накопителей данных. В этом случае объектом исследования выступает компьютерная информация, представленная в виде объектов файловых систем, программ и т. д.

¹ © Галиев Д. В., 2022.

Цифровая форензика, несмотря на свою уже продолжительную историю, все равно считается относительно новым разделом криминалистики. На рынке присутствуют программные и программно-аппаратные продукты, способствующие извлечению цифровых артефактов из исследуемого объекта.

Восстанавливаются удаленные записи журналов событий, осуществляется поиск интересующей информации по ключевым словам и пр.

Нет единого, общепринятого способа проведения расследования. Пока избранный для расследования способ и инструменты выдают достоверные результаты, а также не нарушают законодательство не имеет значения, какие способы, методы и инструменты используются. Оценка степени эффективности каждого инструмента может сводиться к балансу их стоимости, трудозатрат на использование. Эффективная оценка в любом случае будет носить субъективный характер. Используемый подход основывается на процессе расследования преступлений, описанном в статье [1, с. 23]. В этом случае имеется место преступление, которое включает в себя цифровую среду, формируемую из программного и аппаратного обеспечения. Процесс состоит из трех основных этапов:

- сохранение состояния системы;
- поиск доказательств;
- реконструкция событий.

Этапы расследования не обязательно должны следовать один за другим (рис.1).

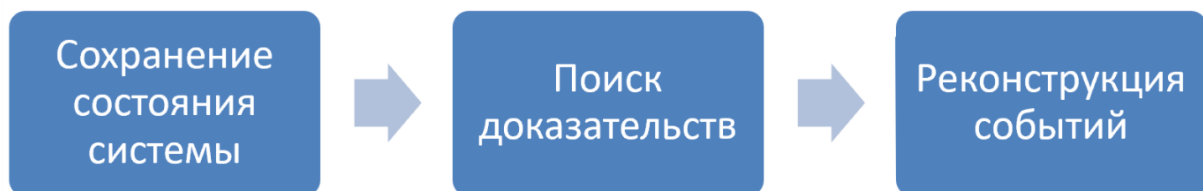


Рис. 1. Этапы расследования

Этот процесс пригоден для исследования систем в различных состояниях. Анализ в реальном времени производится непосредственно во время работы операционной системы для того, чтобы найти цифровые артефакты. Анализ накопителя из-под другой операционной системы используется для запуска доверенных приложений для сбора цифровых артефактов в доверенной среде. При анализе работающей системы присутствует риск получения ложной информации, так как в системе может оставаться активным злоумышленник или программное обеспечение, которое способно скрывать или фальсифицировать данные. Анализ накопителей более предпочтителен.

С целью предотвращения утраты цифровых артефактов, из которых может быть извлечена информация, связанная с расследуемым инцидентом, необходимо создавать побитовые копии всех исследуемых накопителей. В случае анализа в реальном времени – подозрительные процессы могут быть остановлены, сетевое подключение может быть отключено или межсетевой экран настроен на блоки-

ровку всех соединений с целью предотвращения удаленного доступа злоумышленника к исследуемой машине. Необходимо отметить, что важные цифровые артефакты могут быть удалены в процессе проведения осмотра из-за некоторых типичных ошибок специалиста. Например, если необходимо считать файлы, можно сохранить их временные копии для того, чтобы сохранить время последнего доступа к исходным файлам.

Одним из наиболее интересных подходов в проведении осмотра без риска внести изменения в накопитель – использование систем виртуализации. Так, например, VMware Workstation позволяет использовать физические устройства в качестве накопителей в виртуальной машине. Таким образом, подключив накопитель через аппаратный блокиратор, либо используя блокирование записи средствами операционной системы можно запустить ОС с данного диска. При этом виртуальная машина будет записывать изменения не на съемный накопитель, а во временный кэш-файл.

Для того, чтобы сделать это необходимо запустить VMware Workstation -> Create a New Virtual Machine->"Custom (advanced)"->Next >> Create New Virtual Machine.

Важно выбрать ESXi 6.7 или ESXi 6.5.

Выбор технических характеристик не так важен, за исключением HDD, тут необходимо выбрать подключенный через блокиратор PhysicalDriveN – use physical disk.

Особое внимание уделите типу контроллера накопителя на жестких магнитных дисках. В случае ошибки с большой долей вероятности запуск завершится ошибкой с «синим экраном».

Также важно в настройках дисков указать режим работы виртуального накопителя как независимый.

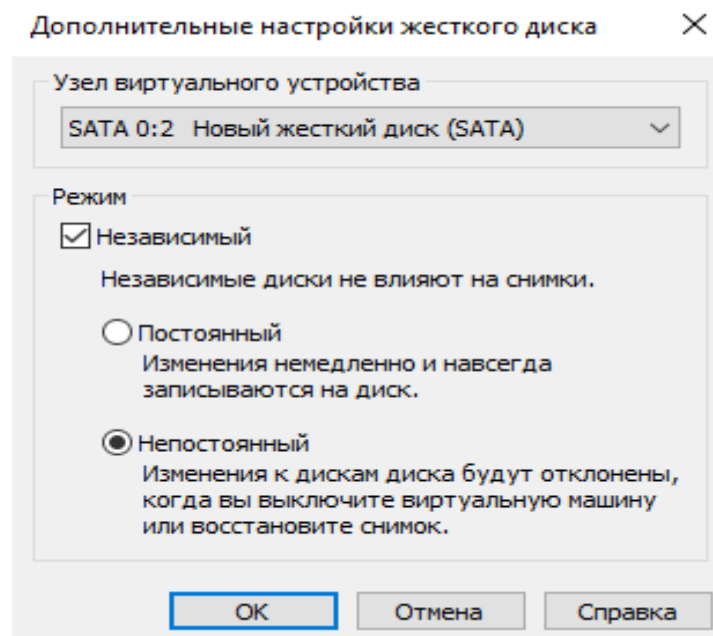


Рис. 2. Настройки виртуального устройства

Когда все необходимые цифровые артефакты собраны, для обеспечения неизменности необходимо выполнить расчет хэш-сумм по нескольким алгоритмам. Алгоритм MD5 более не считается надежным [2] и требуется использовать несколько алгоритмов одновременно (MD5, SHA-1, SHA-256). Алгоритм хеширования представляет собой математическую функцию, которая генерирует выходное значение на основе входных данных. Если какой-либо бит во входных данных изменяется, выходное значение меняется. Алгоритмы разработаны таким образом, что очень сложно подобрать два входных значения, которые генерируют одинаковое выходное значение. Поэтому, если значение, полученное в результате расчета хэш-функции, изменилось – данные были изменены.

Например, если выполняется поиск следов работы в сети Интернет, то просматриваются кэш WEB-браузера, история посещения, список закладок [3, с. 28].

Важно не забывать искать доказательства, опровергающие гипотезу, а не концентрироваться только на подтверждении. В теории процесс поиска доказательств очень прост. Определяются общие характеристики объекта исследования, а затем выполняется поиск цифровых артефактов в нем [4, с. 192].

Заключительным этапом исследования является использование доказательств, которые были найдены, и определение того, какие события произошли в системе. Исследование позволит ответить на вопросы о событиях, произошедших в системе, и действиях пользователя. После этапа реконструкции событий становится возможным сопоставить цифровые события с имевшими место произошедшими событиями.

Список литературы

1. Brian D. Carrier, Eugene H. Spafford (2003). Getting Physical with the Digital Investigation Process.
2. Wang, Xiaoyun, Yu, Hongbo. (2005). How to Break MD5 and Other Hash Functions. Lecture Notes in Computer Science. 3494. 561–561. 0.1007/11426639.
3. Федотов Н. Н. Форензика – компьютерная криминалистика. М.: Юридический Мир, 2007.
4. Противодействие преступлениям в сфере информационных технологий: учебник / В. В. Гончар и др. М.: Московский университет МВД России имени В.Я. Кикотя, 2021.

Худяков В. В.¹,

доцент кафедры информатики и математики

Московского университета МВД России имени В.Я. Кикотя

ПРОБЛЕМЫ КИБЕРБЕЗОПАСНОСТИ В ДЕЯТЕЛЬНОСТИ СОТРУДНИКОВ ОРГАНОВ ВНУТРЕННИХ ДЕЛ ПРИ РАБОТЕ С ИСОД МВД РОССИИ

В целях оптимизации и повышения эффективности работы сотрудников органов внутренних дел с информационно-справочными и поисковыми системами в территориальных органах МВД России, единого централизованного подхода к работе с электронно-вычислительными средствами хранения и обработки информации было принято решение в 2014 г. о вводе в эксплуатацию единой системы информационно-аналитического обеспечения деятельности МВД России (ИСОД МВД России). Процесс развития и внедрения ИСОД МВД России протекал не без шероховатостей. Плановых централизованных программ обучения работе с ИСОД МВД России не предполагалось. Сотрудникам органов внутренних дел, ответственным за внедрение того или иного сервиса в регионе Российской Федерации, приходилось самостоятельно изучать порядок работы с сервисами по предложенным в системе техническим описаниям и методическим разработкам, а затем проводить занятия внутри подразделений со своими коллегами. В некоторых случаях обучение работе с сервисами происходило с опорой на интуицию, методом проб и ошибок. Приоритетной задачей в процессе внедрения и дальнейшего использования сервисов ИСОД являлось приобретение необходимых навыков работы с ними и распространение полученного опыта работы в подчиненных подразделениях. Вопрос обеспечения информационной безопасности в данном потоке работы своей актуальности не терял, но и в составе основных задач безусловным элементом не являлся.

В ряде регионов со слабым развитием информационных систем, где внедрение сервисов ИСОД МВД России можно было сравнить с мега прорывом в области информационных систем, у сотрудников органов внутренних дел зачастую отсутствовали необходимые знания для поддержания на должном уровне состояние информационной безопасности.

Так, например, под одной учетной записью пользователя работало сразу несколько сотрудников подразделения. В качестве оправдания своим действиям приводили тот факт, что они выполняют одну и ту же работу и не видят существенной разницы, кто будет авторизован в системе.

Зачастую встречались случаи, когда сотрудники органов внутренних дел рядового и руководящего составов записывали свои логин и пароль на самоклеящийся стикер и закрепляли его на мониторе своего автоматизированного рабочего места, или подобного рода шпаргалку хранили под клавиатурой на своем рабочем столе. Стоит отметить, что подобного рода нарушения требований кибербезопасности встречаются и сегодня. При проведении внезапных проверок

¹ © Худяков В. В., 2022.

должностными лицами, ответственными за информационную безопасность и доступ к справочно-поисковым системам МВД России (администратор безопасности), установлено, что каждый пятнадцатый сотрудник, зарегистрированный в системе ИСОД МВД России, допускает подобного рода нарушение.

В настоящее время продолжают иметь место факты работы сотрудников полиции под одной учетной записью, когда один из пользователей системы ИСОД прошел авторизацию в начале дежурной смены, а после ее окончания забыл прекратить к ней доступ, т. е. из системы не вышел. В свою очередь сотрудник полиции из числа новой дежурной смены продолжает работать с системой, но не под своей учетной записью, а под учетной записью своего товарища. Данные факты чаще всего встречаются в дежурных частях территориальных органов МВД России.

В приведенных примерах просматривается грубое нарушение нормативных правовых актов, регламентирующих порядок доступа к справочно-поисковым системам и соблюдение требований обеспечения конфиденциальности [1].

Независимо от наличия и качества программно-аппаратной системы защиты персонального компьютера, наиболее слабым звеном в дуэте компьютер – человек остается последний. По статистике 85 % взломов информационных систем происходит путем воздействия на человека с применением элементов социальной инженерии и фишинговых атак [2].

Поступившее электронное сообщение на служебный почтовый ящик домена @mvd.ru сотрудниками органов внутренних за частую воспринимается, как достоверное, не требующее дополнительной проверки указание или информация. Вероятность того, что письмо могло быть подготовлено злоумышленником или адрес отправителя не известен получателю сообщения и содержание письма вызывает сомнение, не рассматривается. Например, в конце минувшего года поступившее сообщение, якобы от сотрудников информационной безопасности, с требованием направить на предложенный в письме почтовый адрес свои учетные данные для входа в систему ИСОД МВД России с целью проверки, у некоторых сотрудников полиции не вызвало никаких подозрений и было выполнено, даже несмотря на то, что проведение проверки было запланировано в период новогодних празднеств. Таким образом, злоумышленники, получив необходимые логин и пароль для доступа к ИСОД МВД России, на время длинных новогодних выходных имели возможность доступа к справочно-поисковым банкам данных системы. А какие сервисы становятся доступными для преступников, возможно выяснить сразу после завладения логином и паролем к ИСОД МВД России и входа в систему на страницу профиля пользователя, где указаны занимаемая должность и наименование подразделения.

К великому сожалению, всегда остается риск оказаться очередной жертвой киберпреступников. Необходимо понимать, что ослабление бдительности при работе с информационными ресурсами и нарушение элементарных правил поведения в информационном пространстве с использованием киберустройств является причиной всех бед в данном пространстве.

Основным и наиболее очевидным способом защиты от различных методов кибератак и применения приемов социальной инженерии безусловно является обучение сотрудников необходимым знаниям и умениям.

Каждый сотрудник в организации для поддержания информационной безопасности должен знать требования руководящих документов и наставлений, в которых содержатся правила по ведению переговоров в служебной обстановке и бесед вне рабочего времени. Сотрудник должен осознавать меры ответственности, применяемые к нему, в случае разглашения конфиденциальной информации. Иначе говоря, каждый сотрудник, независимо от занимаемой должности, должен знать на какие вопросы и на какие темы можно общаться с посторонним лицом, в том числе при проведении служебных переговоров. Любая информация, несанкционированно переданная посторонним лицам, может оказать неблагоприятное влияние на устойчивость информационной безопасности.

Каждый сотрудник должен выполнять требования регламентов по поддержанию информационной безопасности в организации такие, как:

1. Учетные данные: логин и пароль являются собственностью организации, предоставляются сотруднику на время его работы в ней.

2. Перед началом работы с сотрудником проводится занятие, на котором разъясняется, что предоставленные учетные данные не могут быть использованы вне организации. То есть не допускается использовать учетные данные для регистрации в социальных сетях и интернет-ресурсах. Кроме этого, передавать свои учетные данные посторонним лицам, в том числе коллегам по службе не допускается ни при каких обстоятельствах: выход в отпуск, болезнь, командировка и т. д.

3. На регулярной основе проводить занятия с сотрудниками для поддержания их знаний по информационной безопасности на высоком уровне.

4. Проводимые занятия должны отвечать современным требованиям и соответствовать уровню существующих информационных угроз.

5. Наличие в организации регламентов, определяющих порядок работы сотрудников по обеспечению информационной безопасности, обязательно. Сотрудник должен иметь доступ к документации для ознакомления с ней.

6. В регламентах должны быть рассмотрены вопросы о порядке общения, в том числе с посторонними лицами, какие сведения не допускается передавать третьим лицам, на какие темы вести разговор и т. д. В случае, когда тот или иной человек проявляет чрезмерное любопытство к информации, составляющей служебную тайну, доступ к которой ему ограничен, о данных фактах необходимо информировать администраторов безопасности и своего руководителя.

7. Все сотрудники должны знать порядок приема посетителей по служебным вопросам. Остальные переговоры и встречи допускаются в нерабочее время за границей территории организации.

8. Обязательно должен быть указан порядок пребывания в организации и для посетителей. Прибывший в организацию человек должен иметь возможность ознакомиться с правилами и временем посещения. Нахождение на территории

органа внутренних дел посетителя без сопровождения уполномоченным сотрудником не допускается.

9. На компьютере сотрудника органа внутренних дел в обязательном порядке должно быть установлено антивирусное программное обеспечение с актуальными обновлениями антивирусных баз. При этом необходимо учитывать наличие брандмауэра в рабочем состоянии.

10. Локальные ведомственные сети должны быть под постоянным контролем специального оборудования и программ на предмет выявления необоснованной активности в сети, которая в последующем может перерасти в компьютерную атаку или стать причиной утечки конфиденциальной информации.

11. Права пользователей в компьютерной системе и сетях должны быть максимально ограничены и достаточны для выполнения ими своих функциональных обязанностей. Свободное использование посторонних компьютерных программ и приложений влечет за собой нецелевое расходование служебного времени и дополнительную загруженность компьютеров и сетей.

Предложенный перечень правил является далеко не полным для обеспечения информационной безопасности при работе с сервисами ИСОД МВД России, но его выполнение позволиткратно повысить устойчивость от преступных посягательств со стороны злоумышленников.

Список литературы

1. Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 30.12.2021) «Об информации, информационных технологиях и о защите информации» // СПС «КонсультантПлюс» (дата обращения: 20.04.2022).

2. Мэтт Альгрэн. 40+ статистических данных и фактов о кибербезопасности на 2022 год. URL: <https://www.websiterating.com/ru/research/cybersecurity-statistics-facts> (дата обращения: 20.04.2022). Дата публикации: 12 апреля 2022 г. Текст электронный.

Борзунов К. К.¹,

старший научный сотрудник,

доцент кафедры информационной безопасности

учебно-научного комплекса информационных технологий

Московского университета МВД России имени В.Я. Кикотя,

кандидат технических наук

ПРАВОВАЯ ОСНОВА МОДЕЛЬНОГО ЗАКОНА ОДКБ «ОБ ИНФОРМАЦИОННОМ ПРОТИВОБОРСТВЕ ТЕРРОРИЗМУ И ЭКСТРЕМИЗМУ»

И по сей день заслуживающими внимания остаются термины и определения, данные в Доктрине информационной безопасности Российской Федерации (далее – Доктрина информационной безопасности) [1], в Федеральном законе «О безопасности критической информационной инфраструктуры Российской Федерации» [2] и в Модельном законе ОДКБ «Об информационном противоборстве терроризму и экстремизму» [3] (далее – Модельный закон).

В Доктрине информационной безопасности давалось понятие информационной сферы и упор делался на обеспечение национальной безопасности Российской Федерации именно в информационной сфере. Таким образом, возникали представления об информационной безопасности Российской Федерации. Доктриной информационной безопасности предполагается, в частности, обеспечение безопасности информации, а точнее обеспечение безопасности информационных ресурсов, которые в техническом и технологическом планах развивались как особый компонент информационной инфраструктуры Российской Федерации.

В Федеральном законе «О безопасности критической информационной инфраструктуры Российской Федерации» развивались представления о критической инфраструктуре. Так, в частности, давалось понятие «критической информационной инфраструктуры». Далее потребовалось введение дополнительных понятий «объектов критической информационной инфраструктуры» и «субъектов критической информационной инфраструктуры».

И, таким образом, уже Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» нацеливал на обеспечение безопасности как объектов критической информационной инфраструктуры, так и субъектов критической информационной инфраструктуры.

В Модельном законе устанавливались появившиеся дополнительные термины, которые ранее никак не обозначались в Доктрине информационной безопасности *легитимная информационная среда; террористическая и экстремистская информационная среда*. Причем в Модельном законе легитимная информационная среда – это та среда, которая подлежит защите правоохранительными органами, а террористическая и экстремистская информационная среда – это та среда, которая должна подавляться правоохранительными органами.

¹ © Борзунов К. К., 2022.

В условиях проведения Российской Федерацией Специальной военной операции на территории Украины (с 24 февраля 2022 г.) и фактически в ходе противостояния и США, и странам – членам НАТО, и их сторонникам можно отметить, что Российская Федерация успешно реализует защиту собственной легитимной информационной среды, с одной стороны. И, с другой стороны, пока пассивно, не превосходя в противоборстве коллективного противника, оказывает давление на террористическую и экстремистскую информационную среду, угрожающую Российской Федерации.

В Модельном законе устанавливается дополнительный термин *«информационная инфраструктура»*.

В сравнении с Федеральным законом «О безопасности критической информационной инфраструктуры Российской Федерации», который вводил понятие «объектов критической информационной инфраструктуры», этот термин *«информационная инфраструктура»* – несколько иной. Он уже предполагает большее количество объектов, которые требуют повышенного внимания со стороны правоохранительных органов.

Модельный закон развивает понятие «информационное противоборство терроризму и экстремизму». И при этом детализируется информационное противоборство терроризму и экстремизму до уровня информационно-технического и информационно-психологического.

В условиях проведения Российской Федерации Специальной военной операции на территории Украины, начиная с мая 2022 г., появились планы в рамках информационно-технического противоборства терроризму и экстремизму подвергнуть воздействию информационную инфраструктуру Украины. При этом оказывается законным использование информационных операций, которые предусматриваются Модельным законом и могут быть реализованы в виде конкретных действий информационно-технического, информационно-психологического, разведывательного, оперативно-разыскного по воздействию на террористическую и экстремистскую информационную среду на территории Украины и по защите легитимной информационной среды Российской Федерации.

Эффективность ведения информационного противоборства в Модельном законе видимо определяется понятием «информационное превосходство». Обращая внимание на ситуацию, возникшую к исходу 2021 г. в отношениях между Российской Федерации, с одной стороны, и США с их многочисленными сторонниками, с другой стороны, можно отметить, что Российская Федерация использует одну из апробированных информационных операций – *применение «сыворотки правды»*. И пока нет каких-либо данных об активном использовании информационных операций Российской Федерации в рамках проведения Специальной военной операции на территории Украины.

Остальные понятия, не определяемые, но используемые в Модельном законе, понимаются в соответствии с их определениями, установленными иными модельными законами ОДКБ и национальным законодательством государств – членов ОДКБ.

Обращая внимание на некоторую практику использования Модельного закона, Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации», Доктрины информационной безопасности Российской Федерации, можно отметить следующее.

Среди упоминаемых принципов информационного противоборства терроризму и экстремизму в ст. 3 Модельного закона в условиях проведения Российской Федерации Специальной военной операции на территории Украины и активной информационной войны стран Западной Европы во главе с США по отношению к Российской Федерации приоритетными можно считать принципы превентивности, приоритета мер предупреждения терроризма и экстремизма, недопустимости уступок террористам и экстремистам, правомерности причинения вреда террористам и экстремистам.

Вполне очевидно, что в данном случае терроризм и экстремизм воплощается через национализм и более того через нацизм, корни которого укрепились на Украине со времен Великой отечественной войны (1941–1945 гг.).

Российская Федерация, оказавшись в указанных выше условиях, в соответствии со ст. 4 Модельного закона стремится к достижению, прежде всего, следующих трех основных целей:

- разоблачения террористической и экстремистской идеологии, а также форм и методов ее распространения, навязываемой со стороны США и их многочисленными пособниками;
- повышения эффективности деятельности государственных органов Российской Федерации, осуществляющих противодействие терроризму и экстремизму;
- объединения усилий государственных структур и общественных институтов Российской Федерации в вопросах профилактики терроризма и экстремизма.

Однако, пока на текущем этапе не удастся приблизиться к цели достижения и удержания информационного превосходства в информационном противоборстве терроризму и экстремизму. И следует отметить, что причины подобного состояния неизвестны в силу вполне определенных ограничений доступа к данным по проведению Российской Федерации Специальной военной операции на территории Украины.

Но для достижения указанных целей, видимо, необходимо решить определенные задачи. Современная практика комплексного и, можно сказать, глобального противостояния Российской Федерации обозначенному противнику показывает, что пока решаются задачи через работу средств массовой информации по снижению информационно-психологического воздействия идеологии терроризма и экстремизма на личность, общество и государство. Способствует этому также имеющийся «иммунитет» взрослой части населения Российской Федерации, а именно сохранение в коллективной памяти (массовом сознании) истории Второй мировой войны и, в частности Великой отечественной войны – об истоках и причинах нацизма, о жертвах геноцида целого ряда народов, о подвигах героев, приведших к подавлению нацистских идей и разгрому фашистской Германии и их союзников.

Криминальная обстановка на территории Российской Федерации показывает, что в целом решается задача обеспечения профилактического воздействия на население с целью недопущения вовлечения его представителей в террористическую и экстремистскую деятельность. По всей видимости, не допускается использование террористами и экстремистами телекоммуникационных средств для подготовки и совершения преступлений, а также информационного обеспечения своей деятельности.

Несколько сложнее обстоит дело в Российской Федерации по обеспечению упреждающего характера информационного воздействия на террористическую и экстремистскую информационную среду, и защиты легитимной информационной среды, что определяется вполне определенным отставанием в развитии соответствующих информационных технологий. И не случайно одним из приоритетов указана Правительством Российской Федерации необходимость резкой интенсификации развития отечественных информационных технологий.

Список литературы

1. Доктрина информационной безопасности Российской Федерации (утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. № 646).
2. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
3. Постановление Парламентской Ассамблеи Организации Договора о коллективной безопасности о проекте модельного закона ОДКБ «Об информационном противоборстве терроризму и экстремизму» от 30 октября 2018 г. № 11-3.3.

*Лустин В. И.¹,
старший преподаватель кафедры информационной
безопасности учебно-научного комплекса
информационных технологий Московского университета
МВД России имени В.Я. Кикотя*

ВОПРОСЫ РАЗГРАНИЧЕНИЯ ПРЕСТУПЛЕНИЙ ЭКСТРЕМИСТСКОЙ НАПРАВЛЕННОСТИ И БАНДИТИЗМА

Многие из тех, кто устраивает теракты, ранее имели тесную связь с преступными кругами или даже были вовлечены в их деятельность. Более того, доходы от незаконной преступной деятельности являются источником финансирования большей части терактов.

В исследованиях указывается на тонкую грань между преступными и террористическими организациями джихадистской направленности в Европе. Учитывая данные факторы, можно увидеть тесные связи между преступностью и терроризмом во многих странах. Основываясь на подробном анализе Международного центра исследования радикализации и политического насилия, необходимо отметить тот факт, что ряд вставших на сторону террористических движений джихадистов, проживающих в Европе, находились ранее в преступной среде, а также отбыли наказание за эту деятельность.

Выявленная закономерность прослеживается для многих активных членов в террористической организации. Однако это работает не для всех категорий джихадистов, некоторые из которых считались хорошо интегрированными и занимающимися честной деятельностью. Женщины, с другой стороны, занимают особое положение и вовлекаются в сотрудничество на религиозной основе.

Рассматривая далее и возвращаясь к мелким преступникам, ставшим джихадистами, отмечается, что террористическим организациям удалось стать привлекательными в достаточной степени, чтобы заставить их уйти из своей обычной жизни. Более того, их убедили, что им нужно пожертвовать собой на алтарь нового «дела». Вербовщики нередко предлагали им приключения «Безумного Макса», при этом использовались методы психологического и религиозного воздействия, предлагалось искупление всех прошлых прегрешений (какими бы они ни были) в джихаде. И это несмотря на то, что руководство террористических организаций, которое по всей территории, еще находившейся под своим контролем, крайне жестоко наказывает за любые проступки: отрезает руку ворам, забивает камнями за измену и проводит еще более суровые репрессии за другие виды преступлений (например, за употребление и оборот наркотических средств).

Джихадистское движение активно использует квалификацию преступников, отчасти для обеспечения независимости в вопросах финансирования своих ячеек в Европе. Следует отметить, что «Аль-Каида» действовала точно так же: каждая ячейка должна была обеспечить свою деятельность как можно больше.

¹ © Лустин В. И., 2022.

Насколько тонка здесь линия? «Исламское государство» удивило «Аль-Каиду» и начало вербовать последователей среди «профессиональных» бандитов.

В целом, «Аль-Каида» не казалась особенно привлекательной для европейских преступников. Требовались минимальные знания исламистской идеологии и часто для этого необходимо было осуществить следующее: изучить арабский язык в медресе (Египет, Йемен или Пакистан), пройти упорные тренировки в отдаленных лагерях без привычных западных удобств. Фронт в Сирии был новшеством в этом плане, потому что «волонтеры» находили там не только приключения, но и своеобразное «общество потребления», в котором все и вся переправлялось контрабандой. Одно время его даже называли «джихадистским курортом». Идеологи религиозных террористических движений прекрасно понимали настрой и стремления молодых западных бунтарей. И они дали им то, чего они ждали.

Необходимо отметить, что ИГИЛ по своим собственным причинам установил тесные связи с международными преступными организациями, такими как турецкая мафия. Именно она была занята поставками людей и оборудования ИГИЛ и получала в обмен нефть, антиквариат и сырье. Однако не удалось выявить в полном объеме масштабы незаконного оборота наркотиков, который, по-видимому, используется ИГИЛ. В этой области «Аль-Каида» и ее поставки афганского опиума в различные регионы имеют приоритет.

Дело в том, что такие перемещения требуют от преступности активных действий в логистических целях. Высокопоставленные преступники заинтересованы в получении прибыли от своей деятельности, поэтому сотрудничество организованной преступности и террористических движений осуществляется до тех пор, пока оно приносит доход. Возможно, турецкая мафия потеряет интерес к ДАИШ, так как «Исламское государство», скорее всего, прекратит свое существование как таковое, хотя, не будем питать никаких иллюзий, завтра этого не произойдет. Таким образом, борьба с преступностью может помочь нам в борьбе с терроризмом, лишив его части финансирования.

Новый фактор современности состоит в том, что ДАИШ вербует среди преступников. Если эти активисты не в силах отправиться на землю джихада, то могут начать борьбу в своей стране, воспользовавшись связями в преступных кругах для формирования опасных независимых ячеек.

Как обычно, какого-то одного глобального решения тут не существует. Эффективнее бороться с двумя этими явлениями можно лишь при действительной реализации следующих мер: приведение законов (по возможности) к общему знаменателю, расширение сотрудничества судебных органов, полиции и разведки и т. д. Договариваться об этом можно лишь на самом высоком политическом уровне. И хотя интересы там зачастую расходятся, борьба с преступностью и терроризмом не может не интересовать подавляющее большинство государственных лидеров.

Борьба как с террористическими движениями, так и с организованной преступностью должна проводиться совместно — комплексно.

Основными разграничивающими признаками этих преступлений выступают элементы объективной стороны и цели совершения преступлений. Обязательный признак объективной стороны бандитизма – создание устойчивой, вооруженной группировки (банды) в целях нападения. При терроризме создание террористической группировки – лишь приготовление к квалифицированному терроризму, а террористический акт, совершенный организованной группой – квалифицированный терроризм. Нападение – основное общественно опасное действие бандформирований. Терроризм не связан с насилием над конкретными людьми и представителями государственных и общественных организаций, он, скорее, представляет собой «рассеянную» угрозу или опасность населению, обществу.

Таким образом, бандитизм – это организация устойчивой преступной группы, которая может быть мобилизована в любой момент и преступления направлены, в основном, против интересов граждан, а терроризм – это преступления против государства с предъявлением неких условий, требований.

Список литературы

1. Глебова Н. Экономика «Исламского государства» // URL: <http://rabkor.ru/columns/analysis/2015/07/15/the-isis-economy/>.
2. Дамаскин О. В. Криминологические аспекты детерминации современного экстремизма и терроризма : монография. М., 2018.
3. Клейменов И. М. Международный терроризм и транснациональная организованная преступность // Вестник Омского университета. 2017. № 3 (52).
4. Тихонов А., Медведев С. Как противостоять терроризму // URL: <http://archive.redstar.ru/index.php/eliseeva/item/5018-kak-protivostoyat-terrorizmu>.

Клочкова Е. Н.¹,

доцент кафедры специальных информационных технологий УНК ИТ

Московского университета МВД России имени В.Я. Кикотя

ВЫЯВЛЕНИЕ ИНТЕРНЕТ-СТРАНИЦ НЕСОВЕРШЕННОЛЕТНИХ, ПОТЕНЦИАЛЬНО ПОДВЕРЖЕННЫХ ПРОЯВЛЕНИЮ ЭКСТРЕМИЗМА

Развитие компьютерных технологий и электронных средств массовой информации повлекло формирование единого мирового информационного пространства, которое не могло не стать сферой ожесточенной борьбы. Если различные преступные элементы в качестве площадки для своих противоправных действий стали использовать информационное пространство, то и правоохранительным органам приходится его осваивать для пресечения, предупреждения, профилактики преступлений, т. е. мы, можем говорить о том, что в современном мире достаточно распространенным действием стало информационное противоборство.

Информационное противоборство реализуется в форме психологических операций и активных информационных мероприятий, использующих специальные методы, способы и средства манипулирования общественным сознанием. В России создана большая технологическая база, с помощью которой обнаруживаются и расследуются преступления, связанные с противоправными, а иногда деструктивными информационными воздействиями.

Но нельзя забывать о том, что злоумышленники также пользуются некоторыми информационными ресурсами и пытаются воспрепятствовать превентивной деятельности либо и вовсе скрыть факт осуществления своей деятельности.

Одна из проблем, которая в последние годы резко обострилась, это вовлечение подростков в организации экстремистской направленности. Несовершеннолетние молодые люди привлекаются к различным мероприятиям, начиная от распространения литературы радикального характера и заканчивая подготовкой, проведением и участием в массовых беспорядках. Данная категория наших граждан, являясь одной из самых незащищенных, в то же время становится самыми активными участниками конфликтов и различного рода экстремистских организаций. Причиной этого выступает то, что они зачастую имеют больше свободного времени, которое проводят именно в информационном пространстве сети Интернет, общаясь в различных социальных сетях, сообществах или играя. При этом сайты, посещаемые подростками, круг общения в сети фактически никем не контролируется, в лучшем случае родители могут поинтересоваться, чем занимается их ребенок. Они и становятся группой риска, склонной к агрессивно-экстремистским действиям. В силу недостаточного жизненного опыта они легко воспринимают искаженное представление о духовных, общечеловеческих ценностях, легко становясь добычей манипуляторов от экстремизма.

¹ © Клочкова Е. Н., 2022.

Развитие информационных технологий размывает границы личной и общественной жизни, увеличивая незащищенность человека. Если говорить о подростке, то в период взросления он всеми силами пытается определить свое место в этом мире, самоутвердиться, часто ищет того, на кого можно было бы ориентироваться. В то же время любые намерения человека в эпоху Интернета легко формируются и усиливаются, потому что в виртуальном мире индивид еще более одинок, чем в реальном. И им очень легко манипулировать. Поэтому на сегодняшний день проблема профилактики экстремизма среди молодежи и подростков наиболее актуальна.

Использование экстремистских ресурсов составляет потенциальную опасность для предрасположенных к совершению насильственных действий людей, особенно подростков. Все эти ресурсы в общем случае могут быть разделены на три обобщенные категории:

- интернет-сайты;
- личные страницы пользователей социальных сетей;
- сообщества в социальных сетях.

В связи с выше представленными категориями противодействие органов внутренних дел интернет-контенту, побуждающему к совершению суицидальных действий, может осуществляться в следующих направлениях: блокировка сайтов с последующим выявлением причастных к публикации лиц, а также ограничение функционирования личных страниц и сообществ экстремистского характера в социальных сетях с последующим выявлением виновных лиц и привлечением их к ответственности.

Количество заблокированных сайтов в России с каждым годом растет. Доступ к деструктивному ресурсу можно запретить не только в судебном порядке, но и без вынесения соответствующего решения.

Блокировка сайта может происходить по одному из двух сценариев: в судебном или досудебном порядке. В последнем случае Роскомнадзор должен получить жалобу, в которой сообщается о наличии на конкретном сайте запрещенной информации. Сначала ведомство проверяет эти сведения и направляет уведомление хостинг-провайдеру. Тот должен потребовать от владельца ресурса удалить запрещенную информацию за три дня. Если спустя указанное время информация продолжает оставаться доступной для интернет-пользователей, то сайт попадает в реестр и блокируется операторами связи.

Проблемой противодействия интернет-контенту экстремистской направленности занимается не только Роскомнадзор, правоохранительные органы тоже ведут активную работу в данном направлении.

Страница несовершеннолетнего в социальных сетях способна рассказать о нем многое. Рассмотрим признаки, на которые необходимо обратить внимание при изучении страницы несовершеннолетнего.

Существует перечень признаков информации, содержащейся на интернет-странице несовершеннолетнего, которые в совокупности сигнализируют о том, что он, возможно, находится в опасности. Среди основного признака можно выделить следующие:

- подросток имеет несколько аккаунтов (от 2 до 5), причем многие из них под псевдонимами [1];
- в качестве имени, под которым подросток зарегистрирован, используются имена лидеров молодежных движений, субкультур;
- анализ групп, в которых зарегистрирован подросток, показывает, что они пропагандируют насилие. Многие из таких групп являются закрытыми для доступа посторонних. При этом обращать внимание необходимо также и на подписки подростка и на тех, кто подписан на данную страницу;
- аватар, который использует подросток, также может показывать склонность к насилию – это аватарки с изображением людей с оружием, лидеров различных молодежных движений, например, Эрика Харриса и т. д.;
- анализ активности молодого человека в сети, позволяет увидеть сколько подросток проводит времени в Интернете, а также определить время суток, когда происходит самое активное общение. Особую настороженность вызывает, когда общение происходит в ночное время [2];
- содержимое страницы пользователя, также может многое рассказать о владельце аккаунта - наличие изображений оружия, призывов к агрессивным действиям, различное видео, содержащее сцены насилия и т. д.;
- отсутствие реальных людей в друзьях при активном аккаунте [3, с. 165].

В заключении необходимо отметить, что решение проблем экстремизма исключительно силами правоохранительных органов невозможно. Решение данной задачи требует комплексного подхода, включающие организационные, правовые, профилактические, воспитательные мероприятия. И в случае выявления у подростка косвенных признаков вовлеченности в деструктивные Интернет-сообщества – необходимо срочно обращаться к специалистам.

Список литературы

1. Экстремизм в подростковой среде: сущность, характерные признаки, ответственность и профилактические меры. URL: <http://киров.78.мвд.рф/document/14465766> (дата обращения: 14.04.2022).
2. Подростки в сети: методика обнаружения потенциальных угроз. URL: <https://vao.mos.ru/counter-terrorism/memo-to-the-population/adolescents-online-the-technique-detects-potential-threats/?ysclid=l1ysknw1p8> (дата обращения: 14.04.2022).
3. Противодействие преступлениям в сфере информационных технологий: учебник / В. В. Гончар и др. М.: Московский университет МВД России имени В.Я. Кикотя, 2021.

Ковригин В. С.¹,

адъюнкт факультета подготовки

научно-педагогических и научных кадров

Московского университета МВД России имени В.Я. Кикотя

ПРИВЕДЕНИЕ В НЕГОДНОСТЬ ОБЪЕКТОВ ЖИЗНЕОБЕСПЕЧЕНИЯ, СОВЕРШЕННОЕ С ИСПОЛЬЗОВАНИЕМ ИТ-ТЕХНОЛОГИЙ

Топливо-энергетический комплекс является одним из важнейших объектов жизнеобеспечения, который занимает ключевое место в обеспечении общественной безопасности не только отдельно взятой личности, но и всего общества и государства в целом, а также вносит значительный вклад в обеспечение национальной безопасности страны. Стоит подчеркнуть, к числу приоритетных направлений государственной политики в области национальной безопасности Российской Федерации [5] относится «обеспечение общественной безопасности, направленное на повышение уровня антитеррористической защищенности объектов жизнеобеспечения населения, топливо-энергетического комплекса, транспортной инфраструктуры, других критически важных и потенциально опасных объектов» (подп. 6 п. 47).

Действующая редакция ст. 215² УК РФ содержит указание в диспозиции нормы на «иной способ приведения в негодность объектов жизнеобеспечения». Наряду с физическим уничтожением и повреждением объектов жизнеобеспечения вполне допустимо отнести к числу иного способа совершения преступления с использованием ЭВМ, при этом объект жизнеобеспечения должен быть приведен в негодное для эксплуатации состояние [1, с. 57]. Этот качественно новый вид способа в области ИТ-технологий, совершенный с использованием современных компьютерных систем. Применительно к ст. 215² УК РФ детальное его рассмотрение в литературе не освещено. В современное время компьютерные технологии активно включаются практически во все сферы человеческой жизни. Поэтому киберпреступность также достигает определенных успехов и наращивает преступные позиции, охватывая также сферу объектов жизнеобеспечения. В качестве иного способа совершения преступления киберпреступность достаточно актуальна, так как целенаправленные хакерские атаки с использованием различных вирусных программ находят свое отражение и в нашей стране. По словам заместителя Секретаря Совета Безопасности Российской Федерации О. В. Храмова число опасных кибератак на критическую инфраструктуру страны в 2018 г. выросло до 17 тыс. [6]. За первое полугодие 2021 г. их количество выросло на 150 % по сравнению с 2020 г. [7].

Данные кибератаки приводят к удалению, блокированию, изменению или иным негативным воздействиям в работе соответствующего оборудования и программного обеспечения, отвечающих за эксплуатацию объектов жизнеобеспечения, создающих различные неисправности в их функционировании, к сбоям,

¹ © Ковригин В. С., 2022.

ведущим к полному или частичному приостановлению деятельности объекта. При этом непосредственно сам объект жизнеобеспечения остается статичным и внешне не изменяется, т. е. целостность объекта не нарушается, качественная сторона объекта не изменяется, но программный сбой, вызванный внешним вмешательством в функционирование объекта, приводит к его непригодности для дальнейшей эксплуатации. Одним из последних резонансных случаев в нашей стране стала хакерская кибератака на объекты жизнеобеспечения, произошедшая в мае 2017 г., когда объектами атаки стали структурные подразделения МВД России, Министерства здравоохранения Российской Федерации, банковской сферы, в результате использования злоумышленниками так называемого вируса «WannaCry» [8], в результате чего была парализована деятельность экстренных служб по всей стране. От распространения вируса «WannaCry» пострадали 74 страны. Некоторые авторы [2, с. 143, 283–285] называют этот вид компьютерной преступности – кибертерроризмом, который обладает не меньшей общественной опасностью по сравнению с «традиционными» способами, помимо всего прочего обладающий своими специфическими особенностями, набирающий обороты не только в нашей стране, но и по всему миру. По официальным данным в 2021 г. зарегистрировано 517 тыс. киберпреступлений, наблюдается сохранение динамики роста исходя, из данных предыдущих лет, к примеру, по сравнению с 2020 г. (510 тыс.) рост составил 1,4 % [9].

Большинство опрошенных респондентов (83 %) признали, что использование способа в области IT-технологий относится к числу иных способов. Действительно, возможность квалификации причинения вреда путем использования вредоносной программы в контексте ст. 167 УК РФ положительно утверждается специалистами [3, с. 191–192], что допускается относить этот способ и к ст. 215² УК РФ, которая является специальной нормой.

Мы солидарны и разделяем данную точку зрения, поскольку в настоящее время наблюдается активное распространение киберпреступности, которые делают все более уязвимыми объекты жизнеобеспечения в части их несанкционированного воздействия в сфере информационной и технологической безопасности, так как, к сожалению, мы идем по пути «отстающего» по причине отсутствия материальных, технических и человеческих (интеллектуальных) ресурсов по повышению безопасности указанных сфер деятельности. Поэтому мнения респондентов являются вполне обоснованными, поскольку совершение преступлений в сфере информационно-коммуникационных технологий весьма распространено и актуально. Хакерские атаки в отношении объектов повышенной опасности – объектов жизнеобеспечения становятся в центре внимания многих государств по всему миру и немалая роль отводится в борьбе с киберпреступностью.

Внимание к вопросам компьютеризированных способов приведения в негодность объекта жизнеобеспечения в научной литературе не уделялось. На наш взгляд, использование IT-технологий при совершении рассматриваемого преступления в действующей редакции необходимо относить к «иному способу приведения в негодность объектов жизнеобеспечения». Общественная опасность

указанного способа очевидна, поскольку виновное лицо не только не проникает на территорию объекта жизнеобеспечения и остается не замеченным, но и в том, что его специальные умения в области информационных технологий приобретают особое свойство – накопление знаний, и по мере их накопления, совершенствования, лицо может одновременно осуществлять преступные посягательства в отношении нескольких объектов жизнеобеспечения, парализовать их работу применительно на территории не только одного, но и нескольких государств, тем самым обретая массовый характер своих действий.

Можно выделить специфические особенности данного способа:

1. Лицо осуществляет преступные действия дистанционно.
2. Лицо осуществляет преступные действия с помощью современных информационных технологий (ИВМ, компьютерные программы).
3. Лицо действует анонимно, то есть физически себя никак не «выдает», в том числе использует различные программы для маскировки (сокрытия) себя в сети Интернет.
4. Установить виновное лицо крайне сложно, поскольку оно может осуществлять преступную деятельность, находясь за пределами территории, где совершается или планируется совершить преступление.
5. Установить местонахождение и анкетные данные виновного лица также проблематично, поскольку зачастую правоохранительные органы не обладают столь значительным финансированием и современными технологиями по сравнению со злоумышленниками.

На повестке дня также лежит вопрос о том, следует ли в таком случае привлекать виновное лицо к уголовной ответственности за незаконное проникновение на объект жизнеобеспечения (по аналогии с охраняемым объектом по ст. 215⁴ УК РФ)? Например, злоумышленник, находясь дистанционно, используя информационные технологии, привел в негодность объект энергетики – ТЭЦ. После чего получил доступ к камерам видеонаблюдения, планам и схемам расположения объекта, информации о сотрудниках, паролях доступов и прочей информации. Частично эти вопросы были затронуты профессором Е. А. Русскевичем [3, с. 195] в своей диссертационной работе. По его мнению, дистанционное «виртуальное вторжение» на охраняемый объект вполне возможно, поскольку проникновение на объект может быть не только открытым или тайным вторжением, но и тогда, когда лицо использует какие-либо предметы без вхождения на объект [4, с. 412]. С данной позицией мы полностью солидарны с автором. В этом вопросе ключевым будет другое – законодательное определение термина «проникновение», а также перечень видов его проявлений. В современное время представляется, что проникновение может быть не только «физическим», но и «виртуальным».

С учетом вышесказанного мы приходим к выводу, что использование в современных условиях широко распространенных и применяемых ИТ-ресурсов вынуждает законодателя идти в ногу со временем, в связи с чем возникла объективная необходимость предусмотреть в качестве отдельного квалифицирующего признака в ст. 215² УК РФ – **совершение преступления с использованием ИТ-**

технологий (информационно-телекоммуникационных технологий), что позволит в полной мере дифференцировать уголовную ответственность за приведение в негодность объектов жизнеобеспечения.

Список литературы

1. Габдрахманов Р. Л. Преступления против общественной безопасности: учебное пособие. М. : Московский университет МВД России имени В.Я. Кикотя, 2003. С. 57.
2. Костенко Н. И. Уголовно-правовые и криминологические проблемы борьбы с компьютерными преступлениями: монография. М. : Юрлитинформ, 2020. С. 143; 283–285.
3. Русскевич Е. А. Дифференциация ответственности за преступления, совершаемые с использованием информационно-коммуникационных технологий, и проблемы их квалификации: дис. ... докт. юрид. наук. Москва, 2020. С. 191–192; 195.
4. Уголовное право России: учебник в 2 т. Т. 2: Особенная часть / под ред. Н. Г. Кадникова. М., 2018. С. 412.
5. Указ Президента Российской Федерации от 02 июля 2021 г. № 400 «О стратегии национальной безопасности Российской Федерации» // СПС «КонсультантПлюс».
6. Официальный сайт Совета Безопасности Российской Федерации // [Электронный ресурс] // URL: <http://www.scrf.gov.ru/news/allnews/2629/> (дата обращения: 30.03.2021).
7. Официальный сайт Научно-технического центра ФГУП «ГРЧЦ» // [Электронный ресурс] // URL: https://rdc.grfc.ru/2021/07/kiberataki_na_kii/ (дата обращения: 01.03.2022).
8. Официальный сайт Лаборатории Касперского // [Электронный ресурс] // URL: <https://www.kaspersky.ru/blog/wannacry-ransomware/16147/> (дата обращения: 28.11.2021).
9. Официальный сайт МВД России // [Электронный ресурс] // URL: <https://мвд.рф/reports/item/28021552/> (дата обращения: 01.03.2022).

Карпика А. Г.¹,

*доцент кафедры информационного обеспечения ОВД
Ростовского юридического института МВД России,
кандидат технических наук, доцент*

Лемайкина С. В.²,

*начальник кафедры информационного обеспечения ОВД
Ростовского юридического института МВД России*

АКТУАЛЬНЫЕ ВОПРОСЫ ЗАЩИТЫ КОМПЬЮТЕРНЫХ СЕТЕЙ В УСЛОВИЯХ СКООРДИНИРОВАННЫХ АТАК

Атака типа «отказ в обслуживании» позволяет киберпреступнику «занять» компьютерную сеть или сервер поддельным трафиком. Слишком большой трафик перегружает ресурсы и нарушает связь, мешая системе обрабатывать подлинные запросы пользователей. Сетевой ресурс становится недоступным, его владелец несет финансовые и репутационные издержки. В случае, если ресурс имеет отношение к объекту критической инфраструктуры, возникает риск появления уязвимости, чувствительной для функционирования подобного объекта.

Для организации атаки злоумышленники обычно используют сеть предварительно зараженных сетевых устройств – «ботов», так называемую «ботнет». Основная цель использования этих «зомби-устройств» – отправка чрезмерного количества запросов на целевой веб-сайт или IP-адрес сервера. Как только ботнет отправляет достаточно запросов, онлайн-сервисы (электронная почта, веб-сайты, веб-приложения и т. д.) замедляются или выходят из строя.

Согласно отчету Radware [1] средняя продолжительность DDoS-атаки следующая: 33 % атак держат сервисы недоступными в течение часа, 60 % длятся менее полного дня, 15 % хватает на месяц. Хотя DDoS обычно не приводит напрямую к утечке или утечке данных, жертва тратит время и деньги на восстановление доступа к услугам.

Типы DDoS-атак. Несмотря на то, что все DDoS-атаки направлены на то, чтобы перегрузить систему слишком большой активностью, злоумышленники используют различные стратегии с целью вызвать распределенный отказ в обслуживании. Три основных типа атаки: атаки прикладного уровня, протокольные атаки, объемные атаки. Эти три подхода основаны на разных методах, но опытный хакер может использовать все три стратегии для достижения одной цели.

Атаки прикладного уровня. Атака на уровне приложений нацелена на конкретное приложение, а не на всю сеть, и нарушает его работу. Хакер генерирует большое количество HTTP-запросов, которые исчерпывают способность целевого сервера отвечать. Специалисты по кибербезопасности измеряют атаки на уровне приложений количеством запросов в секунду (RPS). Общие цели этих атак включают в себя: веб-приложения, приложения, подключенные к сети Интернет, облачные сервисы.

¹ © Карпика А. Г., 2022.

² © Лемайкина С. А., 2022.

Попытка предотвратить DDoS-атаки этого типа является сложной задачей, поскольку службы безопасности часто пытаются отличить законные HTTP-запросы от вредоносных. Эти атаки используют меньше ресурсов, чем другие стратегии DDoS, и некоторые злоумышленники могут даже использовать только одно устройство для организации атаки на уровне приложений.

Протокольные атаки. Протокольные DDoS-атаки (или атаки на сетевом уровне) используют уязвимости в протоколах или процедурах, управляющих интернет-коммуникациями. В то время как DDoS на уровне приложения нацелен на конкретное приложение, целью атаки на протокол является замедление всей сети. Двумя наиболее распространенными типами DDoS-атак на основе протоколов являются: «SYN-флуд» (одна из разновидностей сетевых атак типа отказ от обслуживания, которая заключается в отправке большого количества SYN-запросов (запросов на подключение по протоколу TCP) в достаточно короткий срок.

Злоумышленник отправляет TCP-запросы с поддельными IP-адресами цели. Целевая система отвечает и ждет, пока отправитель подтвердит рукопожатие. Поскольку злоумышленник никогда не отправляет ответ для завершения рукопожатия, незавершенные процессы накапливаются и в конечном итоге приводят к сбою сервера.

«Smurf DDoS»: хакер использует вредоносное ПО для создания сетевого пакета, прикрепленного к ложному IP-адресу (спуфинг). Пакет содержит сообщение проверки связи ICMP, которое просит сеть отправить ответ. Хакер отправляет ответы (эхо) обратно на сетевой IP-адрес снова, создавая бесконечный цикл, который в конечном итоге приводит к сбою системы.

Эксперты по кибербезопасности измеряют количество атак на протоколы в пакетах в секунду (PPS) или битах в секунду (BPS). Основная причина, по которой они так широко распространены, заключается в том, что эти атаки могут легко обходить плохо настроенные брандмауэры.

Объемные атаки. DDoS-атака на основе объема потребляет доступную пропускную способность цели посредством ложных запросов данных и создает перегрузку сети. Трафик злоумышленника блокирует доступ законных пользователей к службам, предотвращая входящий и исходящий трафик. Все объемные атаки основаны на ботнетах. Объемные атаки являются наиболее распространенным типом DDoS.

Определим наиболее целесообразные меры противодействия подобного вида атакам, которые должны носить превентивный характер.

Разработка плана реагирования на DDoS-атаки. План реагирования на инциденты обеспечивает быстрое и эффективное реагирование сотрудников в случае DDoS. Этот план должен содержать:

- четкие пошаговые инструкции о том, как реагировать на DDoS-атаку;
- как сохранить операционную устойчивость организации;
- задачи сотрудников и ключевых заинтересованных сторон;
- протоколы эскалации (возможного развития событий);
- обязанности службы сетевой безопасности;

- контрольный список всех необходимых программно-аппаратных инструментов;
- перечень критически важных систем.

Способность реагировать на непредвиденные события жизненно важна для обеспечения непрерывности деятельности организации. Безопасность сетевой инфраструктуры необходима для предотвращения любой попытки DDoS-атаки. Поскольку атака имеет значение только в том случае, если у злоумышленника достаточно времени для накопления запросов, способность идентифицировать DDoS на ранней стадии имеет важное значение для контроля радиуса поражения.

Для противодействия атаке целесообразно комплексно использовать все имеющиеся средства сетевой безопасности:

- брандмауэры и системы обнаружения вторжений, которые действуют как барьеры для сканирования трафика между сетями;
- антивирусное и антивредоносное программное обеспечение, которое обнаруживает и удаляет вирусы и вредоносные программы;
- защита оконечных устройств, которая гарантирует, что устройства сети (настольные компьютеры, ноутбуки, мобильные устройства и т. д.) не станут точкой входа для вредоносных воздействий;
- инструменты веб-безопасности, которые удаляют веб-угрозы, блокируют аномальный трафик и ищут известные сигнатуры атак;
- инструменты, которые предотвращают спуфинг, проверяя, имеет ли трафик исходный адрес, соответствующий исходным адресам;
- сегментация сети, которая разделяет системы на подсети с уникальными средствами контроля безопасности и протоколами.

Защита от DDoS-атак также требует высокого уровня безопасности сетевой инфраструктуры. Защита сетевых устройств позволяет подготовить оборудование (маршрутизаторы, балансировщики нагрузки, системы доменных имен (DNS) и т. д.) к скачкам трафика.

Избыточность серверного оборудования в виде нескольких распределенных серверов затрудняет злоумышленнику осуществление атаки на все серверы одновременно. Если злоумышленник запускает успешную DDoS-атаку на одном устройстве, другие серверы остаются незатронутыми и получают дополнительный трафик до тех пор, пока целевая система не вернется в сеть.

К общим признакам наличия DDoS атаки следует отнести: ухудшение связи, снижение производительности, необычно высокое количество обращений на одну страницу или конечную точку, сбои обработки запросов пользователей, необычный трафик, поступающий с одного или небольшой группы IP-адресов, всплеск трафика от пользователей с общим профилем (модель системы, геолокация, версия веб-браузера и т. д.).

Мощность атаки так же может варьироваться от маломасштабной до полномасштабной. Маломасштабные атаки могут быть проверкой или отвлечением для более опасного нарушения (например, программы-вымогателя). Таким образом, обнаружение подобной атаки так же важно, как и определение полномасштабной DDoS.

Эксперты прогнозируют, что к 2023 г. среднее количество ежегодных попыток DDoS вырастет до 15,4 млн. Это число указывает на то, что почти каждая организация рано или поздно столкнется с DDoS атакой, поэтому подготовка к этому типу атаки должна осуществляться в виде стандартной процедуры обеспечения безопасности инфраструктуры организации.

Список литературы

1. Отчет Radware: Оценка ситуации в сфере кибербезопасности веб-приложений [Электронный ресурс] URL: <https://radware.pro/downloads/FINAL-2019-WAS-Research.pdf>. (дата обращения: 10.04.2022).

Гасимова С. А.¹,
студентка КФ ФГБОУВО
«Российский государственный
университет правосудия»

Научный руководитель:
Шевко Н. Р.,
доцент кафедры уголовно-правовых дисциплин
КФ ФГБОУВО «Российский государственный
университет правосудия»,
кандидат экономических наук, доцент

ТЕРРОРИЗМ И ЭКСТРЕМИЗМ В КИБЕРПРОСТРАНСТВЕ: СОСТОЯНИЕ И ВОПРОСЫ ПРОТИВОДЕЙСТВИЯ

Использование Интернета в террористических и экстремистских целях относится к быстро развивающимся противоправным явлениям, которые требуют принятия активных и согласованных ответных мер со стороны государства. По официальным статистическим данным в России в 2021 г. число осужденных за экстремизм выросло до 606 человек. За терроризм в 2021 г. в России было осуждено 682 человека против 575 годом ранее. За преступления экстремистской направленности количество осужденных за это время выросло с 325 до 606 человек [1].

По информации МВД России, преступлений экстремистской направленности за 2021 г. было зарегистрировано 1057, это на 27 % больше, чем в 2020 г. В большей степени их раскрывали сотрудники Министерства внутренних дел Российской Федерации (567 преступлений, рост на 13 %). Благодаря работе сотрудников ФСБ России произошел двойной прирост выявленных преступлений (437 преступлений, рост на 48,6 %). Как выяснилось, на первом месте по преступлениям экстремистской направленности оказалась Москва – более 59 преступлений, на втором месте – Дагестан (58 преступлений), на третьем – Кемеровская область (54 преступления) [2]. Большинство из них совершаются с помощью интернет-пространства (если не как инструмента, то как вспомогательного оружия).

Актуальной проблемой стал рост религиозного экстремизма и терроризма. Это серьезная угроза стабильности общества и национальной безопасности России, как многонационального государства. Данные явления оказывают существенное негативное влияние как на экономику и авторитет страны на международной арене, так и на геополитическое положение.

В этой связи перед государством стоит архиважная задача – формирование системы противодействия идеологии терроризма. Это не просто направление деятельности, не принятие каких-то конкретных отдельно взятых решений по борьбе с данным видом преступлений, а единая целая система, способная эффек-

¹ © Гасимова С. А., 2022.

тивно противодействовать совершению террористических актов, оперативно реагировать на выявление, расследование, раскрытие и пресечение таких деяний, имеющая правовую основу на законодательном уровне. Кроме того, эта система должна регулировать деятельность по предупреждению и профилактике терроризма.

Данные официальной статистики [1] свидетельствуют о периодическом росте преступлений и террористического, и экстремистского характера. В Российской Федерации с 2011 г. число лиц, совершивших террористические преступления выросло более, чем в два раза (2011 г. – 377 человек, 2021 г. – 865 человек). Причем число преступлений выросло более, чем втрое (2136 в 2021 г. против 622 в 2011 г.). Почти половина всех преступлений остается пока нераскрытой (в 2020 г. – 60 %, в 2021 г. – 45,5 %), что, конечно, является недопустимым.

По экстремистским проявлениям ситуация немного лучше. На фоне роста числа преступлений экстремистского характера и лиц, их совершивших (в 2011 г. 622 преступления, 480 преступников, в 2020 г. 833 преступления, 664 преступника, в 2021 г. уже 1057 преступлений и 925 преступников) наблюдается положительная тенденция раскрываемости. С 84 % в 2011 г. раскрываемость выросла до 89 % в 2020 г. и 95 % в 2021 г. Эти показатели, бесспорно, внушают надежду и усиливают чувство защищенности человека и гражданина.

Кроме того, негативно влияет на национальную безопасность информация, распространяемая через всемирную паутину – сеть Интернет, особенно если она сеет панику, распространяет «фейковые» новости, призывает к насилию, пропагандирует геноцид. К сожалению, сегодня это стало реальностью, мы стали свидетелями таких фактов. Многие сайты и провайдеры, распространяющие подобную информацию, были оперативно заблокированы российскими спецслужбами. Иначе последствия могли бы быть необратимыми.

Лучшее противодействие преступности – это ее предупреждение. Профилактика является неотъемлемой составляющей борьбы с преступностью. Особенно в молодежной среде. Здесь, как минимум, две причины. Во-первых, именно подрастающее поколение активно использует гаджеты и информационные ресурсы интернет-пространства в своей повседневной жизни. Во-вторых, именно молодежь подвержена психологическому воздействию, так как имеет еще не сформировавшееся мировоззрение. В связи с этим видится необходимым осуществление ряда мер в целях снижения радикальных проявлений в молодежной среде. Прежде всего, это организация досуга – от строительства и открытия досуговых центров, выставок, социально-культурных учреждений, льготных билетов на культурно-массовые мероприятия, в фитнес-клубы до пропаганды здорового образа жизни, чтобы отказ от вредных привычек стал не просто нормой, но и модным течением. Затем повышение правового сознания, правовой культуры молодежи. Ведь знание закона, своих прав и свобод, обязанностей способствует проявлениям чувства уважения к правам и свободам других. И, конечно же, воспитание толерантности, уважения и терпимого отношения к интересам других лю-

дей. Ну, и конечно, повышение уровня защищенности (социальной, материальной, информационной, правовой и т. д.) молодежи и подростков. То есть необходим всесторонний, комплексный подход для решения этих проблем.

Список литературы

1. Портал правовой статистики. http://crimestat.ru/offenses_chart (дата обращения: 20.03.2022).
2. Российский интернет-портал и аналитическое агентство TAdviser. <https://www.tadviser.ru/index.php> (дата обращения: 10.04.2022).

Гречков В. А.¹,

курсант факультета подготовки сотрудников

для оперативных подразделений полиции

Московского университета МВД России имени В.Я. Кикотя

Научный руководитель:

Гончар В. В.,

начальник кафедры информационной безопасности

учебно-научного комплекса информационных технологий

Московского университета МВД России имени В.Я. Кикотя,

кандидат юридических наук, доцент

ИТ-ТЕХНОЛОГИИ БОРЬБЫ С ФЕЙКОВЫМИ НОВОСТЯМИ В СЕТИ ИНТЕРНЕТ

Рост числа фейковых новостей и спланированных кампаний по дезинформации в сети Интернет не только наносит ущерб экономике конкретных предприятий и является источником репутационных потерь для граждан, но может и в целом повлиять на политическую стабильность общества. Именно поэтому на состоявшемся 20–24 января 2020 г. Всемирном экономическом форуме (ВЭФ), более известном, как Давосский форум, «манипуляции через фейк-ньюс» были в числе главных опасностей, с которыми мир может столкнуться в середине 2020-х гг. [1].

Анализируя мировой опыт борьбы с фейковыми новостями, можно выделить три основные группы методов противодействия распространению дезинформации в сети Интернет:

1. Юридические методы (криминализация процесса распространения фейковых новостей, запретительные и ограничительные меры в отношении распространителей фейков и т. п.).

2. Организационные методы (фактчекинг, проекты медиа-грамотности по выявлению фейков и т. п.).

3. Технологические методы (использование ИТ-технологий для непосредственно выявления и блокировки фейковых новостей).

Рассмотрим более подробно российский и зарубежный опыт использования технологических методов борьбы с фейковыми новостями.

В этой связи наиболее успешно себя зарекомендовали системы искусственного интеллекта, в частности, технология машинного обучения.

Машинное обучение (от англ. «machine learning») – это «класс методов искусственного интеллекта, характерной чертой которых является не прямое решение задачи, а обучение в процессе применения решений множества сходных задач». К таким методам относятся методы оптимизации, семантический анализ, графовый анализ, а также различные техники работы с данными в цифровой форме.

В качестве источника для семантического анализа новости принимаются следующие критерии:

¹ © Гречков В. А., 2022.

- оригинальность URL-адреса опубликованной новости на соответствие домену искомого сайта, так как сайты-двойники могут целиком имитировать крупные онлайн-издания;
- дата публикации материала, поскольку фейковые новости, как правило, не датированы;
- наличие грамматических и пунктуационных ошибок в тексте;
- наличие внутренней согласованности анализируемой статьи, поскольку поддельные новости часто имеют большую несогласованность между различными частями текста;
- наличие совпадений фрагментов разных статей, например, основная статья, вышедшая на авторитетном ресурсе, копируется полностью или переписывается с внесением в нее ложных фактов;
- наличие ссылок в материале: статья будет поддельной, если она сама ссылается на фейковую новость;
- наличие сигнальных (сенсационных) слов – новости, которые содержат в своих заголовках и ключевых словах привлекающие внимание утверждения, часто могут быть фейковыми.

Механизм машинного обучения с использованием семантического анализа таков, что для каждого сообщения предполагается некоторая зависимость между объектами (значением критерия) и ответами (фейковое или истинное сообщение). При этом имеется совокупность прецедентов (пар «объект, ответ»), называемая обучающей выборкой (в данном случае из сообщений). На основе этих данных производится восстановление неявной зависимости, то есть алгоритма, способного для любого возможного входного объекта (сообщения) выдать достаточно точный классифицирующий ответ (фейк или правда).

Например, учеными ФИЦ «Информатика и управление» РАН и МГУ имени М.В. Ломоносова была разработана методика глубинного анализа текста в виде системы динамической контентной фильтрации. Суть метода состоит в том, что из выборки текстов, включающей десятки тысяч образцов с помощью морфологического, синтаксического и семантического методов анализа выделяются специфические слова, словосочетания и фразы, которые позволяют сформулировать множество классификационных признаков, характеризующих текст, как фейковый.

Далее полученные данные используются при обучении различных моделей классификаторов для динамической контентной фильтрации. Они включают в себя системы на основе нейронных сетей и математических методов определения тематической значимости.

Данная методика дает возможность проведения глубокого мониторинга социальных сетей, который осуществляется при помощи специальных ботов (или краулеров), целью которых является непрерывный серфинг по ресурсам Интернета для выявления содержащих фейки аккаунтов, пользовательских групп, а также объявлений и комментариев к ним.

Эффективность данной методики достигает 98 % и позволяет выявлять фейки до десяти раз быстрее, чем автоматический поиск через традиционные системы Яндекс или Google [2].

Схожая отечественная методика с использованием машинного обучения принадлежит Евгению Венедиктову, она называется «Демон Лапласа» и представляет собой автоматизированную систему круглосуточного мониторинга и сбора данных из сети Интернет. Система «Демон Лапласа» позволяет получать и анализировать широкий спектр информации из микроблогов «Twitter», социальных сетей «Facebook» и «VKontakte», персональных блогов «Живого журнала», а также из онлайн-СМИ.

К зарубежным разработкам на основе машинного обучения можно отнести такие как FakeBox, FightHoax, TrulyMedia, SocialTruth и др. Их суть также сводится к поиску признаков специфического стиля написания, сенсационных заголовков и пр.

Согласно результатам проведенного в 2019 г. соревнования по выявлению дезинформации в Интернете, наиболее эффективной для идентификации медиафейков стала модель ELMo. Данная технология может продуцировать бесконечное число вариантов для одного слова, что позволяет учитывать контекст употребления слова не только в конкретном анализируемом тексте, но и во всей выборке [3, с. 22].

Наряду с этим для поиска источника фейковых сообщений в социальных сетях применяется графовый анализ, при котором распространение каждого сообщения в сети представляется множеством графов, у которых вершины – это пользователи, а ребра – связи между ними. Изначально не существует жестко заданной модели данных, и связь нового типа добавляется в процессе каждой пересылки сообщения.

Например, 2 марта 2020 г. специалисты российской компании Group-IB, работающей в сфере детектирования и предотвращения кибератак, при помощи метода графового анализа выявили исполнителей информационного вброса в социальные сети о якобы имеющей место мощной вспышке коронавируса в Москве: за день было зафиксировано более 9500 постов, репостов и публикаций этой новости.

Также стоит отметить, что в июле 2019 г. ученые из лаборатории IBM-Watson Массачусетского технологического института, представили искусственный интеллект, который умеет определять тексты, написанные другим искусственным интеллектом. Инструмент называется Giant Language Model Test Room (GLTR), он тестирует тексты на предсказуемость. Программа не полагается на знание языка, она ищет закономерности в структуре предложений. В связи с тем, что любой искусственный интеллект создает тексты на основе некоего алгоритма, то фактически GLTR определяет этот алгоритм и показывает, что человек не мог структурировать текст таким образом.

Особое внимание стоит обратить на применение глубоких нейронных сетей в борьбе с фейковыми новостями. Такие сети похожи на обычные, но при этом

состоят из множества слоев. Например, рекуррентные нейросети могут динамически меняться и способны запоминать новую семантическую и лексическую информацию. Иерархические сети внимания (HAN) способны фиксировать определенные характеристики структуры документа. Они выстраивают репрезентации предложений и на их основе формируют репрезентацию всего документа.

Применение технологий поиска фейковых новостей с применением машинного обучения в зарубежных странах облегчается наличием баз данных с размеченными фейковыми и реальными новостями. Большой объем выборки повышает точность работы классификаторов вне зависимости от применяемого метода машинного обучения. К таким общедоступным наборам данных можно отнести базу фейковых новостей «Kaggle», перечень сайтов, публикующих фейковые новости «BuzzFeed», сборники фейковых и реальных новостей «Kaidmml» и «LIAR».

Тем не менее российские антифейковые разработки на основе систем машинного обучения также являются весьма перспективными и конкурентоспособными.

Стоит отметить, что революционное развитие систем искусственного интеллекта двояко влияет на проблему фейковых новостей. С одной стороны, совершенствуются механизмы борьбы с фейками, а с другой, технологии искусственного интеллекта активно используются для генерации и распространения ложного контента. Если изначально фейковые новости распространялись только в виде текстовой информации, то сейчас технологии позволяют создавать поддельные аудио- и видеоизображения, которые получили название глубоких фейков (от англ. «deepfake»).

Как известно, в конце мая 2020 г. после успешного запуска компанией Space X пилотируемого корабля Crew Dragon в Интернете стало вирусным видео, на котором Илон Маск поет песню «Трава у дома», где при помощи Deepfake-технологии изображение лица владельца компании Space X соединили с исходной записью концерта группы «Земляне».

Таким образом, технология Deepfake представляет собой «совокупность технологий искусственного синтеза человеческого изображения и голоса, основанных на использовании нейросетей и искусственного интеллекта, позволяющие создавать высокореалистичные фото- и видеоизображения людей либо производить модификацию фото-, аудио- и видеоматериалов».

Данная технология представляет достаточно высокую опасность, так как deepfake-контент весьма реалистичен и зачастую без проведения соответствующего анализа распознать его практически невозможно. Не зря в августе 2019 г. Управление перспективных исследовательских проектов Министерства обороны США (DARPA) в рамках программы «SemaFor» («Семантическая экспертиза»), начала разработку технологий, способных автоматически распознавать сфабрикованный мультимедийный контент – текст, звук, изображение и видео – для защиты от широкомасштабных автоматизированных компаний по дезинформации.

Использование искусственного интеллекта для борьбы с deepfake-контентом осуществляется при помощи так называемого глубинного обучения. Оно применяет некоторые методы машинного обучения для решения реальных задач, используя нейронные сети, которые могут имитировать принятие решений человеком.

Например, в июне 2018 г. ученые в области компьютерных технологий из Политехнического университета в Олбани (SUNY Albany) создали программы выявления глубоких фейков на основе наблюдения за аномальными моделями движения глазного века, когда персонаж на видео моргает. В основе метода лежит сверточная и рекуррентная нейросеть. Алгоритм распознает лица и анализирует частоту морганий, основываясь на предыдущих состояниях кадра. Первая часть алгоритма анализирует открыты или закрыты глаза в текущий момент, а вторая сравнивает результат с предыдущими изображениями.

Другим технологическим методом противодействия глубоким фейкам является технология маркировки контента специальным идентификационным водяным знаком до начала его распространения. На Западе такой подход именуется «концепцией цифрового происхождения» («digital provenance» solution). Компании, такие как «Труэпик» (Truepic), развивают технологии нанесения цифрового водяного знака для аудио-, фото- и видеоконтента в момент его создания, используя метаданные, которые могут быть неизменно зарегистрированы в доступном регистре или блокчейне для последующего сравнения с возможным фейком.

Таким образом, искусственный интеллект является технологией, применяемой как для создания глубоких фейков, так и для борьбы с ними.

Также среди технологических методов борьбы с фейковыми новостями следует выделить блокчейн-технологии, особенностью которой является возможность достоверной идентификации источника новости.

Технология блокчейн (от английских слов «block» – блок и «chain» – последовательность, цепочка) представляет собой полностью реплицированную распределенную базу (реестр) данных, в которой информация упорядочена по определенным правилам в виде цепочки блоков данных. При этом выполняются два условия: каждый блок данных связан с предыдущим и новые блоки добавляются исключительно в конец цепочки.

Авторство блокчейн-технологии приписывается Сатоши Накамото (это псевдоним человека или группы людей), который 31 октября 2008 г. опубликовал статью «Bitcoin: A Peer-to-Peer Electronic Cash System». Именно с создания первой криптовалютной платежной системы Биткойн (от английских слов «bit» – бит, т. е. единица измерения информации, и «coin» – монета) технология блокчейн получила свое широкое распространение.

По сути, в базе данных, работающей по технологии блокчейн, может храниться что угодно – информация о банковских услугах, сделках, денежных транзакциях и т. п. Неоспоримым ее преимуществом является распределенность, т. е. эта база хранится не на одном компьютере, а на разных, где обычно размещается

полная копия всех блоков, что практически исключает возможность самопроизвольной замены какого-либо блока. Для этого потребовалось бы подменить информацию на всех компьютерах сети.

Рассмотрим несколько примеров применения технологии блокчейн в мировой практике борьбы с фейковыми новостями.

Во-первых, это блокчейн-проект The Civil Media, который позволяет подтвердить авторство и права владения контентом. При помощи смарт-контрактов проекта Civil можно отследить контент в сети, его автора и дальнейшее продвижение. Это, с одной стороны, помогает редакциям и журналистам в пресечении незаконного перепечатывания их материалов, а с другой, пользователи защищены, так как знают к кому предъявлять претензии, если контент оказался фейковым или заказными [3].

В конце 2018 г. блокчейн-проект The Civil Media и агентство Associated Press договорились о сотрудничестве, в рамках которого новости и статьи Associated Press должны появляться в ньюсруме Civil. А в середине 2019 г. The New York Times (второе по величине издание в США), подтвердило свое намерение использовать блокчейн для борьбы с поддельной информацией [4].

Вторым примером использования блокчейна для борьбы с фейками является более молодая блокчейн-платформа Po.et (от англ. «proof of existence» – «доказательство существования»), позволяющая регистрировать любой фрагмент цифрового контента, чтобы впоследствии можно было доказать, где и когда он появился, и кто его создал. Po.et без проблем интегрируется с такими известными системами управления контентом, как WordPress, Drupal и Joomla, и имеет собственное мобильное приложение.

Третьим успешным примером использования блокчейн технологии является расширение Trusted News для популярного блокировщика нежелательной рекламы Adblock Plus. Данное расширение оценивает целостность и надежность источников онлайн-новостей и помечает контент как «надежный», «неизвестный», «кликбейт», «сатира», «пользовательский» либо «вредоносный». Таким образом, пользователь имеет возможность самостоятельно решить насколько доверять той или иной новости [4].

Расширение Trusted News использует протокол MetaCert, который поддерживает реестр надежных URL-адресов. Эти данные располагаются на блокчейн Ethereum, а токены MetaCert используются, как защита от манипуляций [5].

Другим весьма успешным и наиболее передовым является блокчейн-решение Hyperledger Fabric. С его помощью американская ежедневная газета New York Times анализирует на предмет подлинности фотоснимки, поступающие в издательство с мест инцидентов, а также хранит на платформе данные в электронном формате о всех файлах, даже когда они были отредактированы [6].

Также вызывает интерес и не совсем обычный блокчейн-инструмент, позволяющий бороться с новостными фейками – платформа Dirt Protocol. Ее необычность в том, что она основана на принципе геймификации (от английского «gamification» – процесс использования игрового мышления и динамики игр для вовлечения аудитории и решения задач). Суть в том, что платформа Dirt Protocol

борется не столько с авторами фейков, сколько с людьми, которые способствуют их распространению. За распространение правдивого контента пользователь получает финансовое стимулирование, а в случае распространения фейка – штраф. Такая система весьма затрудняет работу интернет-троллей и людей, намеренно распространяющих кликбейтовый контент для накрутки «лайков». Хранение информации с использованием блокчейна существенно повышает надежность такой платформы, а децентрализованная система проверки пользователей дает возможность установить правдивость контента [7, с. 201].

Таким образом, блокчейн-технология позволяет эффективно бороться с распространением фейковых новостей, она гораздо менее затратная и более масштабируемая. Из минусов можно отметить то, что блокчейн существенно уменьшает вероятность, но не полностью исключает проникновение ложной информации в Интернет, так как в основном ориентирован не на саму новость, а на источник ее появления.

Подводя итог, можно отметить, что неоспоримыми преимуществами технологических методов борьбы с фейковыми новостями в сети Интернет являются:

- возможность массовой автоматизированной обработки новостей;
- высокая скорость проведения проверки;
- возможность проверки поддельного фото-, аудио- и видеоконтента;
- относительно низкая трудоемкость проведения проверки;
- относительно легкая масштабируемость IT-решений;
- к слабым сторонам технологических методов можно отнести:
- уязвимость любых IT-решений от несанкционированного доступа;
- развитие технологий производства фейкового контента, способных преодолеть фильтры соответствующих анти-фейковых механизмов;
- невозможность выявить сложные (скрытые) фейки.

Таким образом, технологические методы борьбы с фейковыми новостями в сети Интернет являются однозначно перспективным направлением, но также не лишены недостатков.

Список литературы

1. Баловсяк Н. Блокчейн-стартап Dirt Protocol будет бороться с фейковыми новостями. Электронный ресурс: <https://bloomchain.ru/newsfeed/blokchejn-startap-dirt-protocol-budet-borotsya-s-fejkovymi-novostyami/>.
2. Бондарчук Н. The New York Times использует блокчейн для борьбы с поддельными новостями. Электронный ресурс: <https://bits.media/the-new-york-times-ispolzuet-blokcheyn-dlya-borby-s-poddelnymi-novostyami/>.
3. Буланов А. Тест на контекст: фейки в соцсетях зафиксированы в 10 раз быстрее // Газета «Известия» от 14.04.2020. Электронный ресурс: <https://iz.ru/999322/aleksandr-bulanov/test-na-kontekst-feiki-v-sotcsetiakh-zafiksi-ruiut-v-10-raz-bystree>.
4. Воробьева А. В New York Times задействуют для борьбы с фейками блокчейн-решение Hyperledger Fabric. Электронный ресурс: <https://cryptofeed.ru/uncategorized/v-new-york-times-zadejstvujut-dlya-borby-s-fejkami-blokchejn-reshenie-hyperledger-fabric/>.

5. Гриценко Е. Искусственный интеллект научился определять фейки, созданные другим искусственным интеллектом. Электронный ресурс: <https://www.digger.ru/news/iskusstvennyj-intellekt-nauchilsya-opredelyat-fejki-sozdannye-drugim-iskusstvennym-intellektom>.

6. Деместихас К., Ремунду К., Адамопулу Е. Как бороться с фейками в Сети // Открытые системы. СУБД. 2020. № 02. Электронный ресурс: <https://www.osp.ru/os/2020/02/13055463>.

7. Противодействие преступлениям в сфере информационных технологий: учебник / В. В. Гончар и др. М. : Московский университет МВД России имени В.Я. Кикотя, 2021.

Дворянова Н. Е.¹,

курсант факультета подготовки специалистов

в области информационной безопасности

Московского университета МВД России имени В.Я. Кикотя

Научный руководитель:

Клочкова Е. Н.,

доцент кафедры специальных информационных технологий

учебно-научного комплекса информационных технологий

Московского университета МВД России имени В.Я. Кикотя

ПРОФИЛАКТИКА ИДЕЙ ТЕРРОРИЗМА И ЭКСТРЕМИЗМА В МОЛОДЕЖНОЙ СРЕДЕ С ИСПОЛЬЗОВАНИЕМ ВОЗМОЖНОСТЕЙ СЕТИ ИНТЕРНЕТ

В соответствии с Федеральным законом «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.

Актуальность противодействия идеологии экстремизма и терроризма является бесспорной. В России проводится политика по совершенствованию нормативно-правовой базы, которая направлена на профилактику и предупреждение идеологии терроризма в сети Интернет. В особенности важна профилактика среди молодежи, так как, к сожалению, зачастую подростки подвержены деструктивному влиянию со стороны террористических организаций и их пропаганды.

На основании портала правовой статистики Генеральной прокуратуры Российской Федерации, всего лишь за период с января по февраль в 2022 г. в Российской Федерации преступлений террористического характера зарегистрировано 302, а выявлено лиц, которые совершили данные преступления, – 117 [1].

Согласно народной мудрости, которая утверждает, что «если есть необходимость выиграть бой, то, прежде всего, следует заняться воспитанием детей», – выработав механизм, который способен решить проблему противодействия распространений террористических и экстремистских убеждений среди молодого населения в глобальной сети Интернет, а также утверждение средств и методов борьбы, вышеуказанное утверждение носит значительный смысл.

Важным решением вопросов по противодействию деструктивной идеологии терроризма и экстремизма служит усовершенствование образовательного, а также воспитательного процессов. Это можно объяснить тем, что молодые люди, молодежь, ученики – это то население, которое больше всего подвергается влиянию и воздействию тех или иных идеологий, в данном случае идеологиям терроризма и экстремизма [2].

¹ © Дворянова Н. Е., 2022.

С помощью развития приверженности к организациям, осуществляющим экстремистскую и террористическую деятельность, руководители данных групп способны привлекать молодежь в свои круги. Целью служит проведение мероприятий с указанной направленностью, среда совершения – глобальная сеть Интернет.

Существует огромное количество факторов, способствующих тому, что молодежь подвергается разрушительному давлению со стороны экстремистских и террористических идеологий. Экономическая и политическая ситуация в стране и в мире сильно влияет на все слои населения. Молодежь в данном случае не является исключением, наоборот, молодые люди наиболее подвержены восприятию различного рода идеологий и мировоззрений в силу различных факторов. Как правило, у молодежи зачастую отсутствуют четко сформированные жизненные убеждения, собственное мнение, а также система ценностей. Молодые люди часто готовы к конфликтам, излишне эмоциональны при принятии решений и не способны осознать последствия своих необдуманных поступков. Из-за отсутствия жизненного опыта они убеждены в собственных представлениях о справедливости [3].

В связи с вышеперечисленными особенностями молодых людей, террористы дают им обещание быстрого и эффективного решения денежного нехватка, после их согласия предоставляя ресурсы для быстрого заработка на своей деструктивной деятельности.

Именно поэтому необходима система создания специальных сайтов, которая могла бы противодействовать идеологии терроризма в сети Интернет в молодежной среде.

Глобальная сеть Интернет эксплуатируется террористами для расширения собственных идей и убеждений, а также распространения пропаганды или обмена информацией. Подавляющее большинство международных террористических группировок распространяют свои понятия и мысли на всевозможных веб-ресурсах с целью пропаганды. В Интернете широко распространены акции, направленные, в частности, на молодое поколение, поскольку именно эта категория людей особенно восприимчива и может свободно поддаться влиянию той или иной идеологии [4, с. 145].

К примеру, можно привести заманивание молодых людей под знамена ИГИЛа, одурманивание молодежи через различных популярных блогеров (типа А. Навального) и др. Для достижения этих целей используются специалисты, владеющие навыками по несанкционированному доступу к информации. В общих чертах в области образования, а также воспитания молодого поколения необходимо проведение следующих мероприятий:

1. Прекращение и наложение запрета на распространение символики экстремистских и террористических групп в образовательных учреждениях.
2. Осуществление мер, направленных на предотвращение случаев демонстрации среди молодого поколения стереотипов, которые бы пропагандировали вышеописанную деятельность, а также исполнение действий, направленных на прекращение оскорблений граждан иных национальностей.

3. Развитие часов воспитательных работ с обучающимися, суть которых должна заключаться в разговоре о веротерпимости и толерантности.

4. Проведение дополнительной подготовки преподавателей и учителей с целью утверждения понимания, касающегося вопросов толерантности и веротерпимости.

В Российской Федерации существует множество сайтов, занимающихся работой по борьбе с идеологией терроризма и экстремизма. Одними из таких сайтов, функционирующих с целью развития общего информационного антитеррористического пространства, служат порталы «Наука и образование против террора», «Молодежь и Чистый Интернет», «Терроризму-Нет!» и др.

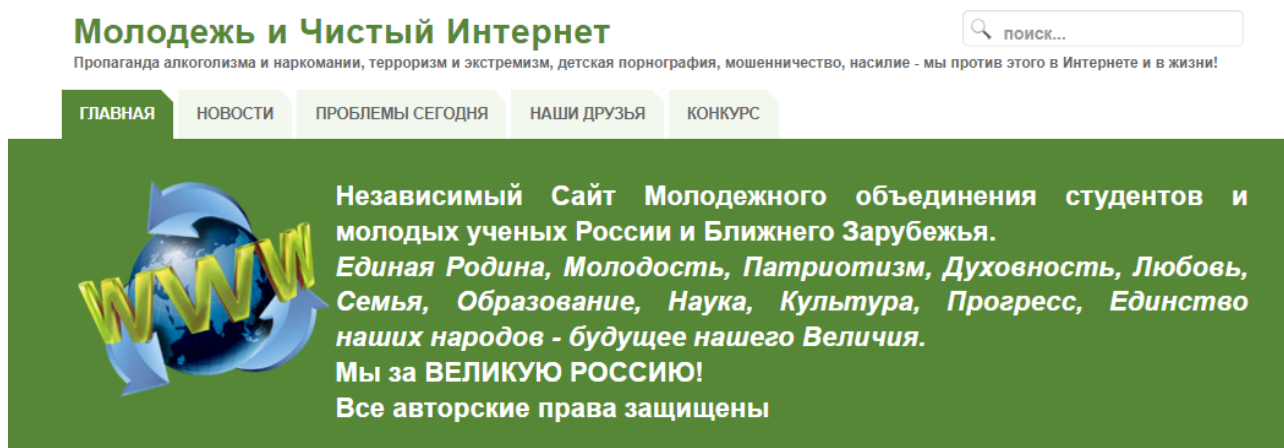


Рис. 1. Интерфейс сайта «Молодежь и Чистый Интернет»

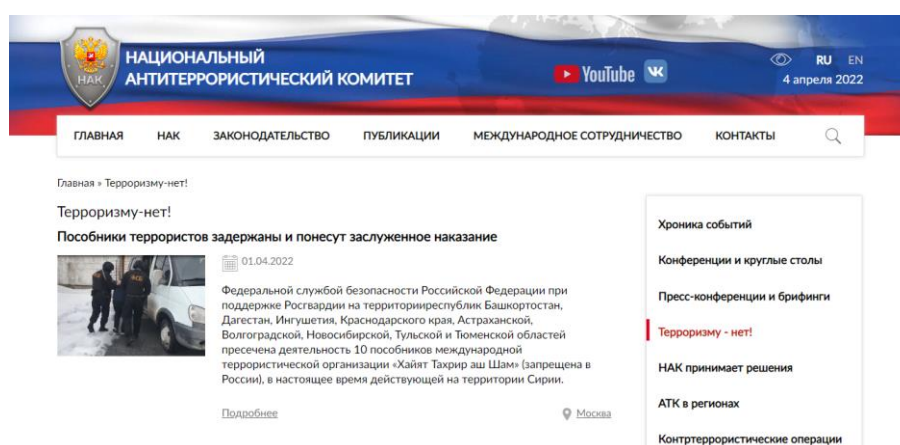


Рис. 2. Интерфейс сайт «Терроризму – Нет!»

Разработанные специалистами данные веб-ресурсы, производящие антитеррористическую пропаганду, воспитывающие среди молодых людей неприятие и непризнание идеологий терроризма и экстремизма, а также утверждения мнения о том, что данная деятельность является деструктивной, служат важным механизмом для борьбы с указанными направлениями.

Задача преподавателей и учителей – распространить данные сайты среди молодых людей. К примеру, посредством проведения веб-семинаров для учеников и студентов. Веб-семинар – это вариант web-конференции, онлайн-встреч или просмотр презентаций через Интернет.

Назначение веб-семинаров среди молодежи в образовательной среде является формирование устойчивого мнения о деструктивном влиянии ресурсов, содержащих пропаганду деятельности террористических организаций.

Веб-семинары должны решать следующие вопросы:

1. Касающиеся процесса образования: демонстрация способов распространения деятельности террористов, в том числе в сети Интернет, знакомства с классификацией терроризма (существующим видами).

2. Воспитательные: пропагандировать сайты, создаваемые на территории Российской Федерации, для воспитания в молодежной среде непризнания идеологии терроризма.

Следует также обратить внимание на правила проведения указанных мероприятий:

1. Не забывать задавать вопросы в ходе проведения веб-семинаров с обучающимися.

2. Редко показывать слайды, в содержании которых только теория, – они, как правило, воспринимаются молодежью хуже.

3. Не забывать про интонацию и голос доводящего информацию преподавателя – использовать энергичные движения и интонации.

4. Не забывать про использование средств интерактивных досок (к примеру, для рисования).

В современной научно-публицистической литературе существует довольно много путей, предлагающих методы противодействия идеологии терроризма в сети Интернет, а также СМИ. Вариантами решения данной проблемы могут являться:

1. Публичное осуждение идеологии терроризма.

2. Массовая пропаганда материалов, касающаяся воспитания уважительного отношения к традиционным ценностям.

3. Привлечение к деятельности просветительной работы духовных лидеров основных конфессий.

Благоприятный результат противодействия деструктивной деятельности терроризма и экстремизма в сети Интернет в значительной мере зависит от таких факторов, как: периодичность проведения данной работы, наступательность и уровень мастерства проведения [5, с. 91].

Немалый вклад вносят и многие вузы, и школы нашей страны. В сотрудничестве с МВД России, различными общественными организациями вышеуказанные организации проводят политику по объяснению корректного поведения:

- непрерывное развитие и использование существующих ресурсов глобальной сети, которые способны выстраивать беседы, которые удобны и восприимчивы студентам и ученикам;

- проведение конференций и форумов с целью пропаганды антитеррористической деятельности;
- проведение конкурсов на лучшую письменную или научную работу по теме противодействия терроризму.

Список литературы

1. Абулин К. А. Безопасность в интернете [интернет-портал]. URL: <http://www.comprice.ru/> (дата обращения: 14.04.2022).
2. Детские браузеры – защита ребенка от угроз интернета [интернет-портал]. URL: http://www.3dnews.ru/software/detskie_brauzeri/ (дата обращения: 14.04.2022).
3. Программы контроля, родительский контроль [интернет-портал]. URL: <http://nicekit.ru/parental-control/time-boss.php> (дата обращения: 14.04.2022).
4. Противодействие преступлениям в сфере информационных технологий: учебник / В. В. Гончар и др. М. : Московский университет МВД России имени В.Я. Кикотя, 2021.
5. Мешков М. В., Гончар В. В. Досудебное соглашение о сотрудничестве: проблемы и перспективы // Закон и право. М., 2011.

Иванов А. А.¹,

слушатель факультета подготовки специалистов

в области информационной безопасности

Московского университета МВД России имени В.Я. Кикотя

Научный руководитель:

Лустин В. И.,

старший преподаватель кафедры

информационной безопасности учебно-научного

комплекса информационных технологий

Московского университета МВД России имени В.Я. Кикотя

ПОВЫШЕНИЕ ЗАЩИЩЕННОСТИ ОБЪЕКТА ИНФОРМАТИЗАЦИИ ОТ УТЕЧКИ ИНФОРМАЦИИ ПО ОПТИКО-ЭЛЕКТРОННОМУ КАНАЛУ

Анализ текущего состояния преступности в сфере информационных технологий позволяет сделать вывод о стремительном развитии средств, методов, доступности технологий для совершения противоправных деяний. С каждым днем у большого количества организаций одной из острых тем для обсуждения встает вопрос об обеспечении должным образом защиты информации. На момент 2021 г. специалистами компании в области защиты от утечек информации, а также предотвращения внешних целевых атак «InfoWatch», приведены статистические данные по количеству утечек из муниципальных, государственных и коммерческих организаций – зафиксировано **2395** утечек данных [1]. В предыдущие периоды (2019–2021 гг.) рост количества зарегистрированных внешних и внутренних утечек информации, имеющих умышленный характер, **сохраняется с настоящими тенденциями**. Ввиду растущих угроз безопасности стоит обратить внимание на всевозможные принципы и каналы утечки для их предотвращения.

Актуальная тема информатизации – серьезная проблема с точки зрения преступности, поскольку злоумышленники используют информатизацию как инструмент для совершения преступлений. Использование информационных технологий для сбора, хранения, обработки, передачи и представления сведений стало неотъемлемой частью успешной деятельности органов внутренних дел. Оптимизация информационных процессов, автоматизированный анализ больших массивов информации, а также оперативный доступ сотрудников к распределенным информационным ресурсам способствуют эффективному выполнению служебных обязанностей. В настоящее время в органах и подразделениях МВД России активно внедряются новые технологии, обеспечивающие связь с Единой системой межведомственного электронного взаимодействия (СМЭВ). Данная система включает в себя информационные базы данных, содержащие сведения об используемых органами и организациями программных и технических средствах, обеспечивающих возможность доступа и взаимодействия с другими информационными системами и электронными ресурсами [2].

¹ © Иванов А. А., 2022.

Ввиду многообразия и важности задач, выполняемых органами внутренних дел, а также обрабатывания большого количества информации в ходе их выполнения возникает потребность в обеспечении сохранности этих данных, а также организации ее передачи наиболее быстрым способом. В настоящее время наиболее используемым источником передачи информации является оптико-электронный канал. Под оптико-электронным каналом в данном случае подразумевается использование технических средств, преобразующих электрический сигнал в оптический и наоборот, а также непосредственно использование оптоволоконных сетей связи и его компонентов. Актуальность использования данного способа организации связи заключается в наличии следующих преимущественных характеристик:

- пропускная способность до 10 Гбит/с или более;
- высокая помехоустойчивость, заключающаяся в отсутствии искажения информации в сегменте сети при нахождении рядом с линиями электросвязи, а также отсутствие возможности несанкционированного подключения к сети без физического ее разрушения;
- широкий температурный диапазон, не влияющий на работоспособность;
- возможность использования цельного, большого сегмента сети (данная характеристика обуславливается весьма малым затуханием в оптоволокне);
- малый вес проводника;
- долговечность использования;
- приемлемая закупочная цена проводника ввиду технологических особенностей производства [3].

Однако в силу появления новых технологий и способов осуществления несанкционированного доступа существует необходимость в создании новых методических рекомендаций по защите оптико-электронного канала, а также доработке существующих требований:

1. Систематическое проведение мониторинга состояния целостности кабеля, а также сигналов, циркулирующих вблизи него.

Для достижения данного результата необходимо использование оптоволокну, в состав которого будут входить специальные волокна, благодаря которым будет осуществляться наблюдение состояния кабеля. Конечно, при внедрении такой технологии в состав оптоволокну цена кабеля будет значительно выше, однако в случае несанкционированного доступа к такой сети связи и изгибах кабеля будут происходить потери контролирующего сигнала и, как следствие, отправка тревожного сигнала о неполадках в работе в систему мониторинга.

2. Периодическое проведение замеров величины оптически значимой мощности.

В процессе работы оптоволоконной сети связи может осуществляться мониторинг уровня оптически значимой мощности. Если величина сигнала будет отличаться от выставленного нормального значения, то система контроля выдаст сигнал тревоги. Однако существует необходимость в проведении соответствующей кодировки сигнала так, чтобы в волокне присутствовал постоянный уровень сигнала, не зависящий от наличия передаваемой информации.

3. Использование оптических рефлектометров.

Поскольку подсоединение к волокну забирает часть оптического сигнала, для обнаружения подключений могут использоваться оптические рефлектометры.

4. Использование специальных структур в оптическом волокне.

Волокно данного вида имеет низкие потери при процессе передачи данных, а также большой радиус сгиба. В структуру данного вида волокна будут входить фотонные кристаллы, которые составляют фотонно-кристаллические световоды. Большая гибкость в фотонно-кристаллическом виде волокна достигается наличием точечного дефекта в центре симметрии. В основном, при создании проводника используют кварц или песок, а также полые места с воздухом. Некоторое количество таких отверстий может быть заполнено иными жидкими или газообразными веществами, а также жидкими кристаллами. Поэтому за счет наличия таких характеристик при прохождении пучка света менее влияют на состояние попытки вытягивания или перекручивания кабеля.

5. Использование шифрования.

Несмотря на то, что использование алгоритмов шифрования защищает информацию на программном уровне, а не на физическом, т. е. никак не сможет пресечь попытку подключения к сети, однако повлиять на целостность самой информации может прямым образом, тем самым в случае утечки расшифрованные данные могут иметь минимум полезного содержания.

Список литературы

1. Аналитический отчет: «Россия: утечки информации ограниченного доступа, 2021 год» // Акционерное общество «ИНФОВОТЧ» URL: https://www.infowatch.ru/sites/default/files/analytics/files/InfoWatch_Мир_Утечки_2021/ (дата обращения: 22.04.2021).
2. Информационные технологии управления и организация защиты информации [Электронный ресурс]: курс лекций / В. А. Апульцин, Ш. Х. Гонов, В. Н. Лебедев, В. Ю. Петрова. Москва: Академия управления МВД России, 2021. URL: https://мвд.рф/upload/site120/folder_page/015/122/996/Apultsin_Gonov_na_sayt.pdf/ (дата обращения: 21.04.2022).
3. Коротун В. / Волоконно-оптический кабель: назначение, конструкция, классификация [Электронный ресурс] // ASUTPP – заметки электрика. URL: <https://www.asutpp.ru/volokonno-opticheskiy-kabel.html/> (дата обращения: 10.04.2022).
4. Преимущества оптоволоконных линий связи и эффективные пути развития систем телекоммуникаций в оборонной промышленности [Электронный ресурс]: статья в сборнике трудов конференции/ А. С. Манжос, Б. К. Дергаус // научная электронная библиотека elibrary.ru. URL: <https://elibrary.ru/item.asp?id=24090817> (дата обращения: 10.04.2022).

Изюмский Д. И.¹,

курсант 192 взвода факультета подготовки

сотрудников для оперативных подразделений полиции

Московского университета МВД России имени В.Я. Кикотя

Научный руководитель:

Гончар В. В.,

начальник кафедры информационной безопасности

учебно-научного комплекса информационных технологий

Московского университета МВД России имени В.Я. Кикотя,

кандидат юридических наук, доцент

К ВОПРОСУ О МЕДИАТЕРРОРИЗМЕ, КАК УГРОЗЕ МЕДИАБЕЗОПАСНОСТИ

Все мы живем в постиндустриальном обществе, в условиях, когда люди работают с немислимыми, для человечества прошлых веков объемами информации, связано это, прежде всего, с развитием информационно-телекоммуникационной сети Интернет, в которой без особого труда ищутся и (или) распространяются знания по определенным вопросам. В связи с чем вопросы медиабезопасности являются как никогда актуальными.

Под медиабезопасностью понимается «как защищенность самой информационной среды, так и защищенность общества от деструктивного воздействия информации на психологическое и социальное воздействие граждан» [1].

В науке выделяют два вида преступности: 1) реактивная; 2) ресурсная. На наш взгляд, терроризм относится именно к первому. Бесспорно, террористические акты могут совершаться для получения денежных средств, однако мы считаем, что большинство общественно опасных деяний такого плана являются ответными действиями, реакцией на определенные решения, принимаемые государством. Такого же мнения придерживается и законодатель, закрепляя в ст. 205 Уголовного кодекса Российской Федерации (далее – УК РФ) цели совершения такого преступления, к которым относятся: «дестабилизация деятельности государственных органов, а равно воздействие на принимаемые ими решения» [2].

В теории выделяют довольно большое количество видов терроризма, таких как экономический, ядерный, технический, информационный, и др. Про последний как раз и будет вестись речь в данной статье. В соответствии с Федеральным законом от 27 июля 2006 г. № 149 под информацией понимаются «сведения (сообщения, данные) независимо от формы их представления» [4].

Терроризм в сфере информации получил название медиатерроризм, представляет из себя «использование возможностей массмедиа для создания тиражирования чувства страха, а также для управления общественным сознанием» [3].

¹ © Изюмский Д. И., 2022.

Основная опасность в данной сфере проявляется в так называемых сайтах террористической направленности, социальных сетях и средствах массовой информации.

Опасность сайтов заключается в пропаганде идеологии, в описании проблем, зачастую резонансного характера, которые призвана решать та или иная террористическая организация. В описании действий необходимых для достижения целей, в даче конкретных пошаговых инструкций, это все усугубляет доступность и легконаходимость нежелательной для нас, как правозащитников, информации, такой как: 1) где найти компоненты для создания оружия массового поражения (далее – ОМП); 2) как создать ОМП; 3) как лучше его применить, и тому подобные сведения.

Помимо всего прочего такие интернет-ресурсы обладают интересной структурой построения информации, зачастую используется интересная формулировка «мы», этим добивается обезличивание террористов и усиление эффекта толпы, который нарастает благодаря наличию на таких ресурсах чатов для общения, в которых «более опытные» люди делятся советами с менее осведомленными.

На наш взгляд, для борьбы с такими ресурсами сотрудникам правоохранительных органов необходимо вступать посредством использования сети Интернет в контакт с такими группами людей и убеждать их отказываться от совершения тех или иных действий, а равно пытаться искоренить их террористические убеждения, наклонности. Похожая ситуация обстоит с социальными сетями. Благодаря мессенджерам террористы находят сторонников, зачастую это люди склонные к принятию чужой точки зрения, несформировавшиеся до конца как полноценные личности и не имеющие своей четкой жизненной позиции, а также координируют действия.

На наш взгляд, основная опасность СМИ заключается в их стремлении осветить все происходящее. Так, если бы большое количество террористических актов не подвергалось огласке, то их количество заметно бы снизилось ввиду снижающегося уровня поддержки населения. Мы считаем, что основная задача СМИ в данном вопросе заключается в освещении порядка действий в случае совершенного теракта, а также в пропаганде антитеррористического мировоззрения. Распространение такой информации должно быть повсюду, на каждом сайте, в любой рекламе, в каждом выпуске новостей, в данном случае у людей на подкорке головного мозга сформируется отвращение к террористам и их деятельности [5, с. 112].

Необходимо отметить, что уголовная ответственность за такого рода деяния предусмотрена ч. 2 ст. 205.2 УК РФ и, на наш взгляд, санкция неоправданно мала, мы предлагаем изменить срок лишения свободы с максимально возможных 5 лет до 15 лет лишения свободы, так как в УК РФ имеются составы преступления, получившие в науке уголовного права наименование «составы опасности», в которых ответственность наступает только за угрозу наступления общественно опасных последствий, а в данном случае такая угроза колоссального масштаба

из-за обращенности сведений к неопределенному кругу людей. Также необходимо добавить ч. 3 ст. 205.2 УК РФ, диспозицию которой сформулировать с учетом того, что действия, предусмотренные чч. 1, 2 данной статьи, повлекшие совершение террористического акта, должны наказываться максимально строго – пожизненное лишение свободы, либо смертная казнь.

Резюмируя все вышесказанное, целесообразно рекомендовать:

1. Сотрудникам правоохранительных органов вступать посредством использования сети Интернет в контакт с такими группами людей и убеждать их отказываться от совершения тех или иных действий, а равно пытаться искоренить их террористические убеждения, наклонности.

2. Основной задачей СМИ сделать не освещение террористических актов, а пропаганду антитеррористического мировоззрения.

3. Конкретизировать редакцию ст. 205.2 УК РФ в соответствии с изложенными в данной статье предложениями.

Список литературы

1. Ежова Е. Н. К вопросу о злоупотреблении свободой массовой информации в сфере новых медиа: опыт лингвистических экспертиз // Знак: проблемное поле медиаобразования. 2017. №2 (24). С. 60.

2. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (ред. от 25.03.2022) // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения: 08.04.2022).

3. Художекова М. А. Медиатерроризм как угроза медиабезопасности. Принципы построения текстов террористических сайтов // Вестник ЧелГУ. 2013. № 22 (313). С. 231.

4. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (последняя редакция) // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 08.04.2022).

5. Организация расследования хищений денежных средств из банкоматов: учебное пособие / В. В. Гончар и др. Казань. Бук. 2021.

Филимонова Ю. В.¹,

курсант факультета подготовки специалистов

в области информационно безопасности

Московского университета МВД России имени В.Я. Кикотя

Научный руководитель:

Галиев Д. В.,

преподаватель кафедры информационной безопасности

учебно-научного комплекса информационных технологий

Московского университета МВД России имени В.Я. Кикотя

ИСПОЛЬЗОВАНИЕ СЕТЕВЫХ УЯЗВИМОСТЕЙ ДЛЯ ПОЛУЧЕНИЯ ОПЕРАТИВНО-ЗНАЧИМОЙ ИНФОРМАЦИИ

За последние десятилетия информатизация и информационные технологии проникли во все сферы жизни общества и области человеческой деятельности. Параллельно с масштабным ростом информационных систем в XXI в. растет и необходимость обеспечения новой формы безопасности общества, информационной. Появляются новые формы преступлений, которые связаны с высокими технологиями, получением несанкционированного доступа к удаленным хостам и информации, хранящейся на них. Целостность систем информационной безопасности может быть нарушена по ряду причин: ошибки в разграничении доступа и политике безопасности, неправильная настройка систем выявления факторов неавторизованного доступа в компьютерную сеть или несанкционированное управление ими, уязвимости установленных сервисов или операционной системы, открытые порты, публичные данные о версии операционной системы, пакетах обновлений и запущенных сервисах, которые могут быть подвергнуты атакам эксплойтов. Также устаревшие системы обнаружения вторжений, антивирусы, другие средства защиты и многое другое.

Открывается возможность осуществления определенных атак, используя подобные уязвимости системы. Например, получить доступ к администрированию системы, управлять разграничением прав других пользователей и политикой безопасности системы в целом, получить доступ к информации ограниченного доступа, внедрить вредоносный код и другие, в зависимости от целей и заготовленных сценариев. Вследствие этого возникает необходимость на этапах проектирования, реализации, тестирования, внедрения и сопровождения администратору системы проводить мониторинг уровня безопасности и защищенности системы, предъявленный к ней.

Для более детального и углубленного рассмотрения тематики данного вопроса обратимся к ГОСТ Р 56546-2015, который трактует информационную систему как совокупность содержащейся в базах данных информацию и обеспечивающие ее обработку информационные технологии и технические средства, а ее уязвимость как свойство, предоставляющее возможность реализации угроз безопасности такой системы. Она может возникать вследствие ряда причин: ошибка

¹ © Филимонова Ю. В., 2022.

при создании программного обеспечения, недочет инженера, проектировавшего систему, отсутствие постоянной поддержки и предоставления компанией-поставщиком обновлений. Существует официальный структурированный список уязвимостей CVE (англ. «Common Vulnerabilities and Exposures»), включающий в себя перечень самых распространенных уязвимостей информационной безопасности, где каждой присвоен идентификационный номер вида CVE-год-номер, а также описание и ряд общедоступных ссылок. Как только новая уязвимость и ее описание появляются в открытом доступе, ей может воспользоваться как злоумышленник и производители программного обеспечения для ее закрытия, так и сотрудники правоохранительных органов с целью получения оперативно-значимой информации для расследования преступлений, совершенных с применением информационных технологий.

С целью реализации установленной уязвимости необходим эксплойт, который представляет из себя полноценную программу, обычный скрипт, т. е. некую последовательность исполняемых команд, использующую уязвимости программного обеспечения для проведения атаки на компьютерную систему или же словесное описание того, как должна быть реализована та или иная уязвимость. Целью такой атаки будет получение несанкционированного доступа, нарушение целостности и функционирования системы и т. п. Для защиты от подобных программ используются разнообразные антивирусы, системы обнаружения и предотвращения вторжений и межсетевые экраны. Для того, чтобы работа этих программ соответствовала требованиям, предоставляемым к ним, необходима их детальная настройка специалистом по пентестингу.

Деятельность пентестера напрямую направлена на оценку безопасности компьютеров и сетей по средствам моделирования атак злоумышленника. Он использует активный анализ системы на наличие возможных уязвимостей, которые могут стать причиной несанкционированного доступа или изменения конфигурации системы. Реализуется такая деятельность путем проведения совокупности тестов на проникновение. Используя специализированное программное обеспечение, базы данных уязвимостей и эксплойтов, специалист пытается заполучить доступ к компьютерному серверу или целевой системе.

Одним из самых уязвимых мест компьютерной системы являются сетевые порты, поскольку, как только пользователи собираются обмениваться информацией по сети, именно они в первую очередь открывают информационные порталы для обмена. Вообще говоря, порт – это некое виртуальное расширение, дополнение к сетевому адресу. Информация дойдет до вашего компьютера по уникальному адресу узла в компьютерной сети, построенном на основе стека протоколов TCP/IP, но без определенного номера порта, он просто не поймет, как обработать ее и с помощью какого программного обеспечения. Сетевые порты компьютера – это связи между сервисами, которые запущены в операционной системе и дублирующими процессами на компьютерах-хостах, которые могут находиться на удаленности многих километров. Например, порты с номерами до 1023 в операционных системах считаются наиболее важными для сетевой дея-

тельности, поэтому для доступа к ним и службам, с ними связанными часто требуется наличие самой высокой степени привилегий в изменении системы, например, root в Unix, т. е. специального аккаунта, владелец которого имеет право на выполнение всех без исключения операций.

В рамках оперативно-розыскных мероприятий данный метод сбора доказательств относится к такому мероприятию как снятие информации с технических каналов связи.

Снятие информации с технических каналов связи – оперативно-розыскное мероприятие, заключающееся в негласном съеме информации, передаваемой по сетям электрической связи, компьютерным и иным сетям, путем контроля специальными техническими средствами работы соответствующих систем и устройств, в том числе излучаемых ими электромагнитных и других полей [1].

Данное мероприятие может быть осуществлено путем:

- внедрения программных, аппаратных устройств для перехвата информации;
- непосредственного перехвата информации в компьютерных сетях и на линиях связи, расшифровки этой информации;
- внедрением программного обеспечения, нарушающего функционирование систем защиты, воздействующего на паролевые системы защиты, компрометации ключей в целях получения доступа к защищаемой информации.

Лицами, уполномоченными на проведение данного оперативно-розыскного мероприятия, выступают оперативные сотрудники, осуществляющие оперативно-розыскную деятельность, с использованием оперативно-технических сил и средств органов федеральной службы безопасности, органов по контролю за оборотом наркотических средств и органов внутренних дел. В ряде случаев возможно привлечение организаций, осуществляющих предоставление услуг связи и сообщений (интернет-провайдер, компания – владелец линии связи и др.)

Однако стоит принимать во внимание тот факт, что приобщение доказательств к материалам уголовного дела, полученных проведением рассматриваемого ОРМ, нередко может вызывать ряд трудностей, вызванных в первую очередь недостаточной разработанностью нормативно правовой базы, а также правоприменительной практики.

Так, получение доступа к информации лица наказывается уголовным законодательством – ст. 272 УК РФ «Неправомерный доступ к компьютерной информации». Подобное получение информации, ее искажение, блокирование, перехват нарушает конституционные права гражданина, закрепленные в ч. 2 ст. 23 Конституции Российской Федерации, в которой говорится, что каждый человек имеет право на тайну переписки, телефонных переговоров, почтовых и иных сообщений, и ограничение данного права возможно только лишь по решению суда.

В данном случае необходимым будет применение данного программного средства в рамках оперативно-розыскной деятельности. В Федеральном законе от 12.08.1995 № 144-ФЗ (ред. от 29.06.2015) «Об оперативно-розыскной деятельности», в ст. 7 содержатся основания для проведения оперативно-розыскных мероприятий.

Однако приобщение подобных материалов к уголовному делу весьма трудоемкий процесс. Существует межотраслевая инструкция, которая регламентирует порядок предоставления результатов ОРМ в суде: приказ МВД России, Министерства обороны Российской Федерации, ФСБ России, Федеральной службы охраны Российской Федерации, Федеральной таможенной службы, Службы внешней разведки Российской Федерации, Федеральной службы исполнения наказаний, Федеральной службы по контролю за оборотом наркотиков, Следственного комитета Российской Федерации от 27 сентября 2013 г. № 776/703/509/507/1820/42/535/398/68 «Об утверждении Инструкции о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд».

В настоящее время использование сетевых технологий является одним из приоритетных направлений в развитии, как правовой, так и технической базы [2, с. 173]. Существует ряд задач, которые необходимо выполнить в ближайшее время, для успешного противодействия преступности:

- совершенствование правовой базы, позволяющей использовать сетевые технологии для получения доказательной базы при расследовании преступлений;
- обучение оперативных сотрудников новым сетевым технологиям, применяющимся в настоящее время;
- совершенствовать техническое оснащение оперативных сотрудников [3, с. 223].

Список литературы

1. Кушнир И. В. / Оперативно-розыскная деятельность. М., 2010.
2. Противодействие преступлениям в сфере информационных технологий: учебник / В. В. Гончар и др. М. : Московский университет МВД России имени В.Я. Кикотя, 2021.
3. Предварительное следствие в органах внутренних дел: учебное пособие / М. В. Мешков и др. М. : МосУ МВД России, 2007.

Куксов В. А.¹,

курсант факультета подготовки

сотрудников для оперативных подразделений полиции

Московского университета МВД России имени В.Я. Кикотя

Научный руководитель:

Мурадян С. В.,

доцент кафедры уголовного права

Московского университета МВД России имени В.Я. Кикотя,

кандидат юридических наук

К ВОПРОСУ О ВОВЛЕЧЕНИИ НЕСОВЕРШЕННОЛЕТНИХ В ЭКСТРЕМИСТСКУЮ ДЕЯТЕЛЬНОСТЬ С ПОМОЩЬЮ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Прогресс развития современного общества сегодня во многом увеличивает защищенность граждан, облегчает процессы их коммуникации, получения услуг и информации. Одновременно он позволяет более плотно взаимодействовать с несовершеннолетними гражданами государства, в том числе и вопреки воле родителей или не ставя их в известность. В этой связи, вопрос о привитии несовершеннолетним антиобщественных взглядов, вовлечении их в совершение преступления экстремистской направленности с помощью информационно-телекоммуникационных технологий встает перед правоохранительными органами как никогда остро.

Для начала определим, что в себя включает понятие экстремистской деятельности, изложенное в п. 1 ст. 1 Федерального закона от 25 июля 2002 г. № 114-ФЗ «О противодействии экстремистской деятельности» [1]. Согласно позиции законодателя понятия экстремистская деятельность и экстремизм являются тождественными и включают в себя:

1. Изменение основ конституционного строя Российской Федерации насильственным путем.
2. Общественное поддержание и оправдание преступлений, направленных на нарушение общественной безопасности, терроризма.
3. Социальную, расовую, национальную и религиозную рознь.
4. Нарушение прав, свобод и законных интересов человека и гражданина в зависимости от его принадлежности к различным сферам жизни общества.
5. Использование различных символик, формирующих отрицательное отношение к идеологии нацизма и экстремизма.
6. Общественные призывы к осуществлению подобной (экстремистской) деятельности.
7. Организацию, подготовку и подстрекательство к экстремистской деятельности.

¹ © Куксов В. А., 2022.

Основания возникновения уголовной ответственности за преступления экстремистской направленности изложены в положениях Конституции Российской Федерации ст.ст. 13, 14, 29 и др. [2]. В Уголовном кодексе Российской Федерации в примеч. 2 к ст. 282¹ [3] содержится определение преступлений экстремистской направленности, согласно которому под преступлениями экстремистской направленности понимаются «преступления, совершенные по мотивам политической, идеологической, расовой, национальной или религиозной ненависти, или вражды либо по мотивам ненависти или вражды в отношении какой-либо социальной группы, предусмотренные соответствующими статьями Особенной части УК РФ и п. «е» ч. 1 ст. 63 УК РФ».

Стоит отметить, что 9 февраля 2022 г. председатель Верховного Суда Российской Федерации В. М. Лебедев в ходе своего выступления на совещании судей арбитражных судов и судов общей юрисдикции отметил рост количества осужденных за экстремизм. В 2020 г. их количество составляло 325 человек, а в 2021 г. составило уже 606 человек.

В свою очередь, отчетные данные МВД России, констатируют общий прирост таких преступлений за 2021 календарный год на 27 % (1057 преступлений экстремистской направленности).

Тенденция к «омолаживанию» экстремизма, присущая сейчас всем формам его проявления, подтверждается активными стремлениями экстремистских организаций вовлечь в свою деятельность несовершеннолетних лиц. При этом роль несовершеннолетних не ограничивается распространением литературы радикального характера, что уже в случае наличия всех признаков состава преступления следует квалифицировать по ст. 280 УК РФ, но часто сопровождается и участием в экстремистских сообществах или в деятельности экстремистских организаций (ст. 280¹ и ст. 280² УК РФ).

Опасность вовлечения несовершеннолетних не только в совершение каких-либо единичных преступлений экстремистской направленности, а в участие в подобных преступных структурах создает предпосылки для стойкой утраты такими несовершеннолетними возможностей к возвращению к правомерному поведению. Реализуется потенциальная опасность в виде формирования аддиктивного поведения, появления склонности и рвения несовершеннолетних к ведению незаконного образа жизни. Для осуществления активной экстремистской деятельности нужны финансовые средства, которые в случае отсутствия заработка могут быть добыты преступным путем. В итоге, несовершеннолетние, вовлеченные в деятельность экстремистской организации, со временем начинают вовлекать более молодых и неопытных субъектов общества в свою преступную деятельность. Таким образом, количество и размеры экстремистских организаций и экстремистски настроенных несовершеннолетних неуклонно растет, создавая «снежный ком» и стимулируя распространение девиантного поведения среди все новых и новых несовершеннолетних.

Непосредственно само вовлечение несовершеннолетнего в совершение преступления по мотивам политической, идеологической, расовой, национальной или религиозной ненависти, или вражды либо по мотивам ненависти или вражды

в отношении какой-либо социальной группы является уголовно наказуемым деянием и выделено законодателем в качестве квалифицирующего признака в ч. 4 ст. 150 УК РФ.

Уголовный кодекс содержит ряд норм, связанных уголовной ответственностью именно за преступления экстремистской направленности (ст. 280 УК РФ «Публичные призывы к осуществлению экстремистской деятельности»; ст. 282 УК РФ «Возбуждение ненависти либо вражды, а равно унижение человеческого достоинства»; ст. 282.1 УК РФ «Организация экстремистского сообщества»; ст. 282.2 УК РФ «Организация деятельности экстремистской организации»). Некоторые статьи, расположенные в иных главах Уголовного кодекса Российской Федерации, также затрагивают те или иные стороны понятия «экстремистская направленность». О проблеме установления объекта преступления экстремистской направленности говорит, например, И. С. Суханова [4], утверждая, что объектом таких преступлений могут выступать как разнообразные личные интересы, субъективные права, блага, основы конституционного строя, общественное спокойствие. В этом и состоит некое уникальное свойство преступлений экстремистской направленности – нельзя выделить конкретного объекта посягательства.

При этом нельзя не согласиться с позицией Л. В. Глазковой, которая в своих трудах приходит к выводу о том, что по своей сути, любые преступления, которые предусматривает Особенная часть Уголовного кодекса имеют в себе квалифицирующий признак экстремизма [5, с. 4].

За совершение противоправных деяний, а не общественно опасных, связанных с экстремистской деятельностью предусмотрена административная ответственность (ст. 20.3 КоАП РФ «Пропаганда и публичное демонстрирование нацистской атрибутики или символики»; ст. 20.3.1 «Возбуждение ненависти либо вражды, а равно унижение человеческого достоинства, если эти действия не содержат уголовно наказуемого деяния»; ст. 20.29 «Производство и распространение экстремистских материалов» [6]).

Выделим детерминирующие факторы, определяющие сущность экстремизма среди несовершеннолетних. Данные детерминанты представляют комплекс причин, которые приводят к такому поведению:

1. Социальные, которые выражаются в социальных и национально-этнических противоречиях внутри социума. Учитывая, что Российская Федерация многонациональное государство, обладающее пестрой национальной «картиной», возникновение в таком государстве противоречий на национально-этнической почве, приводящий к совершению преступлений этнической направленности, вполне закономерно.

2. Религиозные, вытекающие из предыдущей детерминанты. В Российской Федерации нет официально признанной государством религии. Свобода вероисповедания на территории одного многонационального и многоконфессионального государства влечет за собой и некие противоречия, побуждающие к совершению преступлений экстремистской направленности.

3. Экономические, которые связаны с недовольством граждан финансовым положением, расслоением по финансовому признаку, увеличением цен на товары и услуги.

Данный перечень является условным и, конечно же, не исчерпывающим.

Современные информационно-телекоммуникационные сети, являющиеся неотъемлемой частью нашей жизни, в то же время существенно облегчают распространение информации экстремистской направленности среди всех групп населения.

Так, решением Юргинского районного суда житель г. Юрга был осужден по ч. 2 ст. 280 УК РФ. Гражданин Ю. создал профиль в социальной сети «ВКонтакте», в котором призывал к насилию в отношении лиц неславянской национальности. Доказательством позиции обвинителя были результаты лингвистической экспертизы, которые позволили установить в действиях гражданина Ю. наличие публичных призывов к осуществлению экстремистской деятельности, совершенных с использованием средств массовой информации/информационно-телекоммуникационных сетей, в том числе сети Интернет [7, с. 114].

26 февраля 2020 г. было организовано расширенное заседание коллегии МВД России, где были подведены итоги работы органов внутренних дел за 2019 календарный год. В ходе коллегии Президент Российской Федерации В. В. Путин отметил важность профилактической работы с несовершеннолетними, в том числе и в области недопущения вовлечения их в преступления экстремистской направленности [8].

Сегодня дети с раннего возраста приобщаются к пользованию информационно-телекоммуникационной сети Интернет, устанавливая на информационно емкие мобильные устройства игры, «шутеры» и другие приложения, которые с детства учат их жестокости и создают предпосылки для совершения некоторых «игровых» действий в реальной жизни.

Посредством использования компьютерных онлайн-игр также широко распространено вовлечение несовершеннолетних в экстремизм, поскольку их функционал позволяет осуществлять «живое» онлайн-общение в чатах, по голосовому каналу, а также выполнение определенных заданий в реальной жизни, что можно квалифицировать как преступные действия по ч. 2 ст. 280 УК РФ [9, с. 44–50].

Несовершеннолетние в силу еще не сложившейся и неустойчивой психики, становятся легкой «наживой» для лиц, вовлекающих их в занятие экстремистской деятельностью. «Синий кит», «Разбуди меня в 4:20», «U19» и другие названия – некая игра, организованная с целью совершения несовершеннолетними противоправных деяний, а в итоге побуждающая их в конце игры к совершению самоубийства (ст. 110–110² УК РФ) [10, с. 103].

Список литературы

1. Федеральный закон от 25.07.2002 № 114-ФЗ «О противодействии экстремистской деятельности» [Интернет ресурс]. URL: <http://www.kremlin.ru/acts/bank/18939> (дата обращения: 07.04.2022).
2. Конституция Российской Федерации. Принята всенародным голосованием 12 декабря 1993 г. с изменениями, одобренными в ходе общероссийского голосования 1 июля 2020 г. [Интернет ресурс]. URL: http://pravo.gov.ru/proxy/ips/?doc_itself=&nd=102027595#I0 (дата обращения: 30.04.2022).
3. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 25.03.2022) [Интернет ресурс]. URL: <http://pravo.gov.ru/proxy/ips/?docbody&nd=102041891> (дата последнего обращения: 07.04.2022).
4. Суханова И. С. Особенности объекта преступлений экстремистской направленности // Вестник Московского университета МВД России. 2013. № 10. С. 99–103.
5. Глазкова Л. В. Преступления экстремистской направленности, совершаемые с использованием сферы телекоммуникаций и компьютерной информации // Актуальные проблемы российского права. 2021. № 12. // СПС «Консультант-Плюс».
6. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ (ред. от 26.03.2022) [Интернет ресурс]. URL: <http://pravo.gov.ru/proxy/ips/?docbody&nd=102074277> (дата обращения: 07.04.2022).
7. Постановление № 5-2957/2020 от 3 ноября 2020 г. по делу № 5-2957/2020 [Интернет ресурс]. URL: <https://sudact.ru/regular/doc/Xi8SXaf1begQ/> (дата обращения: 13.04.2022).
8. Заседание коллегии МВД России от 26.02.2020. [Интернет ресурс]. URL: <http://www.kremlin.ru/events/president/transcripts/62860> (дата обращения: 07.04.2022).
9. Интернет-портал Интерфакс – диверсифицированная информационная группа [Интернет ресурс]. URL: <https://www.interfax.ru> (дата обращения: 29.04.2022).
10. Противодействие преступлениям в сфере информационных технологий: учебник / В. В. Гончар и др. М. : Московский университет МВД России имени В.Я. Кикотя, 2021.

Макаров Р. Е.¹,

курсант факультета подготовки специалистов

в области информационной безопасности

Московского университета МВД России имени В.Я. Кикотя

Научный руководитель:

Дворянкин О. А.,

старший преподаватель кафедры информационной

безопасности учебно-научного комплекса

Московского университета МВД России имени В.Я. Кикотя,

кандидат юридических наук

ПРИНУЖДЕНИЕ К СОВЕРШЕНИЮ ТЕРРОРИСТИЧЕСКИХ АКТОВ С ИСПОЛЬЗОВАНИЕМ СЕТИ ИНТЕРНЕТ

Терроризм представляет огромную опасность для жизни общества.

Террористические акты имеют трагические последствия, главную роль в которых играют человеческие жизни.

С развитием информационных технологий Интернета он вышел на новый уровень, где его противозаконные действия становятся все более тщательно спланированными и организованными, а также стало легче преступникам вербовать людей для этих деяний. Наряду с этим настоящие технологии позволяют быстро и эффективно, с «определенной» анонимностью, распространять ложную и противозаконную информацию, используя различные сайты, социальные сети, видеохостинги и мессенджеры.

По данным Национального антитеррористического комитета Российской Федерации, на данный момент в мире действует около 5 тыс. интернет-сайтов, которые активно используют террористы. При этом число порталов, обслуживающих террористов и их сторонников, постоянно увеличивается [8].

В «Доктрине Информационной безопасности Российской Федерации», утвержденной Президентом Российской Федерации В. В. Путиным от 5 декабря 2016 г. № 646, отмечено, что экстремизм и терроризм в условиях глобализации и информатизации социума изменяют формы своего проявления, все чаще принимая виртуальный характер, зарождаясь и развиваясь в глобальной компьютерной сети, трансформируются в явления объективной реальности посредством социально-групповой самоорганизации молодежи [1].

В этой связи в настоящей статье особое внимание хочется обратить на распространение суицидального террора.

Для организаторов террористических акций данная технология является очень доступной и выгодной, так как «живая бомба» – самое дешевое оружие в их арсенале.

Стоит понимать, что террористы-смертники лишь конечное звено исполнителей в огромной системе разветвленных террористических организаций. Как пра-

¹ © Макаров Р. Е., 2022.

вило, организаторы терактов стремятся представить их как национальных экстремистов, религиозных фанатиков, а также мстителей за личные или иные обиды. Отметим, что по данным экспертов, около 10 % террористов-смертников действительно имеют черты фанатизма и экстремизма, остальных просто включили в эти две категории (люди, которые пошли на такой шаг не по своей воле либо и вовсе не подозревали о своей судьбе).

С учетом изложенного хотим отметить, что поиск потенциальной жертвы проводится с заранее тщательно отобранными критериями психологически доступных групп общества. В зоне риска находятся такие лица, как лица, испытывающие материальные и другие затруднения, например, люди, попавшие в полную материальную зависимость, лица в тяжелой кризисной ситуации в жизни, находящиеся в сильной депрессии, молодые девушки из неполных семей с низким материальным достатком, хронически больные люди, смертельно больные, лица с психическими отклонениями, с психопатиями, акцентуациями характера, люди с личностными и социальными дефектами (потерявшие работу, семью, смысл в жизни и т. д.), религиозные, идеологические и другие фанатики, акцентированные на борьбу с «неверными», политической властью и т. д., родственники погибших участников незаконных вооруженных формирований, желающие отомстить за смерть близких, сестры, жены или чаще сожительницы участников действующих террористических группировок, не являющиеся матерями их общих детей, внушаемые люди, попавшие под влияние идеологов террористических организаций, прославляющих и мифологизирующих суицидальный теракт как особый «подвиг».

При всем этом, по данным экспертов, исключается вербовка случайных, малознакомых добровольцев, так как они не обладают необходимыми психологическими характеристиками.

Таким образом, делая предварительный вывод, хотим отметить, что для каждого кандидата «потенциальной жертвы» подбирается индивидуальная тактика в зависимости от конкретной жизненной ситуации. Также правильно подобранная манипуляция позволяет умело воздействовать именно на тот мотив, чувства и эмоции человека, которые подходят для конкретного этапа жизни человека. Наряду с этим не стоит исключать шантаж и угрозы, где наиболее частой является угроза – отнять детей у родителей.

Кроме этого самым жестоким методом принуждения является физическое насилие и издевательство, как правило, в отношении женщин, когда она отказывается встать на путь террористки-смертницы. В этой связи особенно уязвимы женщины с «востока» (мусульманские страны), ведь надругательство над ними в корне ломает их нормы и уставы, так как у них нет больше возможности вернуться в семью или выйти замуж, в связи с этим единственным возможным выходом является решение стать на путь смертницы.

На Северном Кавказе все чаще в последние годы мы можем наблюдать активное вовлечение женщин в террористическую деятельность. Действия вербовщиков в данной ситуации происходят в Интернете путем знакомства на определенных сайтах. Вербовщики представляются от имени молодых военнослужащих,

которые боготворят своих жертв, окутывая общение ореолом любви и романтики. После первого свидания, как правило, девушка домой уже не возвращается. Примером подобной истории является 17-летняя Д. Абдурахманова, подорвавшая себя на станции «Парк Культуры» в Москве.

Таким образом, методов и технологий принуждения, как сказано ранее, существует огромное множество, особенно активно используются в последнее время информационные технологии Интернета, которые быстро и очень часто эффективно решают широкий круг задач, т. е. пропаганда, вербовка, радикализация, подстрекательство, финансирование, планирование, координация, обучение и многое другое.

Далее более подробно разберем методы, с помощью которых Интернет используется в террористических целях.

Пропаганда. Основной целью является придание огласке террористической деятельности и привлечение новых потенциальных сторонников для будущей вербовки. Осуществляется пропаганда посредством распространения сообщений, презентаций, аудио- и видеофайлов. Также применяются виртуальные ролевые игры, где игрок выступает в качестве террориста, который выполняет поставленные перед ним цели.

Данный метод несет в себе психологическую манипуляцию, основанную на подрыве веры людей в свои ценности, а также повышение уровня тревоги, страха и паники среди населения или его отдельных групп.

Не стоит забывать и о веб-сайтах, которые выставляют террористические организации в «выгодном свете». В основном такие сайты распространяют идеи терроризма и экстремизма, осуществляют информационную и финансовую поддержку групп международных террористических организаций, разжигают споры относительно расовой или национальной принадлежности, носят ознакомительный характер. Эти темы находят самый большой отклик среди сторонников радикальных взглядов.

Вербовка. Вербовка направлена на установление отношений с потенциальными новобранцами. Террористические организации тщательно собирают информацию о пользователях, посещающих их сайты, далее приступают к непосредственному взаимодействию с наиболее подходящими для них претендентами, предоставляют доступ к закрытым веб-сайтам и чат-группам. Использование таких форумов дает возможность для окончательной вербовки, а также обучения и постоянной поддержки. На этой стадии претендента ослабляют как психически, так и физически. Для этого применяется паразитический контент, который склоняет своих жертв к грусти, печали, тоске. При длительном воздействии такого контента у людей все откладывается на подсознательном уровне.

Отметим, что вербовка полностью адаптирована под конкретные ситуации человека. Проводится тщательная подготовка, учитываются многие факторы, такие, как пол, возраст, социальный статус, экономические обстоятельства. Позднее все это используется для давления на уязвимые места человека, вызывая чувства несправедливости, унижения, изоляции.

Существуют технологии, способные воздействовать и вызывать трансформацию смысловых установок разрабатываемого, а именно:

- положительная привлекательность ощущения принадлежности к тайной могущественной организации. В этом понимании человек обретает символическое бессмертие, недопустимое в обыденной жизни;
- деформация смысла жизни и трактовка экзистенциальных ценностей (исходная позиция: каждый человек верит в нечто более важное, чем жизнь и ищет положения «смерть-жизнь». Чем ближе и более незамедлительна для человека смерть, тем больше необходимы ценности жизни);
- тематика, не связанная с религией, но допускающая террористические формы протеста (борьба за права животных и за спасение окружающей среды может также быть поводами, оправдывающими терроризм);
- характеристика исторических позиций как основ для достижения светлого будущего любой ценой (оправдание террористических событий прошлого);
- групповая ценность, сфокусированная на силе личности в малой группе людей с одинаковыми убеждениями, которые совершают террористическое насилие (романтизация магии сильной личности, которая готова поставить интересы группы выше всех своих жизненных интересов);
- соперничество разных групп ценностей (манипуляция тематикой: какая религия лучше и благороднее, какая религия более гуманна к своим последователям). Ради принадлежности к группе и получения групповой поддержки человек способен на куда более высокий уровень агрессии, чем в индивидуальной деятельности;
- манипуляция, связанная с отчуждением государственных институтов от индивидуальных жизненных ценностей (например, пропасть между богатыми и бедными или чиновник всегда враг, мешающий справедливости и т. д.).

В этой связи Интернет является особенно эффективным средством вербовки несовершеннолетних, так как они составляют значительную часть пользователей сети. Материалами для такой группы являются мультфильмы, видеоматериалы, а также компьютерные игры. В этих материалах используется тактика поощрения и прославления террористических актов.

Такого вида игры носят характер насилия в отношении государства. Предлагаемая награда за выполненную миссию и возможность игры на разных языках мира делают игры очень популярными, с большим количеством поклонников.

Радикализация. Это процесс, в результате которого у новобранцев меняется идеологическое представление жизни. Люди, которые подверглись радикализации, уже не считаются с иными точками зрения, только их взгляды истинны. Они полны решимости совершать террористические и насильственные действия.

В заключение считаем необходимым отметить, что в настоящее время информационные технологии Интернета играют важную роль в совершении террористических актов. Вербовка, радикализация и подстрекательство к терроризму могут рассматриваться как элементы в цепочке тесно связанных между собой явлений. Такие действия происходят благодаря сети Интернет, в том числе финансирование, планирование и снабжение. Существует огромное количество

способов вербовки людей и с каждым годом они становятся все более совершенными. Люди, сами того не замечая, попадают в сети злоумышленников, становясь исполнителями террористических актов.

В этой связи на первое место выходит информационная безопасность, когда люди или человек индивидуально, должен подумать и применить необходимые положения информационной защиты (безопасности), чтобы не попасть под контроль террористических и экстремистских организаций в сети Интернет.

Список литературы

1. Указ Президента Российской Федерации от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности».
2. Информация официального сайта МВД России [электронный портал]. URL: <https://мвд.рф/folder> (дата просмотра: 11.04.2022).
3. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (в действующей редакции).
4. Социально-психологические особенности террориста-смертника [электронный портал] URL: https://studref.com/487778/pravo/sotsialno_psihologicheskie_osobennosti_terrorista_smertnika (дата просмотра: 11.04.2022).
5. Способы использования сети Интернет террористическими структурами [электронный портал] URL: <https://www.gov.spb.ru/gov/otrasl/kmormp/protivodejstvie-terrorizmu-i-ekstremistskim-proyavleniyam/sposoby-ispolzovaniya-seti-internet-terroristicheskimi-strukturami/> (дата просмотра: 11.04.2022).
6. Как используют сеть Интернет экстремистские и террористические организации? [электронный портал] URL: https://internetpolicy.kg/literacymodule/course_2/module2/glava2_2.html (дата просмотра: 11.04.2022).
7. Методические рекомендации по противодействию идеологии экстремизма и терроризма в сети Интернет. URL: https://ksu.edu.ru/files/Svedeniya_ob_organisacii/ANTITERROR/antiterror-mr-v-seti-internet.pdf (дата просмотра: 11.04.2022).
8. Управление Организации Объединенных Наций по наркотикам и преступности «Использование Интернета в террористических целях» [электронный портал] URL: https://www.unodc.org/documents/terrorism/Publications/Use_of_Internet_for_Terrorist_Purposes/Use_of_the_internet_for_terrorist_purposes_Russian.pdf (дата просмотра: 11.04.2022).

Макарова Е. А.¹,

*слушатель факультета подготовки специалистов
в области информационной безопасности*

Московского университета МВД России имени В.Я. Кикотя

Научный руководитель:

Лустин В. И.,

старший преподаватель кафедры

информационной безопасности

учебно-научного комплекса информационных технологий

Московского университета МВД России имени В.Я. Кикотя

ИСПОЛЬЗОВАНИЕ СПЕЦИАЛЬНЫХ КЛЮЧЕВЫХ СЛОВ ДЛЯ ПОЛУЧЕНИЯ ОПЕРАТИВНО-ЗНАЧИМОЙ ИНФОРМАЦИИ ИЗ СОЦИАЛЬНЫХ СЕТЕЙ

Социальные сети – это огромный источник информации, в том числе и оперативно-значимой. Но назревает актуальный вопрос, как сотруднику правоохранительных органов возможно наиболее быстро и эффективно получить необходимую информацию? Данная информация может обеспечить установление обстоятельств совершенного преступления или установить данные о доказательствах.

Возрастает необходимость в реализации новых способов и методов предупреждения, пресечения, расследования и раскрытия преступлений как общеуголовной направленности (в том числе экономических, экологических, политических и т. д.), так и относительно новых видов преступлений в сфере компьютерной информации. А также отсутствие методики для сотрудников правоохранительных органов по поиску и сбору нужных данных в социальных сетях, которые имеют большое значение в их деятельности.

В ОСТМ УВД по СЗАО проведен анализ по мошенничествам, совершенным дистанционным способом за 9 месяцев 2021 г.

Все преступления, совершенные дистанционным способом, можно разделить на категории:

1) мошенничества с банковскими картами (под видом сотрудников банка или службы безопасности банка – 496 преступлений, списание средств со счета – 137 преступлений, оформление кредита с использованием подложных паспортных данных – 12 преступлений);

2) мошенничества с использованием фишинговых ссылок (273 преступления);

3) мошенничества с использованием интернет-сайтов (252 преступления и еще 40 преступлений с использованием «зеркал» популярных веб-сайтов);

4) мошенничества под видом представителей государственных служб (111 преступление, 16 – под видом сотрудников социальной защиты, 10 – под видом сотрудников пенсионного фонда России, еще 8 – под видом

¹ © Макарова Е. А., 2022.

представителей медицинских организаций, и 4 – под видом получения QR-кода о вакцинации);

5) мошенничества, совершаемые через социальные сети (200 преступлений);

6) мошенничества под видом брокерских сделок – 18 преступлений;

7) мошенничества с микрокредитными организациями – 10 преступлений;

8) мошенничества с получением полиса ОСАГО – 6 преступлений;

9) мошенничества под видом предоставления услуг турагенства – 3 преступления;

10) мошенничества под видом букмекерской компании – 3 преступления и др.

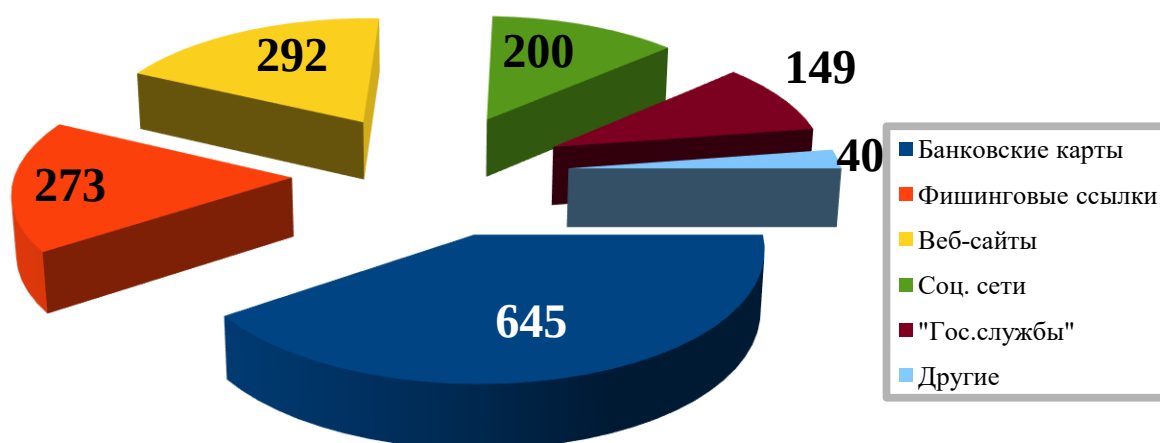


Рис. 1. Диаграмма 1. Категории преступлений, совершенных дистанционным способом

Из приведенной выше диаграммы следует, что самое большое количество мошенничеств, совершенных за 9 месяцев 2021 г. было совершено лицами, которые звонили гражданам и представлялись сотрудниками службы безопасности банков и просили предоставить информацию о картах или вкладах, впоследствии используя ее для перевода денежных средств на свои счета. Также занимают немалую долю от общего числа мошенничеств, совершенных дистанционным способом, преступления, совершаемые через Интернет, а именно: социальные сети и мессенджеры (Вконтакте, Телеграм, *Авито, *Юла, *Авто.ру).

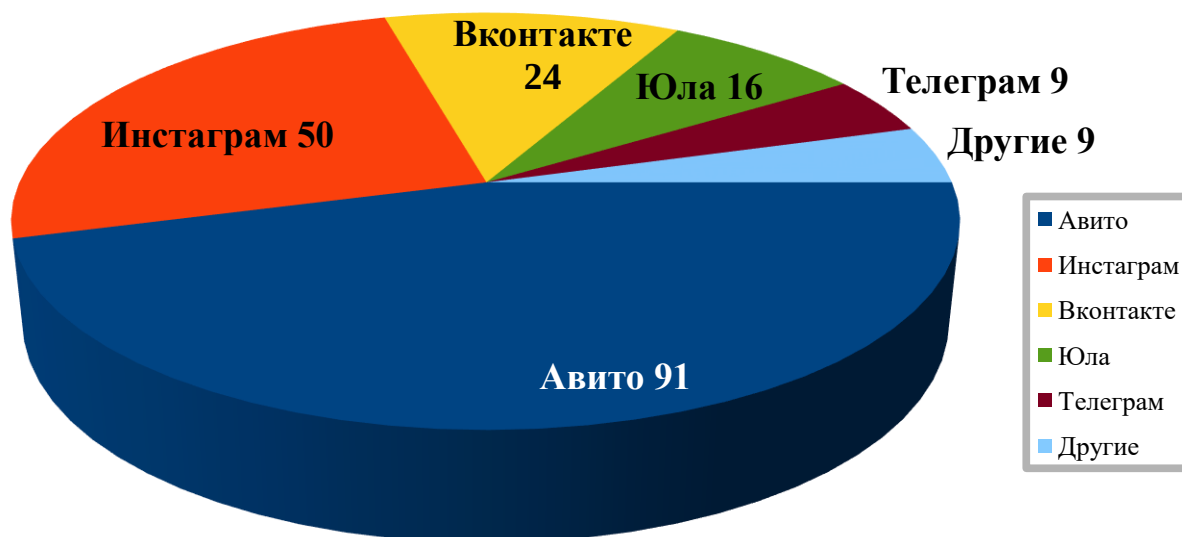


Рис. 2. Диаграмма 2. Распространенность преступлений, совершенных дистанционным способом, по социальным сетям и классифайдам

Вторая диаграмма показывает, что наибольшее количество мошенничеств в социальных сетях было совершено с использованием интернет-сервиса для размещения объявлений о товаре «Авито».

Приведенный анализ статистики преступности в социальных сетях свидетельствует о необходимости активного использования правоохранительными органами технических и технологических возможностей для сбора цифровых следов в сети Интернет.

Основная терминология, употребляемая мошенниками для совершения преступлений через социальные сети

В криминальном мире цифровых мошенников сложились свой сленг (жаргон), понятия и целые схемы взаимодействия с различными услугами, публикуемые на закрытых и даже вполне публичных тематических форумах.

Таким образом, мы собрали основную терминологию, употребляемую мошенниками для совершения преступлений через социальные сети.

Некоторые ключевые слова представлены ниже.

Скам (от англ. – «scam») – афера, мошенничество.

Тима/Проект – это команда, которая имеет фишинговые сайты для обмана доверчивых пользователей на доставку, где работают другие «воры, аферисты, скамеры». В состав проекта входит несколько людей.

ТС – это создатель проекта (мошеннической схемы).

Скамер – это аферист/вор, тот кто занимается обманом людей.

Вокеры – мошенники, которые соучаствуют в схеме по обману людей, например, назначают свидания жертвам через социальные сети и убеждают их забронировать место в досуговой организации путем внесения предоплаты, которая поступает на счета мошенников.

Саппорт – помощник по схеме обмана людей, например, мошенник, который создает фейковые сайты различных увеселительно-досуговых организаций (баров, кафе, кальянных, антикинотеатров и т. д.).

Кодер – это человек, занимающийся техчастью проекта.

Мамонт – жертва мошеннических действий.

Профит – это успешный обман / успешная оплата.

Возврат – это списание средств под видом «Возврата» у мамонта.

Возвратер / ТП – это человек, находящийся в чате технической поддержки на фишинг ссылках. Он помогает воркерам довести мамонта до оплаты.

Иксы – это когда у жертвы снимают несколько раз одну и ту же сумму с карты одновременно.

Фарминг (англ. «pharming») – это процедура скрытного перенаправления жертвы на ложный IP-адрес.

Доски – онлайн-классифайды (интернет-сервисы для размещения объявлений о товарах), например, Юла, Авито и т. д.

Оффлайн / онлайн – виды работы со схемой мошенничества:

- онлайн – работа в Интернете;
- оффлайн – в реальной жизни (предполагает физические передвижения, общение и т. п.).

Обнал – обналичивание денежных средств с карты путем снятия в банкомате.

Ордерить – заказывать товар в виртуальном магазине с использованием реквизитов банковской карты.

Стиллер (от англ. «to steal» – воровать) – программа/вирус, которая при ее запуске отправляет определенные файлы с компьютера, на котором была запущена, на компьютер, электронную почту или еще куда-нибудь распространителя этой программы.

Методические рекомендации по использованию ключевых слов в социальных сетях с целью поиска оперативно-значимой информации

Необходимо отметить, что при исследовании социальных сетей для получения какой-либо оперативно-значимой информации далеко не всегда имеется возможность использовать ведомственные или аттестованные программные средства, специализирующиеся на мониторинге социальных сетей.

На рисунке 3 показан пример поиска оперативно-значимой информации в мессенджере «Телеграм» по ключевому слову «Фрод». Найден чат на данную тему – «Antifrod». Несмотря на безобидное название, мы видим, что в данном чате обсуждаются и предлагаются предположительно незаконные услуги.

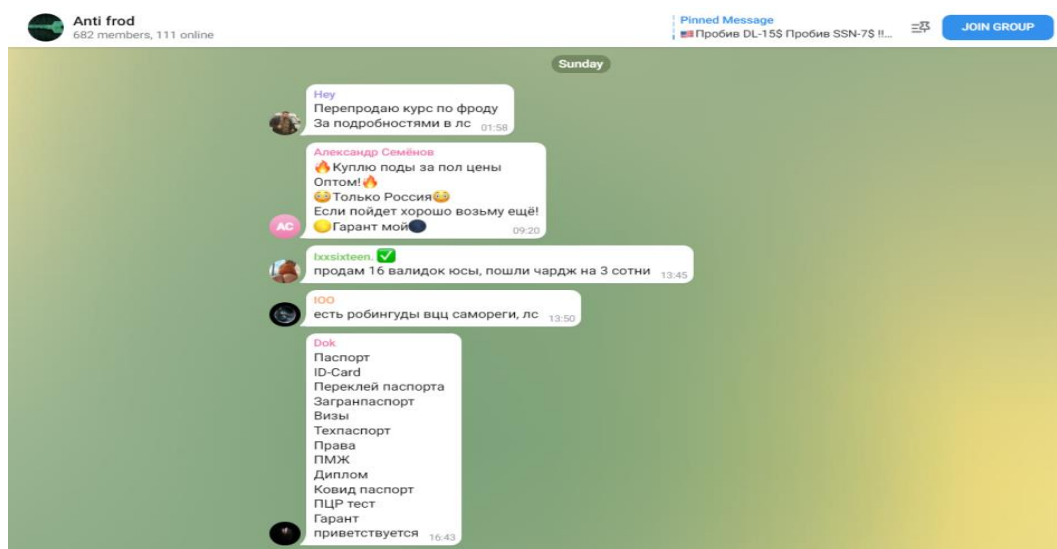


Рис. 3. Канал мессенджера «Телеграм»

Ниже тексты пользователей могут тоже вызвать оперативный интерес.

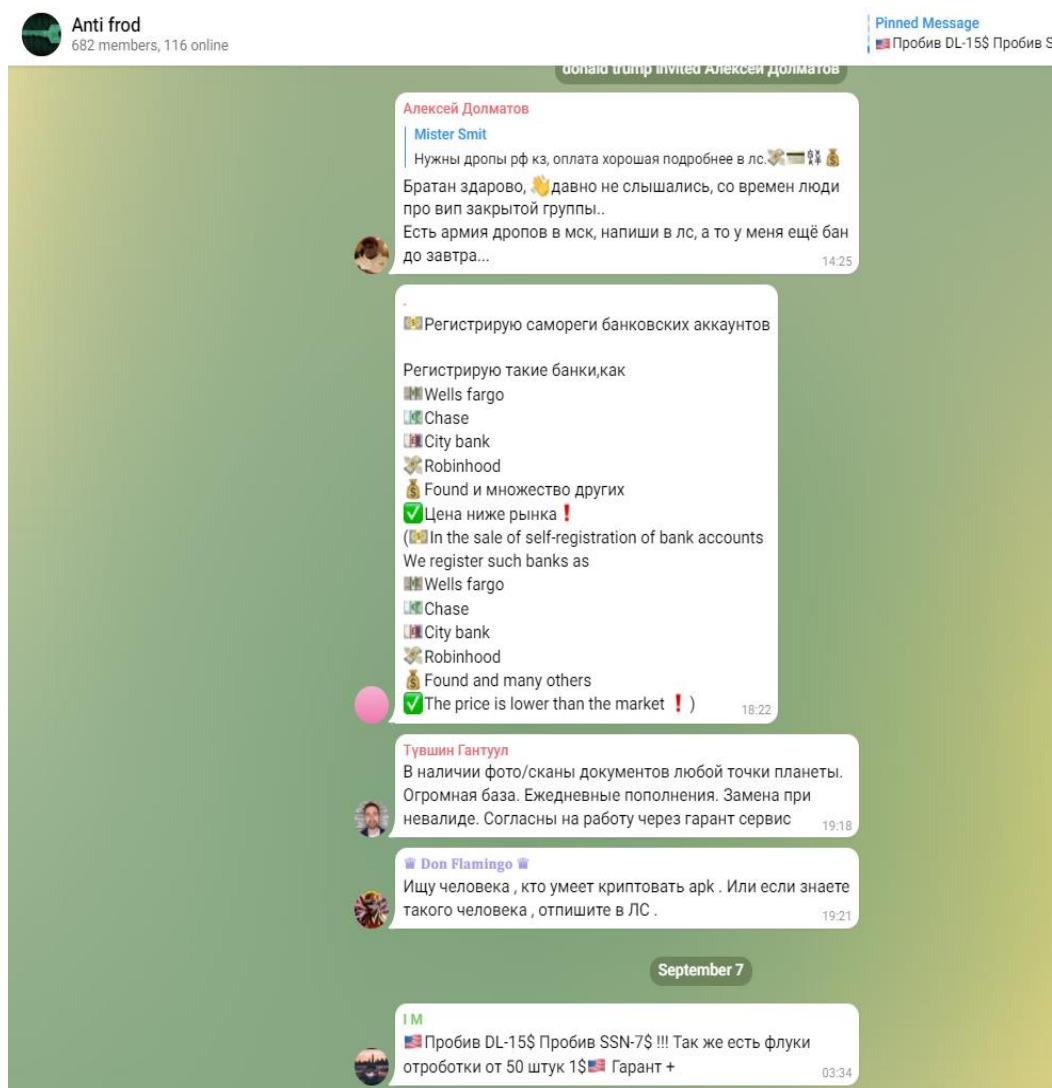


Рис. 4. Тексты пользователей на канале «Antifrod»

Далее найден Телеграм-канал по запросу «Стиллер».

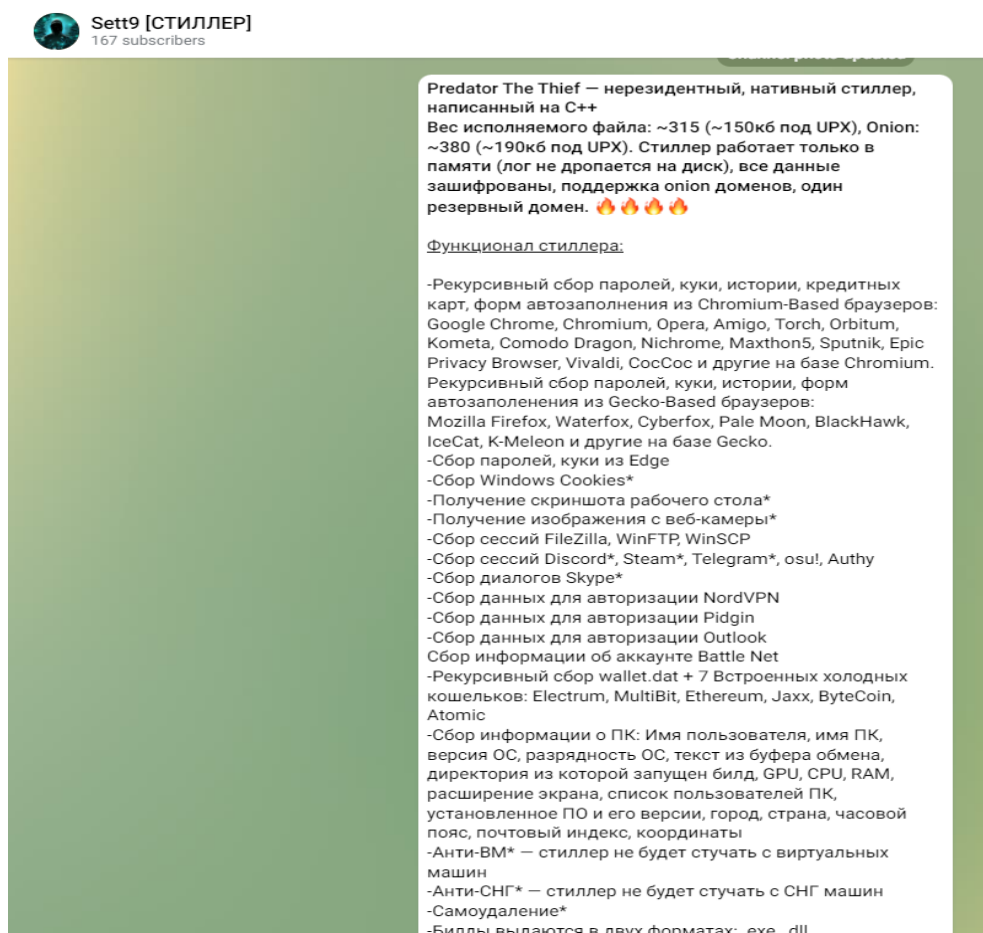


Рис. 5. Телеграм-канал по запросу «Стиллер»

Тут пользователь продает вирус, который при его запуске отправляет определенные файлы с компьютера, на котором был запущен, на компьютер, электронную почту или еще куда-нибудь распространителя этой программы. Функционал вируса описывает сам пользователь ниже (рис. 5).

Подобные действия могут быть классифицированы ст. 273 УК РФ «Создание, использование и распространение вредоносных компьютерных программ».

Далее на рисунке 6 результаты по такому же запросу («Стиллер») в социальной сети «ВКонтакте».

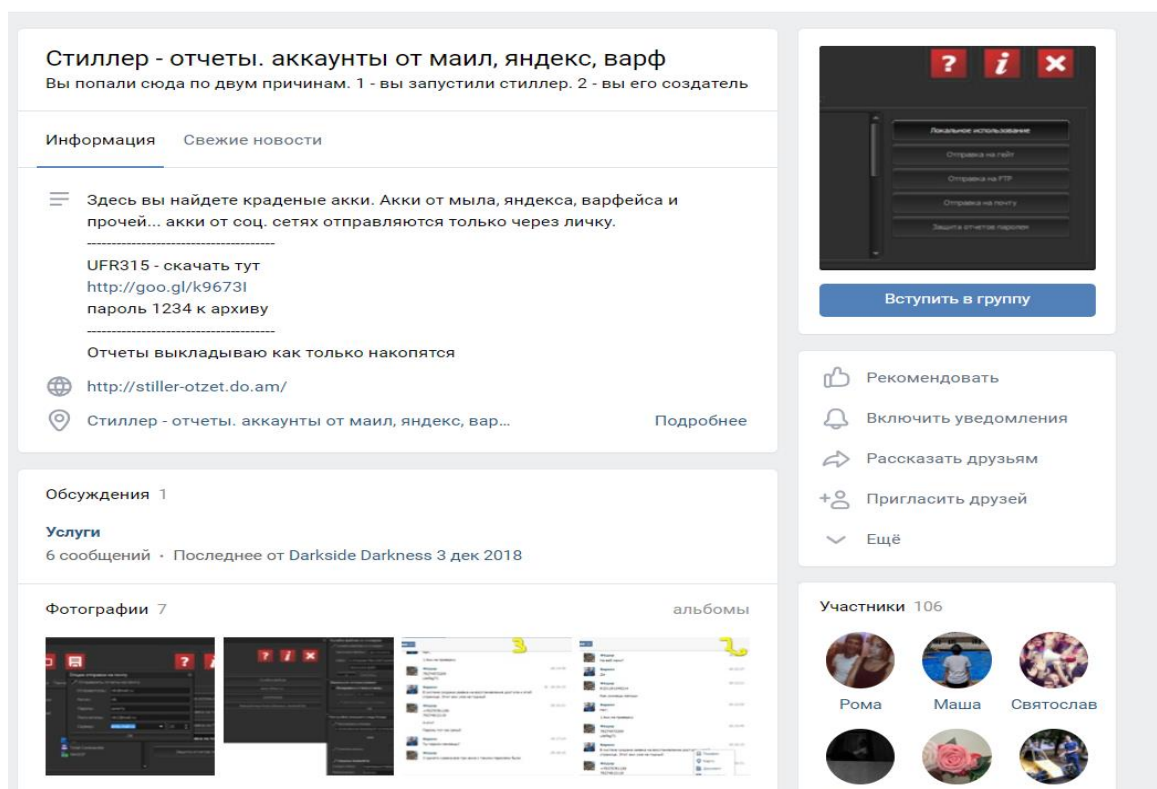


Рис. 6. Сообщество Вконтакте по запросу «Стиллер»

По информации на странице найденного сообщества, можно примерно судить о противоправных действиях его администратора и участников.

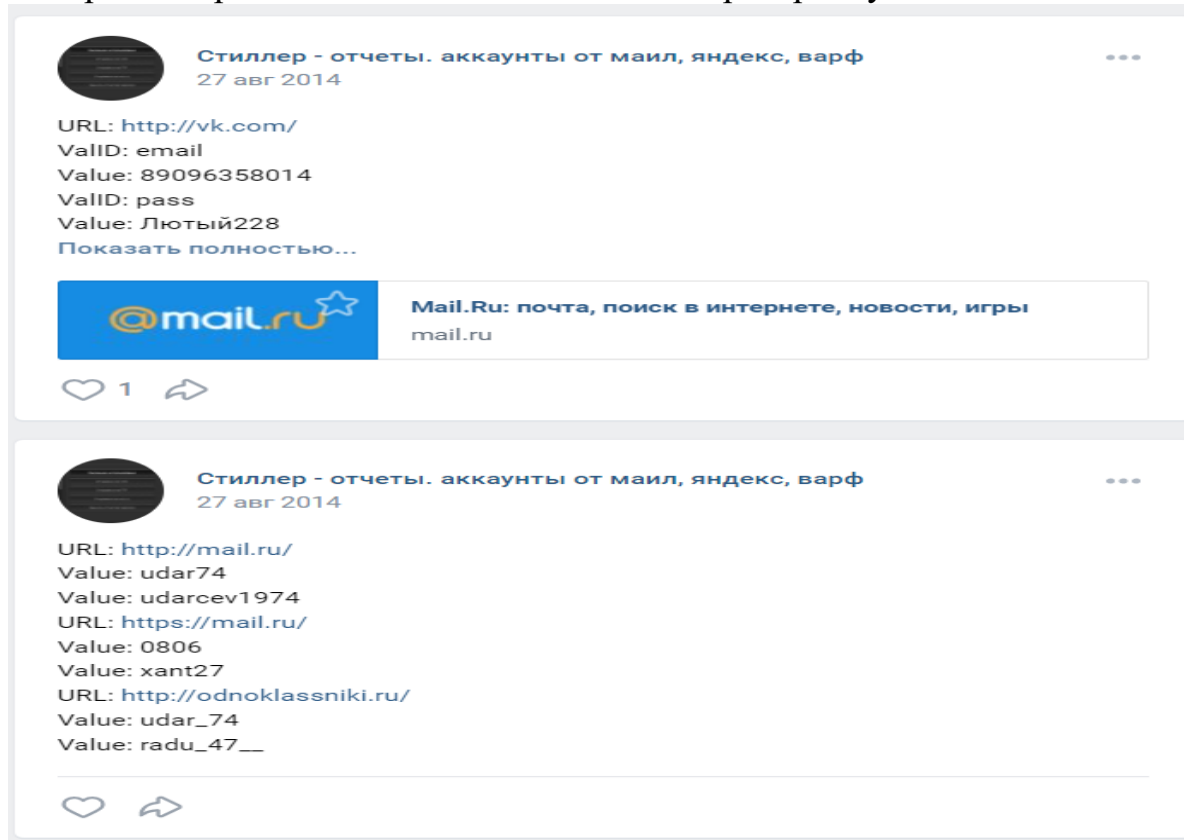


Рис. 7. Посты администрации сообщества Вконтакте

Здесь предлагается приобрести «краденный», т. е. взломанный аккаунт от электронной почты, социальной сети и т. п., что может быть квалифицировано по нескольким статьям Уголовного кодекса Российской Федерации.

Тактика дальнейших действий сотрудников правоохранительных органов по розыску лиц, совершивших преступления с использованием социальных сетей

Получив оперативно-значимую информацию сотруднику правоохранительных органов следует запросить у администрации социальной сети следующие сведения о пользователе/администраторе сообщества (Вконтакте) или канала (Телеграм):

- информацию о пользователе страницы социальной сети (ссылка на страницу): установочные данные, использованные им для регистрации, абонентские номера и электронные почты;
- IP-адреса, использованные для создания и доступа к странице за последние два месяца;
- аналогичную информацию по иным страницам социальной сети «Вконтакте» данного пользователя, установленных при анализе Cookie-файлов (данный пункт не запрашивается в случае взлома страницы потерпевшего или страниц его друзей).

Также сотруднику следует запросить информацию по банковской карте или электронному кошельку мошенника.

Таким образом, были разработаны методические рекомендации по использованию специальных ключевых слов в социальных сетях для получения оперативно-значимой информации, а также дополнительно был выявлен превентивный характер использования предложенных ключевых слов для мониторинга социальных сетей – возможность найти и заблокировать пользователей, сайты и сообщества, занимающихся незаконной деятельностью.

Список литературы

1. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 24.02.2021) // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_110699/ (дата обращения: 26.09.2021).

Миляев Г. А.¹,

курсант факультета подготовки

сотрудников в области информационной безопасности

Московского университета МВД России имени В.Я. Кикотя

Научный руководитель:

Лустин В. И.,

старший преподаватель кафедры информационной безопасности

Московского университета МВД России имени В.Я. Кикотя

ПРИМЕНЕНИЕ КОМПЬЮТЕРНОЙ ЭКСПЕРТИЗЫ ПРИ ПРОТИВОДЕЙСТВИИ ТЕРРОРИЗМУ

В настоящий момент общество все чаще сталкивается с террористическими проявлениями, в особенности с такими проявлениями в информационном пространстве, а также посредством использования информационных технологий. Данная категория преступников имеет в своем арсенале большой круг способов для таких незаконных проявлений как: завладение персональными данными, распространение персональных данных дискредитация органов государственной власти и органов местного самоуправления. Отдельно хочется сказать о дискредитации органов власти, ведь на данный момент совершается огромное количество «вбросов» ложной информации как лицами из-за рубежа, так и лицами на территории нашей страны, распространение фейков². Большинство таких преступлений совершается посредством использования информационных технологий, на что МВД России обращает пристальное внимание и быстро пресекает такие деяния.

Помимо этого, преступники имеют широкий спектр технологий для защиты собственных устройств, с которых совершаются преступные деяния, а также накопительных устройств, на которых хранится вся информация.

Когда преступник обнаружен правоохрнительными органами или в отношении него имеются веские причины полагать, что именно это лицо совершило преступление, то в отношении него проводятся мероприятия по пресечению противоправных деяний. Однако в таких ситуациях правоохрнительные органы не могут быть полностью уверены в виновности лица, потому что им нужны вещественные доказательства о виновности этого лица.

Для установления факта совершения преступления с применением информационных технологий правоохрнительные органы МВД России используют несколько видов компьютерной экспертизы³, которая помогает получить доступ и

¹ © Миляев Г. А., 2022.

² Фейк (от англ. «Fake») – что-либо ложное, недостоверное, выдаваемое за действительное с целью ввести в заблуждение.

³ Компьютерная экспертиза – широкое изучение компьютерной техники и электронных носителей информации на факт их участия в преступлении и имеющейся на них информации.

выявить, совершались ли преступные действия с данного конкретного устройства, а также получить полную информацию с накопительного устройства. Предлагаем рассмотреть основные виды экспертиз.

Информационно-компьютерная экспертиза

Данный вид экспертизы является довольно трудоемким процессом и заключается в полномасштабном изучении экспертом того: как хранятся данные на данном устройстве или носителе информации, каким способом организуется хранение данных. Также она включает в себя установление содержания закодированных файлов, типов файлов, истории действий за определенный период. В ходе проведения экспертизы можно узнать, есть ли на компьютере средства защиты от несанкционированного доступа и для каких файлов, какого содержания эти средства применяются, какие программные продукты и средства хранятся и используются на компьютере, каково их назначение. Эксперт может установить то, каков был изначальный вид данных и подробную информацию об их использовании. Помимо этого, информационно-компьютерная экспертиза позволяет установить связь между произошедшими событиями и определенными процессами, и действиями, совершенными на компьютере.

По результатам информационно-компьютерной экспертизы правоохранительные органы получают полное и широкое представление об информации на устройстве и на носителях информации, а также могут установить виновность подозреваемого лица. Однако по результатам можно определить, что с данного устройства были совершены противоправные деяния, но не подозреваемым лицом, а неким другим злоумышленником с помощью системы удаленного доступа, которую он мог специально внедрить в компьютер жертвы.

Компьютерно-сетевая экспертиза

Этот вид компьютерной экспертизы направлен на нахождение и комплексное изучение действий лица, совершенных в сети Интернет, а также на исследование информационных следов, которые оставил пользователь. В ходе данного компьютерного исследования эксперт изучает взаимодействие пользователя с сетью и то, какими информационными пакетами происходил обмен в сети и каким образом это было устроено. Помимо этого, в ходе компьютерно-сетевой экспертизы эксперт решает такие задачи, как накопители данных взаимодействовали с сетью. Ими могут быть как внешние, так и внутренние накопители данных. Однако основой уклон эксперта в данной ситуации направлен на изучение действий пользователя в сети, ведь чаще всего террористы и экстремисты совершают незаконное распространение вредоносных программных обеспечений, которые они могут использовать для неправомерного доступа к различному роду данных других пользователей сети или же шпионажа.

После завершения всего процесса компьютерно-сетевой экспертизы правоохранительные органы получают полный отчет о действиях лица, совершенных в сети, и могут дать правовую оценку действиям лица, а также использовать результаты этой экспертизы как доказательство виновности лица.

В заключении хотелось бы еще раз подчеркнуть актуальность проблемы терроризма и экстремизма в информационной среде в настоящее время. Борьба с

этим серьезным и довольно опасным видом преступности должна вестись по всем направлениям, и роль компьютерной экспертизы в этой борьбе является довольно высокой, так как может подтвердить или устранить виновность лица.

Список литературы

1. [Электронный портал] URL: <https://sudexpa.ru/expertises/kompiuterno-setevaia-ekspertiza/> (дата обращения: 25.04.2022).
2. [Электронный портал] URL: <https://rtmtech.ru/services/setevaya-ekspertiza/> (дата обращения: 25.04.2022).
3. [Электронный портал] URL: <https://sudexpa.ru/expertises/informatcionno-kompiuternaia-ekspertiza/> (дата обращения: 25.04.2022).
4. Федеральный закон от 31.05.2001 № 73-ФЗ «О государственной судебно-экспертной деятельности в Российской Федерации».

Гизатуллин М. Г.¹,

*начальник отдела по системам электронных коммуникаций, средств охранной и пожарной сигнализации АО «Уралтрансмаши»,
кандидат технических наук, доцент*

Копеина А. В.²,

*доцент кафедры информационного обеспечения
органов внутренних дел Уральского юридического
института МВД России*

НЕКОТОРЫЕ АСПЕКТЫ В ОБЛАСТИ РЕАЛИЗАЦИИ НАПРАВЛЕНИЯ ПРОФАЙЛИНГА ПОВЕДЕНИЯ СУБЪЕКТОВ НА РЕЖИМНЫХ ОБЪЕКТАХ

В рамках проводимого авторами исследования раскрывается достаточно актуальный и важный вопрос, в том числе в условиях нестабильной геополитической ситуации в мире, связанный с таким направлением, как профайлинг поведения субъектов в местах массового нахождения (скопления, пребывания) или транзитного передвижения людей. В данном случае речь может идти и о режимных объектах, относящихся к той или иной организации того или иного министерства или подведомственному ему агентства (МВД России, МЧС России, Минобороны России, Минюст России и т. д.).

Информационной базой в работе явились положения научной литературы ряда отечественных исследователей [1]–[4].

Ни для кого не секрет, что в современном обществе «бытует» такое понятие (направление), как профайлинг поведения субъектов, которые могут находиться в местах массового нахождения или транзитного передвижения людей.

Профайлинг поведения субъектов на объекте чаще всего реализуется специалистами, которые относятся, например, к службе охраны, службе безопасности или другим службам (далее – специалисты), осуществляющим свою служебную деятельность на каком-либо стратегически важном для общества объекте, который можно отчасти отнести к месту массового нахождения или транзитного передвижения людей. К таким объектам можно отнести «ключевые» объекты любого муниципального образования, например, метрополитен, автовокзал, железнодорожный вокзал, аэропорт и т. д.

К чему же сводится такое направление, как профайлинг поведения субъектов на объекте? Ответ на этот вопрос нам отчасти откроет такая научная область, как психология и педагогика. Профайлинг поведения субъектов на объекте сводится к тому, что специалисты осуществляют выявление субъектов – ряда лиц из всего «потока» лиц, которые могут быть потенциально или реально опасны для нашего общества, в частности, для всех людей, находящихся на этом объекте, его инфраструктуры и т. д.

¹ © Гизатуллин М. Г., 2022.

² © Копеина А. В., 2022.

К таким лицам можно отнести, например, лиц, у которых имеются «проблемы» с законом. Авторами сделан акцент на определенной категории лиц, которые могут быть причастны к ранее осуществленному ими террористическому акту либо осуществляющие его «проработку».

Если рассмотреть идеализированный вариант образа таких субъектов (лиц), то перед нами встает образ таких лиц с ярко или не особо ярко выраженными отклонениями в психологическом аспекте, внешнем облике, одежде, в области вербальных и невербальных составляющих и др.

Как правило, специалисты объекта имеют соответствующую подготовку по программе рассматриваемого в работе направления либо образование в области психологии и педагогики.

Данные специалисты осуществляют 24-часовой профайлинг поведения субъектов на объекте. Обязанности таких специалистов существенно отличаются от обязанностей сотрудников силовых ведомств, службы охраны, службы безопасности и других служб, реализующих свою деятельность на данном объекте. Деятельность специалистов является весьма важной для организации безопасности на объекте, ведь именно они могут определить (выявить, «просигнализировать») на ранней стадии тех или иных лиц, которые в дальнейшем могут создать потенциальную или реально существующую угрозу, например, жизни и/или здоровью людей на объекте.

Специалисты объекта отслеживают «поток» субъектов (лиц) в специализированных помещениях, где имеется аппаратно-программное обеспечение развернутой на объекте системы видеонаблюдения, позволяющей оценить реальную обстановку на объекте.

Специалисты подобны «фильтру» в области науки и техники, который определенным образом позволяет разграничить людей на категории:

- категория № 1 – «Интересен. Взять в разработку»;
- категория № 2 – «Интересен, но есть ряд сомнений. Взять в разработку»;
- категория № 3 – «Не интересен. Завершить анализ».

На входе «фильтра» представлены все лица, имеющие связь с объектом. На выходе «фильтра» представлено одно лицо или несколько лиц, внешние и поведенческие составляющие которых коренным образом отличаются от других лиц на объекте.

Специалистов также можно сравнить со «сканерами» в области науки и техники, которые идентифицируют и анализируют человека «с головы до ног» (мика, поведение, движения и/или неподвижность, одежда, взаимодействие с другими субъектами и др.).

Обратим внимание на те аспекты, которые специалисты в первую очередь берут во внимание. В качестве субъектов будем рассматривать лиц, которые входят в поле зрения специалистов с учетом первых двух категорий.

1. Субъект ведет себя подозрительно либо его поведение является отклонением от нормы («шкалы») согласно методике, по которой действует специалист. Субъект осуществляет фото и/или видеофиксацию, например, материально-технической базы объекта, его внешней и/или внутренней инфраструктуры, в том

числе делает записи в блокнот, ежедневник, на телефон и т. д. Если говорить об объектах, где фото и/или видеофиксация запрещена, субъект формирует какие-либо рисунки, чертежи, эскизы также, как и в первом случае, делает записи в блокнот, ежедневник, на телефон и т. д.

2. Субъект пытается получить информацию о системе безопасности на объекте (общественная безопасность, организация режима на объекте, информационная безопасность и т. д.), в том числе о том, как осуществляется смена работников.

3. Субъект в процессе нахождения на объекте невзначай вступает в диалог с другими субъектами на объекте, передает субъектам материальные объекты или принимает от них. Тоже относится к приему и/или передаче нематериальных объектов посредством технологий, использующих для приема/передачи электромагнитные волны на базе проводных и/или беспроводных технологий.

4. В случае, когда рассматривается своего рода «транзитный узел» между объектами или от объекта на «улицу» (и наоборот). Субъект ведет себя также достаточно подозрительно – осуществляет деятельность, несвязанную с продвижением, например, по данному «транзитному узлу».

5. Субъекта интересуют границы контролируемой зоны объекта, места для служебного пользования, организованные для работников объекта, доступ к которым ограничен.

6. Неоднократное посещение субъектом рассматриваемого им объекта с целью реализации его действий, отраженных в пп. 1–5.

7. Как правило, субъекты стремятся минимизировать взаимодействие не столько с сотрудниками силовых ведомств, службы охраны, службы безопасности и других служб, реализующих свою деятельность на данном объекте, сколько с инженерно-техническими средствами защиты объекта, обеспечивающими антитеррористическую защищенность объекта, например, с системой видеонаблюдения, развернутой на объекте.

Что касается эмоционального и иного состояния субъекта, то можно выделить ряд аспектов, на которые специалисты также обращают внимание.

1. На лице и/или открытых конечностях субъекта имеются следы потоотделения (если это возможно идентифицировать), при этом наблюдается постоянная умеренная температура, поддерживаемая на объекте.

2. Проявление «параноидального синдрома» о слежке с позиции анализа субъектом объекта.

3. Выраженное напряжение мышц лица, опорно-двигательного аппарата, переменная (переменно-постоянная, постоянная) дрожь конечностей субъекта.

4. Проявление субъектом повышенного внимания к средствам связи, часам на руке, часам, расположенным на объекте.

5. Выборочное взаимодействие субъекта (речь, мимика и т. д.) с субъектами, находящимися на объекте. Акцент субъекта сделан на пожилых людях, лицах с детьми, инвалидах. Минимизация взаимодействия субъекта с сотрудниками силовых ведомств, службы охраны, службы безопасности и других служб.

6. В результате повышенного потоотделения, субъект осуществляет вытирание, например, платком области лица, шеи, надкусывает ногти на руках и т. д. Кроме того, у субъекта могут проявляться агрессия, раздражительность, суета и т. д.

Специалисты делают акцент также на следующие составляющие:

1. Соответствует ли одежда субъекта сезону, имеет ли одежда несоответствия фигуре субъекта и т. д.

2. Субъект постоянно или периодически держит, например, руку в кармане, за пазухой.

3. Отклоняется ли от нормы манера передвижения субъекта согласно методике, по которой действует специалист.

4. Взгляд субъекта, чаще всего, леденящий. Зрачки субъекта имеют либо ярко выраженное расширение, либо сужение.

5. Проявляется ярко выраженная сбритая ранее область волосяного покрова головы, усов и т. д.

В условиях роста количества преступлений, совершаемых гражданами Российской Федерации, иностранными гражданами, лицами без гражданства, в том числе связанного с напряженной геополитической ситуацией в мире, такое направление, как реализация профайлинга поведения субъектов в местах массового нахождения (скопления, пребывания) или транзитного передвижения людей, становится «критическим». Данному направлению уделяется пристальное внимание, как с позиции объекта, так и с позиции, например, учредителя этого объекта, так как данное направление лежит в основе обеспечения противодействия потенциальным или реально существующим угрозам, например, жизни и/или здоровью людей на объекте.

Реализация профайлинга поведения субъектов на объектах должна быть также ориентирована практически и на все режимные объекты.

В качестве примера рассмотрим режимные объекты МВД России. К такому классу объектов можно отнести образовательные организации высшего образования системы МВД России, территориальные органы МВД России и т. д.

Для прохождения субъекта на такие объекты ему необходимо преодолеть так называемые системы физической защиты и антитеррористической защищенности (например, шлагбаум, турникет, система видеонаблюдения, система контроля и управления доступом, система охранной сигнализации и т. д.). Кроме того, субъекту необходимо преодолеть контрольно-пропускной пункт либо помещение, например, дежурной части, в которых несут службу личный состав образовательной организации высшего образования системы МВД России (постоянный и переменный состав), личный состав территориальных органов МВД России и т. д. В действительности личный состав рассматриваемых структур, находясь на суточном дежурстве, реализует свою служебную деятельность в соответствии с действующим законодательством Российской Федерации, локальными актами объекта (приказы, распоряжения, инструкции и т. д.), кроме того, проходит обучение по дополнительным профессиональным программам

(программам повышения квалификации) согласно выполняемым ими задачам на объекте.

Необходимость использования практики профайлинга поведения субъектов можно также рассмотреть:

- на примере деятельности органов внутренних дел Российской Федерации по охране общественного порядка и обеспечению общественной безопасности на публичных мероприятиях и т. д.;

- на примере деятельности сотрудников службы охраны, службы безопасности или других служб промышленных предприятий оборонно-промышленного комплекса Российской Федерации (заводы, фабрики и т. д.) по обеспечению безопасности режимного объекта.

На основании вышеизложенного материала нам представляется возможным, что, например, в образовательных организациях высшего образования системы МВД России может быть организована и реализована дополнительная профессиональная программа (программа повышения квалификации) в области направления профайлинга поведения субъектов на объектах, организованная для такой категории слушателей, как сотрудники органов внутренних дел Российской Федерации.

Список литературы

1. Душкин А. С., Нежкина Л. Ю. Содержание и технологии дисциплины «Профайлинг, методы выявления лиц, вынашивающих преступные замыслы» в образовательных организациях МВД России / А. С. Душкин, Л. Ю. Нежкина. Текст : электронный // Вестник Санкт-Петербургского университета МВД России. 2021. № 1 (89). С. 195–201. URL: https://www.elibrary.ru/download/elibrary_45542766_53969705.pdf (дата обращения: 16.04.2022).

2. Попова Д. А. Профайлинг и его развитие в современной гражданской авиации / Д. А. Попова. Текст : электронный // Академическая публицистика. 2021. № 2. С. 36–39. URL: https://www.elibrary.ru/download/elibrary_44744937_59622170.pdf (дата обращения: 16.04.2022).

3. Родин В. Ф., Красноштанова Н. Н. Профайлинг как метод разоблачения террористических намерений человека / В. Ф. Родин, Н. Н. Красноштанова. Текст : электронный // Вестник Московского университета МВД России. 2020. № 6. С. 318–322. URL: https://www.elibrary.ru/download/elibrary_44767429_99381692.pdf (дата обращения: 17.04.2022).

4. Рыбин Д. Н. Особенности обучения технологиям профайлинга сотрудников органов внутренних дел на факультете профессиональной подготовки / Д. Н. Рыбин. Текст : электронный // Вестник Барнаульского юридического института МВД России. 2021. № 1 (40). С. 167–169. URL: https://www.elibrary.ru/download/elibrary_46452289_63327309.pdf (дата обращения: 17.04.2022).

Очилов А. И.¹,

слушатель факультета подготовки

иностранных специалистов

Московского университета МВД России имени В.Я. Кикотя

Научный руководитель:

Плотников Г. Г.,

профессор кафедры информационной безопасности

учебно-научного комплекса информационных технологий

Московского университета МВД России имени В.Я. Кикотя,

кандидат технических наук

О ПРОБЛЕМЕ ФИНАНСИРОВАНИЯ ТЕРРОРИЗМА В СОЦИАЛЬНЫХ СЕТЯХ

Социальные сети на сегодняшний день стали неотъемлемой частью жизни человека. Для кого-то это место комфорта и изложения мыслей, для кого-то место для заработка и продвижения, а еще для кого-то социальные сети могут послужить поводом для новых знакомств и этот список можно перечислять долго. На сегодняшний день имеются сотни социальных сетей и самыми крупными из них являются Facebook, Instagram, VK, Tik-Tok, Odnoklassniki и др. Также помимо социальных сетей трудно представить жизнь людей без мессенджеров, самыми крупными мессенджерами на сегодняшний момент в Российской Федерации и во всем мире являются Whatsapp и Telegram, а также самый популярный медиа-сервис YouTube. Именно эти социальные сети и мессенджеры террористы выбрали, как площадку для вербовки, пропаганды и финансирования.

По статистике, за основу которой была взята региональная статистика по Российской Федерации Digital 2021, всего в Российской Федерации насчитывается около 99 млн пользователей соцсетей. Данный показатель больше на 4,8 млн, чем в начале прошлого года. При том, что 95,1 % (94,15 млн) пользователей предпочитают посещать соцсети с мобильных устройств. Для рабочих целей социальные сети используют 32 % пользователей.

Самой популярной социальной площадкой у россиян является YouTube, его посещают около 85 % пользователей в возрасте от 16 до 64 лет. ВКонтакте же посещают всего 78 % пользователей.

По данным Instagram на начало 2021 г., рекламная аудитория соцсети охватывает 45,8 % населения России старше 13 лет. Данный показатель на 3,7 % (2 млн пользователей) больше, чем в 2020 г. При этом 60,7 % пользователей Instagram в Российской Федерации составляют женщины, и всего лишь 39,3 % пользователей являются мужчины.

Стоит учесть, что резкое увеличение посетителей в социальных сетях очень сильно повлияла пандемия COVID-19.

Источники финансирования терроризма можно разделить на внешние и внутренние. К внешнему финансированию можно отнести пожертвование различных

¹ © Очилов А. И., 2022.

частных лиц или помощь иностранных спецслужб. Внутренними являются доходы, полученные за счет легальных и нелегальных источников (например, от предпринимательской деятельности).

До появления социальных сетей главную роль в финансировании терроризма играла помощь спецслужб. Но постепенно они вытеснялись благотворительными и неправительственными организациями, а также частными лицами.

В настоящее время деньги террористам поступают чаще всего небольшими суммами из многих источников. Террористы пользуются жалостливостью и доверием людей для финансирования своих рядов. Например, каждый из нас в социальных сетях хоть раз видел посты с изображением детей, нуждающихся в срочном лечении. Или же сборы средств людям, пострадавшим от каких-либо природных или техногенных бедствий. Поэтому рекомендуется совершать пожертвование через официальные сайты или странички благотворительных организаций, проверенных и зарегистрированных в Российской Федерации.

Существует огромное количество страниц и каналов в социальных сетях, содержащих религиозный контент. Контент у них может быть и незапрещенный и многие пользователи могут, сами того и не зная, профинансировать террористов.

Еще одним популярным способом является мошенничество. К данному способу можно отнести различные интернет-магазины, фейковые рассылки о розыгрышах и т. п. Всему виной опять-таки доверчивость и наивность пользователей. Но иногда интернет-мошенники настолько сильно входят в доверие людей, что не вызывают у них ни капли подозрения. Например, взломав аккаунт пользователя, они рассылают сообщение близким и знакомым с просьбой перевести им срочно деньги якобы на лечение тяжелой болезни и т. п. Поэтому рекомендуется удалять данные своих карт с переписок.

Выше были перечислены всего лишь несколько примеров из десятков видов финансирования терроризма. К сожалению, ежегодно они находят все новые способы.

Чтобы повысить эффективность усилий по борьбе с финансированием терроризма страны должны активнее обмениваться информацией служб финансовой разведки, а также повышать уровень координации между государственным и частным секторами. К сожалению, полностью перекрыть поток финансирования невозможно, но поспособствовать его ослаблению может каждый пользователь. Для этого достаточно соблюдать несколько базовых правил при посещении социальных сетей да и всего Интернета. Первое – никому не передавать данные своей карты, а если даже и передали, удалять их с чата. Второе – осуществлять благотворительность только через те организации, которые проверены и зарегистрированы государством. Третье и, наверное, одно из самых главных правил – не быть равнодушными. Если вы стали свидетелем интернет-мошенничества или же обнаружили подозрительные аккаунты, то немедленно сообщайте в администрацию социальной сети. Если каждый пользователь будет соблюдать вышеперечисленные элементарные правила, то он непременно внесет свой вклад в борьбу с терроризмом.

Список литературы

1. Жилина И. Ю. Финансирование терроризма (реферативный обзор). 2017. 03. 033-038.
2. Интернет и соцсети в России в 2021 году – вся статистика. URL: <https://www.web-canape.ru/business/internet-i-socseti-v-rossii-v-2021-godu-vsya-statistika/> // Обращение: 12.05.2022.

Рыжак В. А.¹,

адъюнкт факультета подготовки

научно-педагогических и научных кадров

Московского университета МВД России имени В.Я. Кикотя

ОТДЕЛЬНЫЕ АСПЕКТЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ В РАМКАХ СОДРУЖЕСТВА НЕЗАВИСИМЫХ ГОСУДАРСТВ ПО ПРОТИВОДЕЙСТВИЮ ТЕРРОРИЗМУ И ЭКСТРЕМИЗМУ В ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ

Терроризм любого происхождения и формы является неоправданным и непростительным преступлением, представляет собой чрезвычайную угрозу свободному обществу и правам каждого человека, государствам и мировому сообществу. После терактов в США 11 сентября 2001 г. международный терроризм вышел на новый уровень – произошло информирование всех государств об актуальности и интенсивности террористической угрозы, о важности борьбы с терроризмом и международного сотрудничества в этой области. Террористические акты отличаются преднамеренностью, осуществляются индивидуально и организованными группами, покушаясь на информационное пространство, действуя анонимно и открыто. Они способны вызвать настоящий системный кризис и подрыв деятельности органов государственной власти, международных организаций, нарушение сотрудничества связей. Цифровизация в повседневной жизни значительной части населения ускоряется, а преступники быстро и динамично адаптируют свой режим деятельности под формирующиеся новые условия.

На национальном и международном уровнях становится все труднее выявлять и предотвращать действия террористической направленности в цифровой среде. Одной из основных тенденций такой преступной деятельности в современном мире стало стремительное развитие террористическими организациями собственной информационно-пропагандистской инфраструктуры и использование современных информационно-коммуникационных технологий в целях дезорганизации нормального функционирования органов государственной власти, дестабилизации обстановки, демонстрации сил и возможностей террористов, пропаганды террористической идеологии и т. п. [1, с. 131]. Параллельно с этим происходит изменение форм и методов деятельности террористов. Среди них – осознанное привлечение к поддержке терроризма профессионалов со светским образованием (программистов, инженеров, врачей), а также молодежи, владеющей IT-технологиями и опытом работы в социальных сетях [2, с. 145].

Содружество Независимых Государств (далее – СНГ), как одна из региональных международных организаций, активно участвует во всех усилиях по противодействию терроризму, а также в одном из его ответвлений – непосредственно в вышеуказанной информационной сфере.

За все время существования СНГ было принято несколько важнейших документов, посвященных противодействию терроризму:

¹ © Рыжак В. А., 2022.

1) Концепция сотрудничества государств – участников СНГ в борьбе с терроризмом и иными насильственными проявлениями экстремизма (2005 г.);

2) Концепция формирования информационного пространства Содружества Независимых Государств (1996 г.);

3) Положение об Антитеррористическом центре государств – участников СНГ (2000 г.);

4) Положение о порядке организации и проведения совместных антитеррористических мероприятий на территориях государств – участников СНГ (2002 г.).

Данные документы могут рассматриваться как основы, необходимые для противодействия терроризму и экстремизму в информационном пространстве. Не следует забывать и о Модельном законе Содружества Независимых Государств «О противодействии терроризму» [3], а также Программе сотрудничества государств – участников Содружества Независимых Государств в борьбе с терроризмом и иными насильственными проявлениями экстремизма на 2020–2022 гг. Данная программа была специально разработана Антитеррористическим центром (далее АТЦ) государств – участников СНГ и непосредственно самими участниками Содружества в целях развития, совершенствования сотрудничества государств – членов и органов СНГ по борьбе с терроризмом (т. е. по пресечению и наказанию за уже состоявшееся преступное деяние, а также минимизации и ликвидации последствий проявлений терроризма, террористических атак) и иными насильственными проявлениями экстремизма.

В ней обозначены организационно-правовые и организационно-практические мероприятия, осуществляемая информационно-аналитическая деятельность и др., обязательные к исполнению всеми участниками СНГ для реализации поставленных задач. В части противодействия терроризму в информационной среде следует выделить наиболее важные пункты Программы, несущие практическую значимость:

1) п. 1.1.3, посвященный рекомендациям по совершенствованию законодательства государств – участников СНГ по направлениям и вопросам, касающимся проведения исследований информационных ресурсов;

2) п. 1.5.4, отвечающий за разработку, совершенствование правовых основ по информационному противодействию терроризму и иным насильственным проявлениям экстремизма, а также противодействие публикации материалов террористического и экстремистского характера;

3) п. 2.1.10, закрепляющий за собой мероприятия по идентификации и установлению лиц (групп лиц), применяющих различного рода технологии, в том числе и глобальной сети Интернет, в целях осуществления террористической и экстремистской деятельности;

4) п. 2.3, затрагивающий аспект работы компетентных органов государств – участников СНГ по укреплению безопасности информационного пространства, выраженное в совершенствовании их деятельности по выявлению, нейтрализации информационных, веб-ресурсов, террористических группировок.

Отдельного внимания заслуживает п. 2.1.7, в котором закреплено положение о «противодействии распространению идеологии терроризма и экстремизма, а

также подстрекательству к ним, публичным призывам к осуществлению террористической деятельности и оправданию терроризма, в том числе пресечение:

а) информационно-пропагандистской деятельности террористических и экстремистских организаций и ликвидация материально-технической базы такой деятельности;

б) распространения экстремистских материалов, в том числе с использованием современных информационно-телекоммуникационных технологий» [4].

Каждые несколько лет Программа корректируется и дополняется, что позволяет государствам – участникам СНГ осуществлять эффективную антитеррористическую деятельность на всех уровнях, применять более совершенные методы борьбы по данным направлениям.

Вызовы, создаваемые терроризмом, возрастают во всем мире и требуют немедленного реагирования. Действующие на международном уровне террористические организации и сети извлекают выгоду из процессов, происходящих в мире. Защита от текущих опасностей является ядром международной безопасности, и солидарность международного сообщества в противодействии терроризму и экстремизму дает о себе знать.

Так, 16 февраля 2022 г. в г. Москве в штаб-квартире Организации Договора о коллективной безопасности состоялось подписание Совместной позиции Региональной антитеррористической структуры Шанхайской организации сотрудничества, Антитеррористического центра государств – участников Содружества Независимых Государств и Секретариата Организации Договора о коллективной безопасности по вопросам противодействия терроризму и экстремизму [5]. В Совместной позиции Организации придали немаловажное значение противодействию использованию террористическими организациями сети Интернет в своих целях, что еще раз подчеркивает серьезные намерения участников вести полномасштабное противодействие терроризму в цифровом пространстве.

Компетентные органы СНГ во взаимодействии с такими авторитетными международными институтами, как Контртеррористическое управление ООН, соответствующие структуры ОБСЕ, ШОС, ОДКБ постоянно работают над совершенствованием своей деятельности и усилением координации предпринимаемых мер [6, с. 211]. Следует отметить, что их интенсивная работа оправдана и имеет существенное значение в связи с недавним предупреждением руководителя АТЦ СНГ «о нарастании активности экстремистских и террористических организаций в информационном пространстве, включая пропаганду, вербовку и сбор финансовых средств, также использование дезинформации» [7]. Последнее особенно легко сделать, а с развитием средств массовой информации и Интернета это стало намного проще, чем 20 лет назад.

Дополнительно подчеркнем, что ранее предпринятые меры государствами – членами СНГ по противодействию терроризму дают положительные результаты на практике. Специальные службы совместно с партнерами из пенитенциарных служб государств – участников СНГ ведут обширную кампанию, направленную на установление лиц и прекращение их террористической,

экстремистской деятельности, в особенности в информационной сфере. По итогам проведенных в 2021 г. операций «Трал-Антитеррор», «Идентификация» и «Розыск» компетентными органами государств – участников СНГ было задержано более 100 лиц, разыскиваемых за совершение преступлений террористического характера [8]. Здесь также важно более тесно согласовывать внешнюю политику стран Содружества по борьбе с терроризмом и экстремизмом, активно работать над унификацией антитеррористического законодательства и стандартов подготовки соответствующих специалистов.

Обобщая сказанное, необходимо отметить, что тщательно спланированные теракты продолжают демонстрировать повышенную угрозу для государств – участников СНГ. Своевременные организационно-правовые и практические мероприятия позволяют объединить усилия государств – членов СНГ, направленные на противодействие терроризму и экстремизму в различных сферах общества, в том числе в информационном пространстве, и добиться в этом высоких результатов. Результаты проведенного исследования вновь указывают на обязательное применение оптимизированного и скоординированного подходов, без которых невозможно дальнейшее укрепление потенциала компетентных органов СНГ на глобальном уровне.

Список литературы

1. Сидненко Г. Ф. Информационно-пропагандистская деятельность религиозных радикалов в сети «Интернет» как одна из угроз безопасности России в области информационного противодействия терроризму // Информационное противодействие терроризму и экстремизму в современных условиях : материалы международной конференции АТЦ СНГ (г. Москва, 10 февраля 2015 г.). М. : ОЛМА Медиа Групп, 2015. С.128–135.
2. Сидоренко Г. Ф. Информационное противодействие терроризму: политологический аспект / Г.Ф. Сидненко. М. : Изд-во Триумф, Лучшие книги, 2019.
3. Модельный закон «О противодействии терроризму». Принят постановлением Межпарламентской Ассамблеи государств – участников СНГ от 3 декабря 2009 г. № 33–18) // Информационный бюллетень Межпарламентской Ассамблеи государств – участников СНГ. 2010. № 46.
4. Программа сотрудничества государств – участников СНГ в борьбе с терроризмом и иными насильственными проявлениями экстремизма на 2020–2022 годы: утв. Решением Совета глав государств Содружества Независимых Государств о Программе сотрудничества государств – участников Содружества Независимых Государств в борьбе с терроризмом и иными насильственными проявлениями экстремизма на 2020–2022 годы от 11 октября 2019 г. [Электронный ресурс]. URL: <https://www.cisatc.org/1291/1334> (дата обращения: 03.04.2022).
5. Совместная позиция Региональной антитеррористической структуры ШОС, Антитеррористического центра государств – участников СНГ и Секретариата ОДКБ по вопросам противодействия терроризму и экстремизму [Электронный ресурс]. URL: <https://odkb-csto.org/documents/accepted-docs/> (дата обращения: 03.04.2022).

6. Сборник информационно-аналитических материалов «Развитие и деятельность Содружества Независимых Государств в 2021 году» (выпуск № 10), Исполнительный комитет СНГ, 2022.

7. Антитеррористический центр СНГ предупредил о наращивании активности экстремистов в информационном пространстве [Электронный ресурс]. URL: <https://www.belta.by/society/view/antiterroristicheskiy-tsentr-sng-predupredil-o-naraschivanii-aktivnosti-ekstremistov-v-488172-2022/> (дата обращения: 05.04.2022).

8. В СНГ фиксируют попытки экстремистских организаций усилить протестные настроения / Задержания за терроризм [Электронный ресурс]. URL: <https://tass.ru/mezhdunarodnaya-panorama/13935553> (дата обращения: 05.04.2022).

9. Каримов Р. Р., Каримова Г. Ю. Противодействие терроризму в рамках СНГ: нормативные и институциональные аспекты // Человек: преступление и наказание. 2016. №2 (93).

Серов И. С.¹,

курсант факультета подготовки специалистов

в области информационной безопасности

Московского университета МВД России имени В.Я. Кикотя

Научный руководитель:

Клочкова Е. Н.,

доцент кафедры специальных информационных технологий

учебно-научного комплекса информационных технологий

Московского университета МВД России имени В.Я. Кикотя

ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ РЕЛИГИОЗНОМУ ТЕРРОРИЗМУ В СЕТИ ИНТЕРНЕТ

Противодействие терроризму – это одно из первостепенных и приоритетных направлений по обеспечению национальной безопасности России.

В соответствии с Указом Президента Российской Федерации от 31 декабря 2015 г. № 683 «О Стратегии национальной безопасности Российской Федерации» к одному из главных факторов, наносящих вред государственной и общественной безопасности, относится организация террористической и экстремистской деятельности, а также организация мероприятий, связанных с осуществлением деятельности посредством использования информационных и коммуникационных технологий, носящих целью расширение и агитацию идеологии терроризма.

Актуальность данной статьи заключается в наличии многочисленной угрозы в области информации со стороны распространения идеологии терроризма и их организаций, которая развернулась в сети еще в 2015 г. во время начала глобальной агитации идеологии, передаваемой «Исламским государством» (ИГИЛ – террористической организацией, деятельность которой запрещена в Российской Федерации). Для привлечения граждан с целью организации данной деятельности и пропагандирования понятия и мировоззрения терроризма, наряду с формированием образа, привлекаемого террористическими организациями, последователи данных группировок прибегают к большинству используемых на данный момент социальных сетей и мессенджеров (WhatsApp, Telegram, Facebook, Twitter, Instagram, ВКонтакте, Одноклассники и др.) и другие возможные интернет-ресурсы, в том числе различные рассылки, посты, размещение фото-, аудио-, видео- и прочих мультимедийных материалов, добавление «активных» ссылок к комментариям и пр.

Религиозный терроризм – это самый опасный вид деятельности террористических организаций. Его отличительная черта заключается в том, что основой является колоссальная идеологическая идея, которая предоставляет возможности активного использования террористических форм и методов в разных социально-политических условиях и регионах. Но в то же время цель религиозного

¹ © Серов И. С., 2022.

терроризма сформулирована и не ясна, она затрагивает применение непонятной многим, сложной религиозной фразеологии.

В большинстве случаев религиозные террористы под своей деятельностью предполагают вести священную войну, уничтожить мировое зло (чаще всего в лицах США и стран Запада), осуществить исламскую революцию, создать теократическое государство и т. д.

В каждой религиозной традиции существуют знаки и облики насилия. Рассматривая хронологию формирования коллективных идентичностей, можно сделать вывод, что с пропагандой Библии в зарубежной культуре ее сюжет стал фундаментом, прежде всего, негативного восприятия этнической, религиозной и национальной тождественности ввиду того, что она формируется через противопоставление себя иному. Религии первоначально свойственно не только исключение, но и насилие: почитание единственному законному божеству предполагает выстраивание и оборону сакральных границ. Этому высказыванию следственно и иное: единобожие служит причиной недостатка ресурсов. В большинстве библейских сюжетах Бог есть не как бесконечно разрешающий, а как удерживающий и забирающий: блага и права, которые он вправе предоставить, приобретают не все. Недостаток ресурсов внедрен в Библию по принципу исключительности (одна земля, один человек, один народ) и в религиозном мышлении (одно Божество). Данная особенность создает призыв исключительной верности сообществу, в случае нарушения которой существует угроза насильственным отстранением. Трансляция этого образа в светские формы провоцирует не столько безопасность, сколько угрозу.

К одному из опасных с точки зрения проявления взаимосвязи религии и религиозного терроризма относится то, что спекулятивное применение религиозной идеологии в системе религиозного терроризма способно обеспечить легитимацию, т.е. возможность применения насилия религиозными предписаниями законно. Использование насилия в структуре террористической деятельности и их участников признается ими как божественная необходимость или священное деяние. Наделение насильственной деятельности священным смыслом связано с эксплуатацией унижающих человеческое достоинство понятий («слабые», «собаки», «дети сатаны»). Вдобавок к этому поддержка со стороны государства религиозного терроризма оказывается обычной практикой в деятельности несчетного количества зарубежных государств, стремящихся применить террористическую деятельность для осуществления собственных внешнеполитических намерений.

Религиозный терроризм в сети Интернет – устойчивое словосочетание, под которым следует понимать совершение таких действий, которые способны убедить, распространить и внедрить идею террористических организаций. Целью данной деятельности является распространение паники в обществе, отвлечение правоохранительных органов от возможного совершающегося в данный момент террористического акта.

В январе – феврале 2022 г. зарегистрировано 79,7 тыс. преступлений, совершенных с использованием информационно-телекоммуникационных технологий

или в сфере компьютерной информации. В общем числе зарегистрированных преступлений их удельный вес остался на уровне января – февраля 2021 г. и составил 26,3 %. Всего преступлений террористического характера на территории Российской Федерации было зарегистрировано 302, раскрыто из них – 160.

Совсем в недавнем прошлом истории России терроризм воспринимался в качестве происшествия, которое поражает своей жестокостью. События последующих лет, самым громким из которых стал распад СССР, привели к деформации таких понятий, как мораль, право, общественный порядок и общественная безопасность. На сегодняшний день, миновав Холодную войну, существующий мир подвергается воздействию новой эпохи – эпохи информационных противоборств и войн. В отличие от традиционных понятий о вооружении в информационном пространстве средства противоборства могут применяться и в мирное время. Особенность использования этих средств заключается в том, что они способны быть доступны не только государству, но и террористическим организациям, в том числе отдельным лицам.

Пример осуществления деятельности религиозного терроризма являет собой террористический акт на Дубровке в Москве. 23 октября 2002 г. Чеченские террористы взяли в плен граждан (зрителей, работников и актеров мюзикла «НордОст») в помещении театрального центра. В контртеррористической операции 26 октября 2002 г. были элиминированы все участники, а также эмансипировано подавляющее большинство заложников, из которых 130 граждан умерли.

Кроме того, к примеру проявления религиозного терроризма, необходимо отнести происшествие в метрополитене в Санкт-Петербурге. 3 апреля 2017 г. террорист-смертник произвел разрыв взрывного устройства на остановке между станциями «Сенная площадь» и «Технологический институт». Вследствие теракта пострадали около 100 человек, 16 из которых погибли (в том числе лицо, осуществившее теракт).

Интернет служит наиболее доступным ресурсом для трансляции пропаганды терроризма ввиду его доступности и не успевающего надзора со стороны власти. Отсюда следует рост в сети в последние годы в геометрических прогрессиях экстремистско-террористических материалов, что порождает и рост числа потребителей данного вида информации, которые впоследствии могут пополнить ряды приверженцев данной деструктивной идеологии.

В Интернете функционирует целая система ресурсов, которая ориентирована на обработку идеологии и обучение методам и способам совершения террористической деятельности, в данном контексте оказывая влияние на социально-политическое развитие страны и общества.

С одной точки зрения, Интернет способствует развитию потенциала личности через обучающие программы, телевидение, информационные потенциалы и СМИ. С другой точки зрения, развитие информационно-коммуникационных систем приводит к появлению новых способов совершения преступлений, которые отражаются в общем количестве преступлений Российской Федерации и являются более сложными с точки зрения их обнаружения и раскрытия.

Учитывая активную борьбу мирового сообщества с терроризмом и развитие новых информационных технологий, террористические организации все больше предпочитают проявлять свою деятельность в сети, используя при этом информационно-коммуникационные системы как среду, реализующую свои идеи, цели и задачи.

Вред, наносимый деятельностью террористов, распространяющих свою идеологию в сети, наносит вред не только конкретным пользователям, людям, но и государству, при этом угрожая интересам национальной безопасности страны.

Здесь следует отметить существующие проблемы в направлении противодействия террористической деятельности:

1. Отсутствие единого нормативного правового акта в области международного сотрудничества, регулирующего сотрудничество правительств в сфере противодействия идеологии терроризма в Глобальной сети.

2. Недостаточно проработанная база уголовного законодательства в указанной выше области.

3. Использование аппаратного оборудования, при помощи которого возможно реализовывать террористическую идеологию.

Решением указанных проблем может стать:

1. Инициирование принятия Конвенции по борьбе с терроризмом посредством Всемирной сети, целью которой признать сотрудничество по части противодействия распространения идеологии терроризма в глобальном информационном пространстве.

2. Изменение Уголовного кодекса Российской Федерации в области утверждения прав, обязанностей и ответственности пользователей Всемирной сети на территории России. К примеру, обозначить следующую редакцию статьи: «... те же деяния, которые были совершены посредством применения средств сетей Интернет».

3. Ужесточение характера административных санкций, среди которых можно выделить ст. 19.12 «Передача либо попытка передачи запрещенных предметов лицам, содержащимся в учреждениях уголовно-исполнительной системы или изоляторах временного содержания» Кодекса Российской Федерации об административных правонарушениях.

Список литературы

1. Билык В. И. Противодействие идеологии терроризма и экстремизма в сети Интернет / В. И. Билык, Павел Билык // Пробелы в российском законодательстве. 2016. № 4. С. 270–273. URL: <https://rucont.ru/efd/563357> (дата обращения: 12.04.2022).

2. Профилактические меры противодействия религиозному экстремизму. URL: <https://wiselawyer.ru/poleznoe/18475-profilakticheskie-mery-protivodejstviya-religioznomu-ehkstremizmu> (дата обращения: 12.04.2022).

3. Методические рекомендации по противодействию идеологии экстремизма и терроризма в сети Интернет. Костромской государственный университет. URL: https://ksu.edu.ru/files/Svedeniya_ob_organisacii/ANTITERROR/antiterror-mr-v-seti-internet.pdf (дата обращения: 12.04.2022).

Ситников А. А.¹,

курсант факультета подготовки специалистов

в области информационной безопасности

Московского университета МВД России имени В.Я. Кикотя

Научный руководитель:

Клочкова Е. Н.,

доцент кафедры специальных информационных

технологий учебно-научного комплекса информационных технологий

Московского университета МВД России имени В.Я. Кикотя

ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЕ ПРОЯВЛЕНИЕ ЭКСТРЕМИСТСКОЙ ДЕЯТЕЛЬНОСТИ В СОЦИАЛЬНЫХ СЕТЯХ

Последние годы все активнее протекают процессы глобализации и информатизации, при этом растут потребности человечества в коммуникации, доступности технологий и увеличении скорости обмена сообщениями. Все это в свою очередь, так или иначе оказывает влияние на изменение социально-психологической сферы жизни. На сегодняшний день согласно опросам, проводимым «Лабораторией Касперского», россияне в среднем проводят в социальных сетях около трех часов ежедневно [1], просматривая контент и общаясь с друзьями. Распространение новой вирусной инфекции в последние два года также способствовало увеличению количества активных пользователей, а также росту времени, проводимому в сети. При этом наиболее активными пользователями являются молодые люди, подростки, которые проводят в сети зачастую значительно больше времени, чем среднестатистический россиянин.

Отличительной особенностью данной категории пользователей является то, что они еще в силу своих знаний, опыта, возраста не обладают способностью критического анализа получаемой через сеть Интернет информации, иногда наносящей деструктивный характер. Объем ресурсов, циркулирующих в сети, ежегодно увеличивается в геометрической прогрессии, при этом возникает ситуация, когда уполномоченные органы далеко не всегда имеют возможность осуществлять фильтрацию данных для конечного пользователя.

Наиболее распространенными площадками в русскоязычном сегменте сети до настоящего времени были Instagram, ВКонтакте и Youtube, но в последние месяцы начали набирать популярность такие социальные сети, как Telegram, TikTok и Twitter. На рисунке 1 представлена диаграмма процентного соотношения названных выше площадок, а также других ресурсов.

¹ © Ситников А. А., 2022.

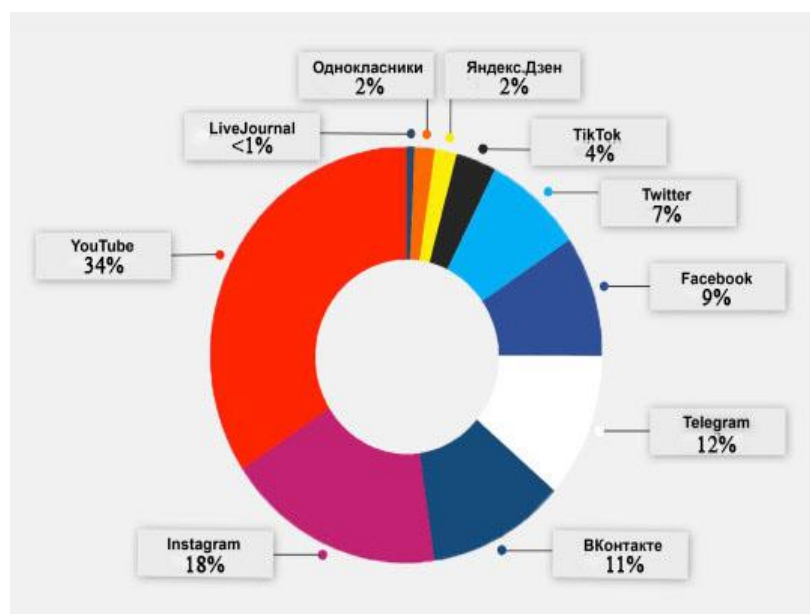


Рис. 1. Диаграмма популярности соцсетей

Использование социальных сетей позволяет поддерживать контакты пользователям, находящимся на расстоянии друг от друга (в разных городах, странах), делая их ближе. Но в то же время практика показывает, что социальные сети применяются не только для простого общения, для которого они были изначально созданы, но их стали очень активно использовать в противоправной деятельности различные экстремистские и террористические организации. Имея возможность действовать в ряде случаев анонимно, преступные группы с помощью социальных сетей продвигают радикальные взгляды и вербуют новых членов. И как мы уже отметили, самой незащищенной, подверженной особому риску становится молодежь, которая и становится главной целью противоправной деятельности.

Статистика показывает, что возраст четырех из пяти лиц, совершивших различного рода преступления экстремистской направленности, составляет менее 30 лет [2]. Нередко членами преступных групп, действующих из материальных побуждений, становятся подростки 14–18 лет. Как правило, эти лица являются выходцами из маргинальных слоев общества, не имеют источника постоянного дохода, занимаются неквалифицированным трудом или подработкой на биржах фриланса. Занимаясь самопиаром в социальных сетях, они проявляют потенциальную открытость для налаживания диалога с кураторами и пропагандистами, ведущего к последующему привлечению к противоправной деятельности.

Лица, действующие из идеологических побуждений, имеют совершенно иную криминологическую характеристику. Это люди среднего класса, возраст в пределах 35–45 лет. Психоэмоционально они проявляют замкнутость, низкое правосознание, нигилизм общественных ценностей. В силу использования информационных технологий в рамках своей противоправной деятельности, данные лица либо имеют соответствующее образование, либо явный интерес к данной области.

Мотивирующими факторами для молодых людей могут стать материальная или идеологическая составляющая, или даже просто проявление интереса к

принципиально новому виду активной опасной деятельности. Изначально любая мотивация разделяется на личную и групповую. Личная мотивация обычно связана с желаниями, целью конкретного человека. Социальные сети, предоставляя широкие возможности удаленного построения организаций и групп, позволяют так называемым «кураторам» оказывать негативное влияние на аудиторию. Под таким воздействием личная мотивация молодых людей постепенно изменяется на групповую. В итоге все это может приводить к постановке новых целей и постепенному уходу от старых, к возникновению проблем неконтролируемого обмена мнениями, знаниями и опытом преступной деятельности в разных сферах, а также к призыву отдельными участниками сообщества к участию в активных проявлениях противоправной деятельности. Последние события на Украине показывают актуальность данной проблемы и необходимость постоянного мониторинга, контроля, автоматизированного обнаружения экстремистских профилей, а также открытых чатов, сообществ и групп в социальных сетях.

Рассматривая любую сеть, как платформу для предоставления фейковой информации широкому кругу заинтересованных лиц и обмена сообщениями, содержащими экстремистские материалы, выделим некоторые особенности, существенно влияющие на информационно-психологическое противоборство:

- огромный объем данных, осложняющий своевременную обработку и оперативное реагирование;
- география расположения пользователей, а также офисов компаний, оказывающая влияние на юрисдикцию;
- использование пользователями социальных сетей средств анонимизации, затрудняющих определение конечного лица или группы лиц, совершающих противоправное деяние;
- неограниченность распространения различного рода информации и доступа к ознакомлению с ней, затрудняющая локализацию опубликованных данных;
- неочевидная форма представления данных, оказывающая влияние на время фиксации и признания материалов экстремистскими.

За последний 2021 г. количество выявленных уголовно наказуемых деяний экстремистской направленности выросло по сравнению с предыдущим годом с 833 до 1057. При этом значительная часть преступлений была связана с публичными призывами к осуществлению экстремистской деятельности (+32,4 %, 486) и больше половины (456) совершено с использованием глобальной сети Интернет. Сотрудники правоохранительных органов активно работают в данном направлении. На рисунке 2 представлена диаграмма, отражающая число зарегистрированных противоправных деяний по федеральным округам.

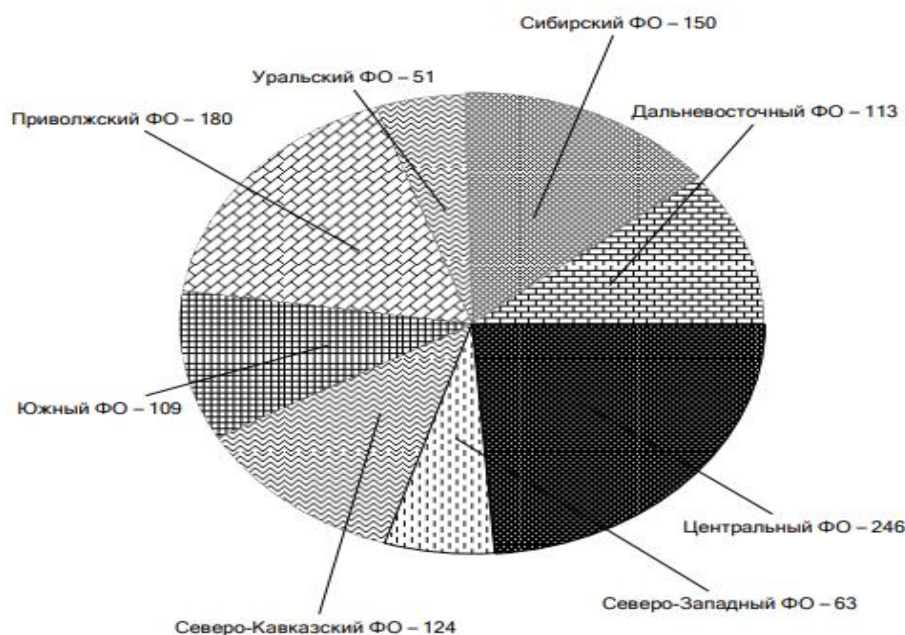


Рис. 2. Диаграмма сведений о зарегистрированных преступлениях экстремистской направленности

Исходя из динамики прошедшего года, а также в свете последних событий следует вывод о том, что ожидается рост преступных деяний в данной сфере. Стоит отметить должную законодательную реакцию на быстрое изменение ситуации в стране. Так 4 марта 2022 г. вступил в законную силу Федеральный закон № 32-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и статьи 31 и 151 Уголовно-процессуального кодекса Российской Федерации». Особенно интересной в силу информационно-психологического противоборства является ст. 280.3, диспозиция которой составлена следующим образом: «Публичные действия, направленные на дискредитацию использования Вооруженных Сил Российской Федерации в целях защиты интересов Российской Федерации и ее граждан, поддержания международного мира и безопасности».

На сегодняшний день можно предложить два основных решения обозначенных выше проблем. Это блокирование запрещенного контента с помощью использования специализированного программного обеспечения, а также методов, встроенных в информационную структуру компании, с дальнейшим надлежащим реагированием и передачей правоохранительным органам на предмет рассмотрения вопроса привлечения лица, имеющего прямое или косвенное отношение к опубликованному противозаконному контенту, к административной или уголовной ответственности. Данное решение является эффективным, но, к сожалению, на данный момент не все социальные сети готовы предоставить такую возможность, некоторые открыто поддерживают проявление экстремистской направленности и радикальные взгляды по отношению к нашему государству и гражданам. Следует наладить организационное и правовое взаимодействие или ограничить присутствие продуктов компании на территории Российской Федерации.

Второе решение, по мнению автора статьи, имеется возможность реализовать в рамках осуществления такого важного направления деятельности полиции, как

предупреждение преступлений и административных правонарушений. Создание отдельного подразделения, занимающегося вопросами формирования общественного мнения, противодействия «фейкам», а также качественным информированием пользователей достоверной информацией, что в перспективе повлечет за собой дестабилизацию организации экстремистских сообществ и вовлечения новых членов. Пункт 11 ст. 57 «Стратегии национальной безопасности Российской Федерации» прямо указывает на решение задач «противодействия использованию информационной инфраструктуры Российской Федерации экстремистскими и террористическими организациями, специальными службами и пропагандистскими структурами иностранных государств для осуществления деструктивного информационного воздействия на граждан и общество» [3].

Список литературы

1. Лаборатория Касперского «Опрос компании Opinium о среднем времени, проведенном в социальных сетях». URL: https://www.kaspersky.ru/about/press-releases/2021_laboratoriya-kasperskogo-rossiyane-provodyat-v-socialnyh-setyah-v-srednem-tri-chasa-v-den (дата обращения: 05.04.2022).
2. Портал правовой статистики Генеральной прокуратуры Российской Федерации. URL: <http://crimestat.ru/analytics> (дата обращения: 05.04.2022).
3. Официальный интернет портал правовой информации. URL: <http://publication.pravo.gov.ru/Document/View/0001202203040007?index=2&rangeSize=1> (дата обращения: 05.04.2022).
4. Центральный Административный Округ города Москвы «Особенности профилактики и борьбы с проявлениями экстремизма и терроризма в молодежной среде». URL: <https://cao.mos.ru/counteringextremism/features-for-the-prevention-and-suppression-of-manifestations-ofextremism-and-terrorism-in-the-yout/> (дата обращения: 05.04.2022).

Скворцов П. Д.¹,

*командир отделения факультета подготовки специалистов
в области информационной безопасности
Московского университета МВД России имени В.Я. Кикотя*

Научный руководитель:

Клочкова Е. Н.,

*доцент кафедры специальных информационных технологий
учебно-научного комплекса информационных технологий
Московского университета МВД России имени В.Я. Кикотя*

МЕТОДИКА ПОИСКА ИНФОРМАЦИИ ТЕРРОРИСТИЧЕСКОЙ И ЭКСТРЕМИСТСКОЙ НАПРАВЛЕННОСТИ В СЕТИ ИНТЕРНЕТ

Интернет является основным ресурсом получения информации современной молодежью. Учитывая данную тенденцию, различные экстремистские и террористические группировки размещают противоправный контент в глобальной информационной среде. Сложная геополитическая ситуация привела к тому, что все больше ресурсов размещают на своих страницах данные экстремистской направленности, пропагандирующие насилие. В последние месяцы эта проблема стала еще более острой и, несмотря на то, что Роскомнадзор блокирует такие интернет-ресурсы, масштаб проблемы не становится меньше.

Рассмотрим, что же такое экстремизм в современном мире. Экстремизм – это приверженность крайним взглядам и способам действий, что означает участие в террористических акциях. Основными сущностями рассматриваемой проблемы являются экстремистские материалы. Призыв к экстремистской деятельности может принимать любые формы, от печатной до аудио и визуальной. Еще одним немаловажным фактором является то, что распространители такой информации зачастую не действуют по шаблону, а каждый раз выбирают новые способы для достижения своих целей. И с увеличением доступности сети Интернет, информационных технологий они также увеличивают свое присутствие в этом медиапространстве, увеличивая количество и качество публикуемого материала. И если некоторое время назад владельцы социальных сетей хотя бы формально придерживались политики о запрете противоправного контента, то сегодня многие даже не делают вид, что у них существуют такие запреты.

Для подтверждения данного тезиса можно вспомнить недавний случай с организацией Meta, которая является владельцем таких популярных ресурсов, как Instagram и Facebook. Данные ресурсы на территории Российской Федерации были признаны экстремистскими. Предпосылкой для этого стало решение Meta от 11 марта 2022 г. Американская компания официально разрешила размещать в сети информацию с призывами к насилию над русскими военными.

Другая проблема связана с тем, что блокировка ресурса, далеко не всегда позволяет защитить пользователей сети от противоправного контента. Блокировка приводит к тому, что посетители не имеют доступа к конкретному ресурсу, но

¹ © Скворцов П. Д., 2022.

информация о пользователях продолжает оставаться у владельца, который имеет возможность распространять эти данные на разных платформах, создавать резервные копии сообществ и учетных записей. Фактически предоставляя идеологам террористических и экстремистских сайтов быстро перенаправлять незаконный контент и поддерживать основную базу подписчиков.

Одним из способов решения рассмотренных выше проблем является, как мы уже отметили, поиск такого противоправного контента. И здесь самое трудное как раз и оказывается найти его среди огромного числа достоверной, законной информации. В качестве примера решения данной задачи можно предложить воспользоваться средствами поиска, которые реализованы в современных поисковых системах, например, Яндекс. Принцип поиска заключается в том, что открытые источники необходимо проанализировать на наличие определенных ключевых слов, которые необходимо аккумулировать и консолидировать, выделяя из них новые выражения.

Поиск по открытым источникам получил название OSINT. OSINT – это процесс, в результате которого производится обнаружение, выбор, сбор и анализ информации и данных, находящихся в открытом сегменте Интернета. Выделяют три разных метода сбора данных в OSINT:

- автоматическими средствами;
- при помощи сервисов;
- ручными методами.

Для поиска информации формируется запрос, для уточнения которого применяются различные специализированные ключи, редко используемые простыми пользователями сети. Пример структуры такого поискового запроса показан на рисунке 1.

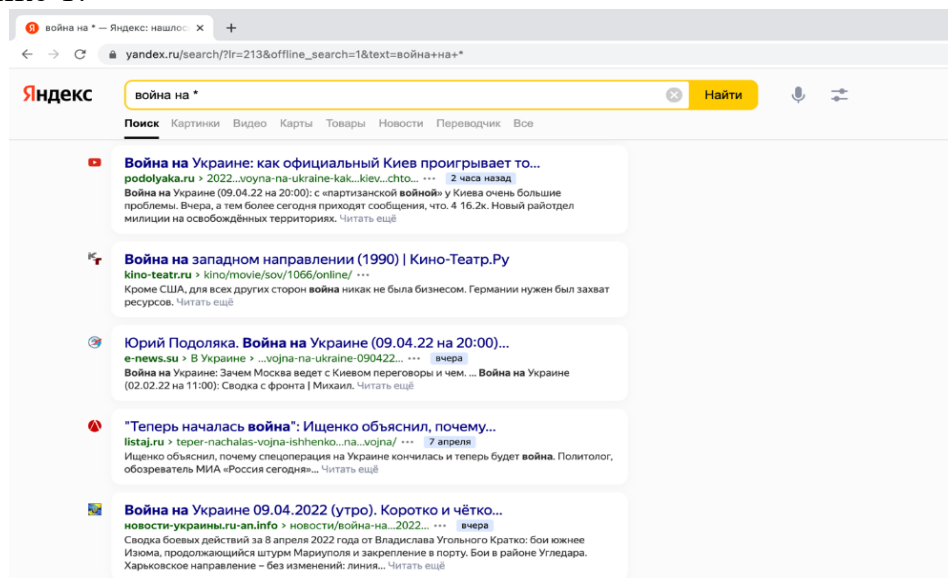


Рис. 1. Пример структуры поискового запроса с параметром

В поисковых системах разработчиками предусмотрен достаточно широкий набор таких специальных ключей, на рисунке 2 представлены некоторые из них с описанием синтаксиса и выполняемых функций.

Символ	Синтаксис	Для чего используется
Восклицательный знак !	Слово	Фиксирует слово в заданной форме, позволяя искать без учёта других падежей, числа, времён. Например, по запросу <i>купить билет в !Париж</i> :
	слово и !другие ! слова !фразы	- будет показано <i>купить билет в Париж</i>; - не будет показано <i>купить билет в Париже</i>.
Плюс +	+слово	Фиксирует слова, которые обязательно должны содержаться на странице. Обычно Яндекс убирает малозначимые служебные части речи, местоимения и другие слова без дополнительного смысла.
	слова +с предлогом	Например, по запросу <i>работа +на дому</i> : - будет показано <i>работа на дому</i>; - не будет показано <i>работа по дому</i> и <i>работа дома</i>.
Минус —	-слово	Минус позволяет исключить из поиска слова, а вернее, документы, в которых содержится выделенное минусом слово.
	фраза без -слова	Например, по запросу <i>уроки живописи -начинающий</i> : - будет показано <i>уроки живописи для взрослых</i>; - не будет показано <i>уроки живописи для начинающих</i>.
Кавычки " "	"слово"	Фиксирует количество слов в заданной фразе, не показывая расширенные варианты. Но разные словоформы разрешены. Кавычки используются для поиска по точной цитате.
	слово и "все слова фразы"	Например, по запросу <i>"домик в аренду на двоих"</i> : - будет показано <i>домик в аренду на двоих</i> и <i>домик аренда на двоих</i>; - не будет показано <i>домик в аренду для двоих</i> и <i>домик в посуточную аренду на двоих</i>.
Звёздочка *	"слово1 * слово3"	Поиск документов, которые содержат цитату с пропущенным словом или словами. Одна звёздочка заменяет одно слово.
	"слово1 * слово3"	Важно! Используется только при поиске цитат, то есть внутри кавычек. Например, по запросу <i>«у лукоморья * * златая»</i> : - будет показано <i>у лукоморья дуб зелёный; златая цепь на дубе том</i>; - не будет показано <i>у лукоморья дуб зелёный</i> (если на странице нет слова "златая").
Вертикальная черта	слово1 слово2	Поиск документов, которые содержат хотя бы одно из слов, размеченных вертикальной чертой.
	фраза с одним другим третьим	По нашим наблюдениям, предпочтение отдаётся документам, которые содержат оба запроса, а в таком случае выдача бывает непредсказуемой. Например, по запросу <i>заказать еду роллы пицца</i> : будет показано <i>заказать роллы и пиццу, заказать роллы, заказать пиццу, заказать роллы "пицца", заказать пиццу "суши"</i> (суши выводятся как синоним)

Рис. 2. Система запроса с параметром

Хоть рассмотренный метод поиска является очень простым, но он позволяет обнаруживать первичные следы информации террористической и экстремистской направленности, а имея определенный опыт и навыки, может стать базовым и эффективным инструментом.

Примером такого использования может стать запрос в информационно-поисковой системе Яндекс, позволяющий определить общее количество запросов по заданной пользователем тематике:

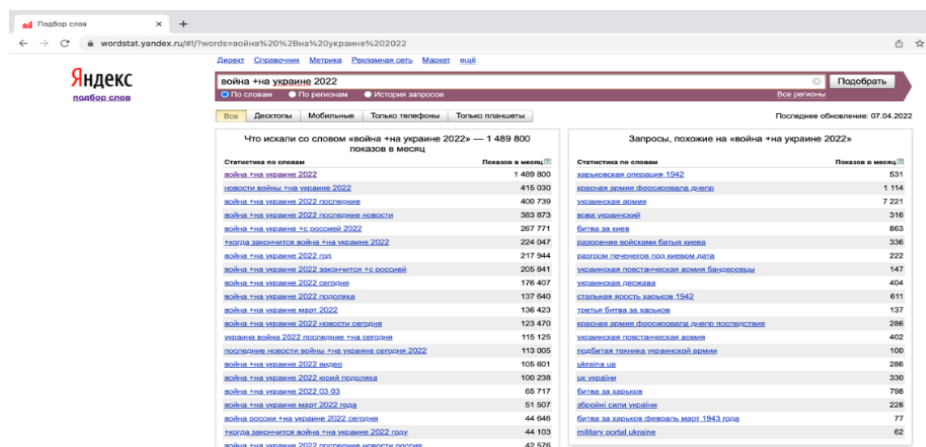


Рис. 3. Пример поиска информации через сервис подбора слов

Описанные в статье проблемы являются наиболее острыми в настоящее время, именно поэтому необходимо для их решения также применять современные технологии. В некоторых случаях они являются очень простыми, как рассмотренные в статье, но достаточно эффективными.

Список литературы

1. Почему Instagram признали экстремистской организацией. URL: // <https://www.amic.ru/news/voprosdnya/instagram-priznali-ekstremistskim-chto-eto-znachit-i-budu-li-ya-schitatsya-ekstremistom-esli-tam-sizhu> [дата обращения: 11.04.2022].
2. Сбор информации из открытых источников - как видят вас потенциальные злоумышленники? URL: // https://www.anti-malware.ru/analytics/Threats_Analysis/Gathering-information-the-waycybercrooks-see-you [дата обращения: 11.04.2022].
3. Поиск информации в Интернете. URL: // <http://help.rgsu.net/uchebnik/searchinfo/> [дата обращения: 11.04.2022].
4. Боевой OSINT – разведка и сбор информации из открытых источников URL: // <https://habr.com/ru/company/pentestit/blog/554006/> [дата обращения: 11.04.2022].
5. Методика работы в социальных сетях по выявлению экстремистского и иного противоправного контента. URL: // <http://viperson.ru/articles/metodika-raboty-v-sotsialnyh-setyah-po-vyyavleniyu-ekstremistskogo-i-inogoprotivopravnogo-kontenta> [дата обращения: 11.04.2022].

Бегларян М. Е.¹,

*заведующий кафедрой социально-гуманитарных
и естественнонаучных дисциплин*

*Северо-Кавказского филиала ФГБОУВО «Российский
государственный университет правосудия»,*

кандидат физико-математических наук, доцент

Спирина В. Ю.²,

студентка 4 курса Северо-Кавказского филиала

ФГБОУВО «Российский государственный университет правосудия»

КОМПЬЮТЕРНЫЕ И ПРАВОВЫЕ ТЕХНОЛОГИИ БОРЬБЫ С ТЕРРОРИЗМОМ В ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ РУНЕТА

Трансформация угроз в современном мире – это тренд информационного общества. Информация, которая всегда ассоциировалась с разумом, знаниями и опытом человечества, теперь стала источником опасений и угроз для самого человечества. Социум и его отдельные субъекты научились использовать информационные ресурсы, знания и данные для совершения актов терроризма и экстремизма. Внимание и финансы разумного человечества отвлекаются на борьбу с негативными проявлениями информационного и цифрового прогресса. Терроризм и экстремизм в форме информационного процесса стали реалиями современного цифрового мира. Социальная и экономическая стабильность информационного общества, его физическое и духовное развитие неразрывно связано с победами в сфере борьбы с информационным терроризмом, как отдельных граждан, так и органов государственной власти. Особенно активны попытки влияния на развитие глобального в целом и российского, в частности, социума со стороны информационных террористических организаций, предопределили направление формирования специальных государственных политических решений для обеспечения национальной безопасности в информационной сфере [1, с. 14].

Термины терроризм и экстремизм не требуют расшифровки, но они приобретают новые формы в информационном обществе при современном темпе цифровизации, поэтому стоит рассматривать такую форму как информационный терроризм. Будем понимать под этим явлением устрашение в информационном пространстве, совершаемое посредством информационно-телекоммуникационных сетей. Иногда информационный терроризм имеет реальный диалог жертвы и преступника или преступной группы либо террорист устрашает и запугивает жертву посредством социальных сетей или иного виртуального взаимодействия. Самый опасный вид информационного терроризма возникает тогда, когда есть внедрение в работу критических систем, обеспечивающих жизненно важные процессы, так называемая критическая инфраструктура, совершаются деяния с

¹ © Бегларян М. Е., 2022.

² © Спирина В. Ю., 2022.

помощью компьютерной техники и глобальных информационных систем, преступники находятся далеко от места преступления. Экстремизм в информационном обществе является пособником терроризма. Радикально настроенные элементы являются благодатной почвой для террористов и прочих противоправных направлений во всем мире.

В ст. 3 Федерального закона Российской Федерации «О противодействии терроризму» [2] зафиксировано, что «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».

Террористические организации и отдельные субъекты используют информационную террористическую и экстремистскую деятельность, содержание которой можно классифицировать или систематизировать по этапам осуществления преступного процесса: 1) организация и подстрекательство; 2) вербовка и обучение; 3) вовлечение сторонних аналогичных преступных организаций, которые владеют дополнительными информационными ресурсами; 4) пропаганда идей терроризма, распространение материалов, обосновывающих или оправдывающих террористические деяния; 5) подбор объектов, на которые будут направлены кибератаки [1, с. 19].

В Российской Федерации противодействие терроризму осуществляется по всем вышеперечисленным направлениям в рамках общегосударственной системы мер, которая представляет собой в первую очередь Закон, т. е. нормативные правовые акты, регулирующие деятельность по выявлению, предупреждению и пресечению, раскрытию и расследованию террористической деятельности, минимизации и ликвидации последствий проявлений терроризма. Важным элементом борьбы является «Комплексный план противодействия идеологии терроризма в Российской Федерации на 2019–2023 годы», который утвержден Президентом Российской Федерации 28 декабря 2018 г. [3].

В России создан Национальный Антитеррористический Комитет – НАК, который имеет свой официальный сайт <http://nac.gov.ru/>, и это подразделение ведет серьезную работу именно в информационном пространстве Интернета и Рунета.

В «Стратегии противодействия экстремизму в Российской Федерации до 2025 года» [4] сказано, что «в современных социально-политических условиях крайним проявлением экстремизма является терроризм, который основывается на экстремистской идеологии. Угроза терроризма будет сохраняться до тех пор, пока существуют источники и каналы распространения экстремистской идеологии». В «Концепции противодействия терроризму в Российской Федерации» [5] субъектами противодействия терроризму являются уполномоченные органы государственной власти и органы местного самоуправления, в компетенцию которых входит проведение мероприятий по противодействию терроризму, негосу-

дарственные организации и объединения, а также граждане, оказывающие содействие органам государственной власти и органам местного самоуправления в осуществлении антитеррористических мероприятий.

Необходимо противостоять терроризму в информационной сфере. Это целый ряд мероприятий, четкая система, которая имеет определенную государством структуру. Она состоит из следующих компонент:

- техническая;
- информационная;
- идеологическая и политическая;
- правовая и международно-правовая;
- административная и организационная.

Все усилия, направленные на уничтожение террористического информационно-психологического контента, сведение к минимуму воздействия экстремистских организаций на человека и социум, а также на противодействие использованию информационных и коммуникационных технологий в деструктивной деятельности политических и иных противников и их пособников.

Анализ Федерального закона от 7 июля 2003 г. № 126-ФЗ «О связи» [6] и Федерального закона от 25 июня 2002 г. № 114-ФЗ «О противодействии экстремистской деятельности» [7] свидетельствует о том, что в рассматриваемых нормативных правовых актах законодатели уклоняются от детализирования регламентирующих мер по пресечению и предупреждению применения средств связи, используемых террористами для того, чтобы дестабилизировать социальную и политическую обстановку. При этом законодатели делают отсылки к общим нормам Федерального закона «О противодействии экстремистской деятельности» и законодательству в сфере связи.

Президент Российской Федерации В. В. Путин неоднократно обращал внимание на проблему информационного терроризма, причем, не только проводя встречи с компетентными органами, но и на международных встречах, на государственных совещаниях различного уровня. На заседании Федеральной службы безопасности Российской Федерации 24 февраля 2021 г. Президент Российской Федерации В. В. Путин обратил свое внимание на то, что «...в 2020 г. количество опасных для российских информационных ресурсов атак увеличилось более, чем в три с половиной раза». На этом же заседании было сказано буквально следующее: «В этих условиях нам нужна долгосрочная, выверенная стратегия действий по защите национальных интересов в цифровой сфере, основанная на прогнозировании ситуации, на учете потенциальных рисков для общества и государства и, конечно, опирающаяся на самые передовые технологии и технологические решения. Вместе с партнерами из других стран надо развивать и систему обеспечения международной информационной безопасности» [8].

12 апреля 2021 г. Президентом Российской Федерации В. В. Путиным была утверждена и подписана новая концепция, из названия которой понятно, что Россия теперь имеет четкие ориентиры в области глобального информационного

взаимодействия, которые изложены в «Основах государственной политики Российской Федерации в области международной информационной безопасности» [9].

Необходимо изменить законодательно закрепленные правила и сделать их понятными и применимыми, можно даже сказать удобными для сотрудников МВД России, когда дело касается пресечения террористической деятельности в информационной сфере. Важно упростить механизм, позволяющий ограничить свободный доступ к «вражеским» интернет-ресурсам. Это можно сделать через изменение Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Статья 15.3 «Порядок ограничения доступа к информации, распространяемой с нарушением закона» [10] требует тщательной проработки. Также требует нормативного закрепления возможность использования сотрудниками правоохранительных органов программного обеспечения и приложений без ограничений.

Научные исследования должны быть выполнены совместно юристами и работниками ИТ-сферы – и это самое главное условие и залог успешной борьбы с террористами и экстремистами в информационном пространстве [10]. Для детальной проработки новых правовых норм только такой междисциплинарный подход даст ощутимый результат. Например, необходимо проработать действующие, законно утвержденные правила, которые позволят региональным прокурорам в случае экстренной необходимости блокировать интернет-сайты террористического характера в целях повышения оперативности реагирования на возникновение возможных террористических или экстремистских информационных атак.

Необходимо четко определить полномочия органов внутренних дел в области антитеррористической деятельности и определить правила такой работы в информационном пространстве, при этом закрепить их в Федеральном законе «О полиции» [12] и Федеральном законе «О противодействии терроризму», дополнив их соответствующими нормами.

Важно, в частности, прописать такие действия, которые будут направлены на уменьшение радикальных проявлений конкретно в молодежной среде. Для этого не надо придумывать новые процессы. Необходимо вспомнить и реализовать классические приемы воспитания, но в новом информационном, цифровом формате: 1) формировать высокую правовую культуру в молодежной среде; 2) воспитывать у молодежи толерантное мировоззрение в отношении национальности, религии, социального, имущественного положения и иных обстоятельств; 3) досуг и отдых молодежи должен быть не формально, а реально организованным и духовно близким к целевой аудитории; 4) молодежь должна быть материально заинтересована и защищена, должна быть востребована в своей стране и нужна своей Родине. Трудоустройство, поддержка в социальном, материальном и жилищном вопросах должны быть ощутимы, т. е. государство должно организовать «информационный» патронаж, чтобы у экстремизма и терроризма не было шансов подобраться к будущему нашей Родины, к молодежной информационной сфере.

Список литературы

1. Ахмедова В. Х., Сидненко Г. Ф. Современные аспекты информационного противодействия терроризму в Российской Федерации // Управление образованием: теория и практика. 2015. № 4 (20). С. 14–26.
2. Федеральный закон «О противодействии терроризму» от 06.03.2006 № 35-ФЗ. URL: <http://pravo.gov.ru/proxy/ips/?docbody=&nd=102105192> (дата обращения: 20.04.2022).
3. Комплексный план противодействия идеологии терроризма в Российской Федерации на 2019–2023 годы, утвержден Президентом Российской Федерации 28 декабря 2018 г. № Пр-2665. URL: <http://nac.gov.ru/terrorizmu-net/kompleksnyy-plan-protivodeystviya-ideologii-terrorizma-v.html> (дата обращения: 20.04.2022).
4. Указ Президента Российской Федерации от 29 мая 2020 г. № 344 «Об утверждении Стратегии противодействия экстремизму в Российской Федерации до 2025 года». // СПС «Гарант». URL: https://base.garant.ru/74194369/#block_1000 (дата обращения: 20.04.2022).
5. Концепция противодействия терроризму в Российской Федерации (утверждена Президентом Российской Федерации 05.10.2009) // Консорциум Кодекс. URL: <https://docs.cntd.ru/document/902180267> (дата обращения: 20.04.2022).
6. Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи» (с изменениями и дополнениями) // СПС «Консультант». URL: http://www.consultant.ru/document/cons_doc_LAW_43224/.
7. Федеральный закон от 25 июля 2002 г. № 114-ФЗ «О противодействии экстремистской деятельности» // Консорциум Кодекс. URL: <https://docs.cntd.ru/document/901823502> (дата обращения: 20.04.2022).
8. Заседание коллегии ФСБ России 24 февраля 2021 г. // URL: <http://kremlin.ru/events/president/news/65068> (дата обращения: 20.04.2022.).
9. Основы государственной политики Российской Федерации в области международной информационной безопасности, утверждены Указом Президента Российской Федерации от 12 апреля 2021 г. № 213 // Сайт СБ РФ. URL: <http://www.scrf.gov.ru/security/information/document114/> (дата обращения: 20.04.2022).
10. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ (последняя редакция). URL: http://www.consultant.ru/document/cons_doc_LAW_61798/.
11. Кобец П. Н. Противодействие терроризму в информационной сфере: опыт и проблемы // Научный портал МВД России. 2021. № 3 (55). С. 18–26.
12. Федеральный закон от 7 февраля 2011 г. № 3-ФЗ «О полиции» (с изменениями и дополнениями) // Официальный интернет портал правовой информации. URL: <http://pravo.gov.ru/proxy/ips/?docbody=&nd=102145133> (дата обращения: 20.04.2022).

Золоторев Д. В.¹,

курсант факультета подготовки специалистов

в области информационно безопасности

Московского университета МВД России имени В.Я. Кикотя

Научный руководитель:

Дворянкин О. А.,

старший преподаватель кафедры информационной безопасности

учебно-научного комплекса информационных технологий

Московского университета МВД России имени В.Я. Кикотя,

кандидат юридических наук

НЕЗАКОННЫЙ ОБОРОТ НАРКОТИКОВ И ЕГО ВЗАИМОСВЯЗЬ С ТЕРРОРИЗМОМ В СЕТИ ИНТЕРНЕТ

Начиная с момента своего существования, терроризм и незаконный оборот наркотиков оказались тесно связаны и переплетены с международной организованной преступностью, незаконным оборотом оружия, религиозным и политическим экстремизмом, незаконной миграцией. Все это относится к гигантской разветвленной криминальной системе.

Оценивая угрозу терроризма и незаконного оборота наркотиков на жизнь современного общества, то опасность этих явлений практически равнозначны.

В связи с этим правоохранительные органы как различных стран, так и России, а также различные международные организации по всему миру уделяют огромное внимание к этой проблеме.

Если обратиться к истории, то взаимосвязь между этими явлениями криминального мира можно проследить еще с самых давних времен, когда человек впервые начал употреблять вещества, приводящие к состояниям измененного сознания и потом в состоянии аффекта совершать противозаконные действия [1].

В качестве примера, по данным экспертов, можно вспомнить тайную боевую организацию «ассасинов», члены данного объединения подготавливали убийц, которые совершали свои преступления под действием каннабиса. Также необходимо отметить деятелей французской революции 1848 г., активно употреблявших наркотики в якобинском терроре. Наряду с ними отметились представители Латинской Америки, которые выращивали кусты коки на сельской местности (на ранчо) и потом поставляли некий продукт, в последующем названный кокаином, для поставок в Соединенные Штаты Америки во время гражданской войны 1861–1865 гг. для солдат, которые под его воздействием более активно вели боевые действия, не чувствуя боли и страха [2].

В дальнейшем, в том числе в настоящее время, тенденции не только не изменились, а только стали более жесткими и прагматичными. Наркотики и терроризм, объединившись, стали серьезно влиять на политический строй государств, а также играть значительную роль в жизни общества и людей. Наркотические средства и психотропные вещества стали более активно применять при боевых

¹ © Золоторев Д. В., 2022.

действиях, террористических актах, вербовке людей в террористические организации при «подсадке» на наркотики и т. д.

Правители многих государств взяли на вооружение и стали активно использовать наркотики и терроризм в своей политической деятельности, например, по данным экспертов, наркотики – для получения огромных неконтролируемых денежных средств, а методы терроризма – для запугивания населения на подконтрольной или внешней территории.

На примере можно рассмотреть пострадавшую от военных действий территорию Центральной и Западной Африки, где, по данным экспертов, повстанческие группы и террористические организации приобретали оружие и боеприпасы на средства, полученные от незаконной торговли наркотиками. Похожие проблемы прослеживались и на территории Центральной Америки. Также можно отметить Афганистан, где более 20 лет американские войска, по данным экспертов, проводили аналогичную политику зарабатывание денег на наркотиках и «террористические акты» для контроля над населением.

Таким образом, можно отметить, что незаконный оборот наркотиков и терроризм представляют огромную угрозу политическому, экономическому и социальному развитию государств по всему миру.

Однако в последнее время с появлением сети Интернет и ее информационных технологий для террористов и наркодилеров открылись новые горизонты для противозаконной деятельности.

Они стали открыто и в полном объеме использовать информационную открытость цивилизованного мира для достижения своих целей.

Так, если раньше террористам многие действия было совершать трудно (затруднительно) и/или сложно, например, быстро организовывать и координировать свои действия или управлять взрывными устройствами (бомбами) из-за нехватки средств и информационных (электронных) технологий, молниеносно координировать свои действия, а также открыто поставлять и реализовывать наркотики, то сейчас с помощью Интернета или его теневого сегмента Даркнета преступники получили возможность синхронизировать время и место проведения теракта [3].

Кроме этого в виртуальном мире (интернет-пространстве) с помощью различных программ, сервисов и ботов наркодилеры и террористы получили возможность проводить необходимые сделки по доставке и реализации наркотиков и взрывчатых устройств. Так, например, сервис «Google Maps», который в Интернете активно используется значительным количеством пользователей для получения, работы со спутниковыми снимками и картами любой местности, стал активно применяться террористами и наркодилерами. Именно данный сервис, по данным экспертов, использовался при террористических атаках в 2008 г. в индийском городе Мумбаи (Индия).

В связи с этим специальными органами было рекомендовано сотрудникам и разработчикам сервиса «Google Maps», разработать дополнительное специальное программное обеспечение, позволяющее размывать в данном сервисе на картах особо важные объекты (больницы, государственные учреждения, школы,

университеты, церкви и т. п.), чтобы детальное изучение их было практически невозможно.

Еще одним сервисом (мессенджером), которым они воспользовались, являлся Telegram, на площадке которого, по данным экспертов, в открытом виде, но завуалировано, предоставляется большой спектр услуг, связанных с незаконным оборотом наркотиков, начиная с магазинов, занимающихся распространением и продажей наркотических средств, и их рекламой, и заканчивая активными предложениями вакансий, связанных с наркобизнесом.

Таким образом можно отметить, что риск распространения криминальной деятельности, связанной с незаконным оборотом наркотиков и терроризмом в Даркнете, Telegram и на других сервисах, ботах, программах, заключается в его высокой степени анонимности (сервис VPN-шифрования предоставляет пользователю тайное нахождение в сети, поэтому отследить его IP-адрес практически невозможно) [4].

Наряду с этим государственными органами всех стран было отмечено, что в первую очередь под негативное влияние наркопреступников и террористов в сети Интернет попадает молодое поколение, которое потом активно используется в противоправной деятельности.

В этой связи были приняты международные документы, а также государственные, в том числе в Российской Федерации, направленные на решение проблемы по вовлечению молодых людей в террористические организации и наркотические структуры посредством сети Интернет.

Однако так как значительная часть пользователей Интернета – это несовершеннолетние лица, которые не имеют устоявшихся моральных, психологических норм, устоев и в этой связи наиболее сильно подвержены манипуляции из сети, к сожалению, профилактических мер, принимаемых для предотвращения наркоторговли и терроризма, в том числе с помощью информационно-коммуникационных технологий, оказалось недостаточно.

В заключение хотим отметить, что в целях недопущения распространения указанных фактов необходимо активизировать координацию деятельности правоохранительных органов, в том числе с контролирующими структурами, а также с различными общественными организациями, по профилактике и противодействию наркопреступникам и террористам в сети Интернет.

Кроме того, продолжать разработку правовых норм, совершенствовать технические механизмы борьбы в данной сфере, активно противостоять пропаганде идеологов этих явлений и сформировать у населения и в первую очередь у молодых людей твердую нравственную позицию и взгляды.

Список литературы

1. Зиновьев В. В. Антинаркотическая политика России: уголовно-правовые и криминологические аспекты реализации: дис. ... канд. юрид. наук. Саратов, 2017. С. 248.

2. Терроризм и наркобизнес [электронный портал] URL: https://studbooks.net/1005214/pravo/narkotiki_terrorizm (дата просмотра: 24.03.2022).

3. Терроризм в Интернете [электронный портал] URL: <https://www.saferunet.ru/adult/news/982/> (дата просмотра: 24.03.2022).

4. Соловьев В. С., Осипенко А. Л. Рынок нелегальных товаров и услуг в Darknet и Telegram-каналах. Международная научно-практическая конференция «Уголовная политика и культура противодействия преступности» в 2-х томах. 2018. С. 138–141.

Боровиков В. Б.¹,

профессор кафедры уголовного права

Московского университета МВД России имени В.Я. Кикотя,

кандидат юридических наук, доцент

Боровикова В. В.²,

доцент кафедры уголовного права

Московского университета МВД России имени В.Я. Кикотя,

кандидат юридических наук, доцент

ПРОБЛЕМЫ УГОЛОВНО-ПРАВОВОГО ПРОТИВОДЕЙСТВИЯ ПРЕСТУПЛЕНИЯМ ТЕРРОРИСТИЧЕСКОЙ И ЭКСТРЕМИСТСКОЙ НАПРАВЛЕННОСТИ В ИНФОРМАЦИОННОЙ СФЕРЕ

Развитие информационных технологий во всем мире, в том числе Российской Федерации, существенным образом повлияло на состояние и динамику преступности. По данным интернет-изданий в 2021 г. доля преступлений, совершенных с использованием IT-технологий в общей структуре российской преступности, составила 26 % (517000) [1]. В ней все большее место стали занимать преступления, совершаемые с использованием электронных или информационно-телекоммуникационных сетей, в том числе сети Интернет. В этой статье, учитывая различную терминологию, которую использует законодатель для обозначения указанных выше признаков составов преступлений, авторы придерживаются термина «преступления, совершаемые с использованием информационных технологий». Это не случайно, так как применение данных технологий значительно увеличивает возможности представителей криминального мира в достижении преступных целей. Этот вывод в полной мере обоснован и применителен к преступлениям террористической и экстремистской направленности. Вот некоторые данные, свидетельствующие о состоянии преступности террористического и экстремистского характера в Российской Федерации. За 11 месяцев 2021 г. следователи СК РФ направили в суд 197 уголовных дел о преступлениях террористического характера (+19,4 % по сравнению с тем же периодом за 2020 г.) и 184 уголовных дела о преступлениях экстремистской направленности, что более чем в 2,5 раза превышает показатели 2020 г. (70 дел) [2]. Например, при наличии рассматриваемых технологий расширяются пределы деятельности соучастников преступлений. В частности, подстрекатель может завербовать, вовлечь в совершение общественно опасных посягательств, подпадающих под признаки статей, предусмотренных чч. 1, 2 ст. 206, ст. 208, чч. 1, 2. 3 ст. 211, ст.ст. 220, 221, 277, 278, 279 и 360 УК РФ, значительно большее число лиц, чем это имеет место в обычных условиях. Соответственно, организатор получает дополнительные средства воздействия на других членов организованной группы или преступного

¹ © Боровиков В. Б., 2022.

² © Боровикова В. В., 2022.

сообщества (преступной организации), что в конечном счете повышает эффективность его деятельности по организации и руководству данными формами преступных проявлений. Увеличивается «потенциал» деятельности интеллектуального пособника, использующего анализируемые технологии.

Повышаются и «перспективы» для совершения таких преступлений, как, например, публичные призывы к осуществлению террористической деятельности, публичное оправдание терроризма или пропаганда терроризма (ст. 205.2 УК РФ), прохождение обучения в целях осуществления террористической деятельности (ст. 205.3 УК РФ), публичные призывы к осуществлению экстремистской деятельности (ст. 280 УК РФ), публичные призывы к осуществлению действий, направленных на нарушение территориальной целостности Российской Федерации (ст. 280.1 УК РФ).

В названных случаях, кстати, судебная практика признает перечисленные формы антиобщественного поведения оконченными преступлениями уже с момента публичного распространения хотя бы одного подобного обращения, независимо от того, удалось ли склонить кого-либо к преступной деятельности или нет. Тем самым законодатель в определенной мере «работает» на сотрудников правоохранительных органов, сужая предмет доказывания по уголовному делу. Важно при таком подходе установить сам факт наличия этих публичных призывов. Повлияли они на поведение аудитории или нет – это обстоятельство уже не влияет на квалификацию содеянного.

Полагаем, создание формальных составов при конструировании уголовно-правовых норм, предусматривающих ответственность за преступления в информационной сфере, – правильный путь, соответствующий реальной общественной опасности этих деяний и специфике психологического воздействия информационных технологий на сознание людей.

В целом можно сделать вывод, что за последние годы законодатель проделал немалую работу по совершенствованию уголовно-правовых норм, предусматривающих ответственность за преступления террористической и экстремистской направленности и деяния, создающие условия для существования названных выше антиобщественных явлений, включив в них в качестве квалифицирующих признаков состава – использование информационных технологий, в том числе сеть Интернет (например, ч. 2 ст. 205.2, п. «в» ч. 3 ст. 222, п. «в» ч. 5 ст. 222, п. «в» ч. 3 ст. 222.1, п. «в» ч. 5 ст. 222.1, п. «в» ч. 3 ст. 222.2, п. «в» ч. 5 ст. 222.2, ч. 1 ст. 282 УК РФ).

Вместе с тем есть резервы, использование которых, на наш взгляд, будет способствовать повышению эффективности уголовно-правового противодействия преступлениям террористического и экстремистского характера в информационной сфере.

Конечно, законодателю целесообразно продумать вопрос о включении в ст. 163 УК РФ в качестве обстоятельства, отягчающего наказание, такое как совершение преступления с использованием информационно-телекоммуникационных сетей, в том числе сети Интернет (терминология может быть изменена, так как в настоящее время не существует единообразия в статьях Особенной части УК РФ,

в части использования IT-технологий в качестве признака состава преступления).

Главный аргумент в пользу этого предложения состоит в том, что использование данных информационных технологий при совершении преступления получило уже широкое распространение и причиняет значительный вред интересам граждан, государства и общества. В определенной мере будет восстановлена справедливость, связанная с реальной оценкой содеянного в случае, когда законодатель еще не признает названное обстоятельство в качестве признака основного или квалифицированного состава преступлений.

Конечно, сформулированный ранее вывод не означает, что законодатель должен прекратить деятельность по совершенствованию уголовно-правовых запретов, предусматривающих ответственность за преступления террористической и экстремистской направленности. В частности, анализ соответствующего законодательного материала показывает, что вопрос о включении в ряд уголовно-правовых норм в качестве квалифицирующего признака – «использование информационных технологий» еще не получил своего окончательного решения. Так, очевидно, что деяния, перечисленные в ст. 205.1 УК РФ (Содействие террористической деятельности), представляют большую общественную опасность, если совершаются с использованием информационных технологий. Нет каких-либо сомнений, что склонение, вербовка или иное вовлечение лица в совершение хотя бы одного из преступлений, перечисленных в чч.1 или 2 ст. 205.1 УК РФ (речь идет о преступлениях, образующих террористическую деятельность, например, теракте, организации незаконного вооруженного формирования или участия в нем, захвате заложника при отягчающих обстоятельствах, угоне судна воздушного или водного транспорта или железнодорожного подвижного состава, незаконном обращении с ядерными или радиоактивными веществами) осуществляется более результативно при применении информационных технологий.

Аналогичные доводы можно привести, когда речь идет о таких формах преступного поведения как прохождение обучения в целях осуществления террористической деятельности (ст. 205.3 УК РФ), заведомо ложное сообщение об акте терроризма (ст. 207 УК РФ), массовые беспорядки (ст. 212 УК РФ). Хотя деяния, предусмотренные ст.ст. 207, 212 УК РФ, не признаются согласно примечанию к ст. 205.2 УК РФ разновидностями террористической деятельности, они имеют тесное отношение к созданию условий для совершения преступлений террористической и экстремистской направленности. Полагаем в перечисленных выше случаях, включение в ст.ст. 205.3, 207 и 212 УК РФ квалифицирующего признака – «использование информационных технологий» позволит более адекватно оценить общественную опасность анализируемых деяний.

Следует отметить, что использование информационных технологий в террористической и экстремистской деятельности требует переосмысления отдельных положений Общей части российского уголовного законодательства.

Это касается, в частности, норм о соучастии в преступлении. Так, как показывает жизнь, совершение преступления по предварительному сговору группой

лиц или в составе организованной группы с использованием сети Интернет не требует личного знакомства участников этой формы преступного поведения. Лица, завербованные для участия в том или ином преступлении террористической или экстремистской направленности, могут не знать в лицо организатора, других соисполнителей (общение осуществляется посредством логинов, паролей, зашифрованных сообщений в условиях анонимности). Это явление заставляет задуматься о таком необходимом признаке соучастия как наличие двусторонней субъективной связи. Ответа на данный вопрос пока нет.

По-новому надо трактовать и признаки приготовления к преступлению, в частности, когда речь идет о толковании такой его разновидности как приискание соучастников преступления и сговор на совершение преступления. Опять-таки возможна ситуация, при которой приискание соучастников преступления осуществляется посредством Интернета, также как и при заключении сговора на совершение преступления.

Названные выше обстоятельства, как минимум, надо учитывать при квалификации и расследовании преступлений террористической и экстремистской направленности.

По-новому надо относиться к понятию физического и психического насилия как обстоятельства, исключаящего преступность деяния. Полагаем, психическое принуждение вполне может осуществляться путем применения ИТ-технологий. Следовательно, есть почва для корректирования наших представлений о данном обстоятельстве, исключаящем преступность деяния.

Таким образом, жизнь предъявляет новые требования к решению различных уголовно-правовых вопросов, связанных с фактами использования информационных технологий в процессе совершения преступлений террористического и экстремистского характера.

Список литературы

1. Бабахина А. Основные тенденции российской преступности в 2021 г.: исследование «если быть точным». URL: <http://tochno.st/material/osrovi> (дата обращения: 25.04.2022).
2. Козлова Н. Следствие без тайн // Р.Г.2022. 14 января.

Гунина К. Е.¹,
студентка КФ ФГБОУВО
«Российский государственный
университет правосудия»

Научный руководитель:
Шевко Н. Р.,
доцент кафедры уголовно-правовых дисциплин
КФ ФГБОУВО «Российский государственный
университет правосудия»,
кандидат экономических наук, доцент

КИБЕРТЕРРОРИЗМ КАК ФОРМА ТЕРРОРИЗМА

Современный этап развития общества включает в себя применение и развитие сферы информационных технологий. Практически все процессы в мире основываются на коммуникационных и информационных технологиях. Сегодня практически любая деятельность тесно связана с получением, обработкой, хранением и использованием информации, имеющей важное значение. Практически любая сфера жизни человека зависит от информации. Это повлекло появление новых возможностей для совершения преступлений. Многие из них перешли в так называемое «виртуальное пространство», причем последствия, к сожалению, остались в реальном измерении. Так появились новые термины – «киберпреступность», «кибертерроризм» и др.

Сегодня без глобальной сети Интернет невозможно представить ни дня: от общения в социальных сетях, мониторинга мессенджеров и новостных каналов до работы, исполнения своих должностных обязанностей, обеспечения населения всем необходимым. Интернет охватывает большинство сфер жизни общества, что способствует формированию у современного человека определенной Интернет-зависимости. Злоумышленники используют эту особенность современного человека в своих целях. Зачастую преступные деяния совершаются именно посредством гаджетов и всемирной паутины. Не является исключением и терроризм, приобретая форму кибертерроризма. На современном этапе он является самой опасной угрозой для государства и общества, требует всестороннего анализа, исследования сущности и методов борьбы с ним [2].

Число преступлений, совершаемых в глобальном информационном пространстве, растет каждый год. На данный момент киберпреступления распространены больше в экономической сфере, но стремительно увеличивается и число преступлений террористического характера с использованием современных информационных технологий. Террористы пользуются сетью Интернет потому, что она предоставляет большие организационные и наступательные возможности. Такие преимущества глобальной сети, как простота доступа, широкая аудитория (в том числе и трансграничность), высокая скорость обмена информацией, анонимность и возможность скрыть свое истинное лицо являются основой

¹ © Гунина К. Е., 2022.

для возникновения преступлений террористического характера в киберпространстве. При организации преступления в виртуальном пространстве не осуществляются личные встречи, отсутствует привязка к конкретному месту, нет имен. Такой готовящийся теракт отследить и спрогнозировать практически нереально.

Предположительно термин «кибертерроризм» был употреблен в 1997 г. Специальный агент ФБР Поллит определял его как «преднамеренные политические мотивированные атаки на информационные, компьютерные системы, компьютерные программы и данные, выраженные в применении насилия по отношению к гражданам» [3].

Кибертеррористы в целях осуществления своих преступных намерений привлекают профессиональных хакеров, которые зачастую взламывают сайты, чтобы обеспечить доступ к различной информации, включая секретную. На многих сайтах местных органов власти можно найти, казалось бы, совершенно безобидную, но в то же время весьма важную и совершенно незащищенную информацию (например, схема подземных коммуникаций).

Ученые выделяют два основных вида кибертерроризма.

Первый вид: террористические действия совершаются с помощью компьютерных сетей и гаджетов. Для этого вида характерны следующие особенности:

- всевозможные компьютерные атаки, с помощью которых можно несанкционированно проникнуть или перехватить управление атакуемой сетью;
- рассылка компьютерных вирусов, которые блокируют, модифицируют или уничтожают информацию;
- использование «троянских коней», с помощью которых можно выполнять вредоносные действия без ведома владельца зараженной системы и др.

Примером данного вида преступного посягательства служит нарушение работоспособности информационной системы, которое может привести к неправомерному контролю за всеми функциями поражаемого объекта (военная сфера, предприятия химического и атомного производства).

Второй вид кибертерроризма заключается в том, что глобальное информационное пространство используют террористические группы в целях распространения информации. К нему относятся:

- проведение пропаганды террористических целей, планируемых действий (например, размещение видеоматериалов протеррористического характера в Интернет-пространстве);
- использование Интернета для психологического воздействия на людей анонимного привлечения к террористической деятельности соучастников; сбор информации для планируемых терактов (например, в декабре 1997 г. по телевидению Японии показывался анимационный фильм, содержащий контаминацию цветовой гаммы, мигания визуальной информации, от просмотра которого десятки людей получили психофизические расстройства разной тяжести);
- распространение в открытом доступе схем по самостоятельному изготовлению оружия, взрывных устройств и др.

Статистика преступлений, совершенных с использованием Интернета в России, неуклонно растет. Так, за 2018 г. было совершено 121,2 тыс. преступлений с использованием информационных технологий, в 2019 г. – 180,1 тыс., в 2020 г. количество выросло на 73,4 % и составило 510,4 тыс., на 2021 г. – 518 тыс. [1].

В целом количество кибератак на одну организацию в мире в неделю характеризуется следующими показателями: Африка – в среднем 1615 атак; Азиатско-Тихоокеанский регион (АТР) – в среднем 1299 атак; Латинская Америка – 1117 атак; Европа – в среднем 665 атак; Северная Америка – в среднем 497 атак [1].

Таким образом, число преступлений террористического характера, к сожалению, с каждым годом увеличивается, растет и количество киберпреступлений. Противостоять этому надо, причем всем миром. Одной, отдельно взятой стране, бороться с кибертерроризмом бессмысленно. Необходимо организовать сотрудничество государств, международных организаций, противостоящих кибертерроризму и компьютерной преступности.

Список литературы

1. Портал правовой статистики [электронный ресурс] // Официальный сайт Генеральной прокуратуры Российской Федерации. Режим доступа: URL: http://crimestat.ru/offenses_chart (дата обращения: 20.03.2022).
2. Токбаев А. А. Современные аспекты противодействия терроризму // Актуальные проблемы гуманитарных и естественных наук, 2013. № 10-2. С. 134–136.
3. Krasavin S. What is Cyber-terrorism? / S. Krasavin // Computer Crime Research Center (CCRC). URL: <http://www.crime-research.org/library/Cyber-terrorism.htm>. (дата обращения: 13.04.2022).

Заманова А. Н.¹,
студентка КФ ФГБОУВО
«Российский государственный университет правосудия»

Зарифуллина А. Р.²,
студентка КФ ФГБОУВО
«Российский государственный университет правосудия»

Научный руководитель:
Шевко Н. Р.,
доцент кафедры правовой информатики,
информационного права и естественнонаучных дисциплин,
Казанский филиал ФГБОУВО «Российский государственный
университет правосудия»,
кандидат экономических наук, доцент

ПРОФИЛАКТИКА ЭКСТРЕМИСТСКИХ И ТЕРРОРИСТИЧЕСКИХ ПРОЯВЛЕНИЙ СРЕДИ МОЛОДЕЖИ В ИНФОРМАЦИОННОЙ СЕТИ ИНТЕРНЕТ

Сегодня сеть Интернет является основным связующим звеном информационного взаимодействия людей всего мира. Молодежь является активным пользователем интернет-ресурсов. Благодаря всемирной паутине многие могут позволить себе пройти онлайн-обучение в удобное для них время, практически в любое время дня и ночи в сети можно найти необходимую информацию об интересующем объекте, часто Интернет используют для общения с людьми на всех континентах. Ведь современные информационные технологии позволяют сокращать время, расстояния и предлагают новые возможности. Однако помимо позитива, Интернет, к сожалению, может быть использован и в преступных целях. За счет трансграничного характера, массовости распространения информации за считанные секунды по всему миру и анонимности Интернет используется и злоумышленниками – незаконный оборот оружия, наркотиков, распространение запрещенных веществ, мошенничество, вербовка. Все чаще в глобальной сети размещаются материалы пропагандистского характера, направленные на возбуждение ненависти либо вражды, геноцида и расизма. В последнее время участились случаи вступления молодежи в экстремистские организации, информация о деятельности которых распространяется через всемирную сеть.

Экстремистская деятельность (экстремизм) – это призыв социальных масс к насильственным действиям против существующего политического, религиозного или социального строя. Экстремизм напрямую связан с терроризмом, так как развитие экстремизма в общественной среде создает предпосылки для проявления терроризма. В свою очередь террористическая деятельность (терроризм) – это преступление, главной целью которого является нарушение общественной

¹ © Заманова А. Н., 2022.

² © Зарифуллина А. Р., 2022.

безопасности, которое выражается в посягательстве на жизнь и здоровье граждан, объекты инфраструктуры, природную, информационную среду, органы государственного управления, государственных и общественных деятелей [2].

Однако экстремистская и террористическая деятельность может проявляться не только в реальной жизни, но и в глобальной информационной сети Интернет (в том числе в социальных сетях) [3].

Социальные сети в современном мире активно стали развиваться. Постепенно они стали универсальными средствами общения. Надо отметить, что и количество пользователей социальных сетей, как во всем мире, так и в России неизменно растет. По официальным данным число российских юзеров соцсетей в 2022 г. составило около 106 млн человек [1].

Экстремизм в молодежной среде обладает рядом отличительных признаков, что объясняет особую актуальность вопроса профилактики экстремизма среди этой социальной группы. Обусловлено это постоянно формирующимися очагами напряжения, затрагивающими интересы молодежи, а также ограниченностью форм, методов и реальных практик профилактической работы среди молодежи.

Анализ ситуации поможет выявить причины, по которым чаще всего в ней имеют место быть экстремистские и террористические проявления [2].

Во-первых, самой главной причиной является возраст. Он характеризуется, как «буря и натиск», когда человек отправляется на поиск новых ощущений.

Во-вторых, большую роль играет протестная активность молодежи. Точки социального напряжения вызывают у них особый интерес, и они реагируют на них особо остро. По мнению экспертов, студенты, неработающие молодые люди, неработающие пенсионеры и безработные являются наиболее активными участниками протестов в Российской Федерации. Но важно отметить, что необходимо различать действия, которые носят конструктивный характер и направления на преобразование социальной среды от незаконных.

В-третьих, напряжение связано с присутствием иностранных граждан на территории региона. Сложности связаны как с неготовностью молодежи принимать особенности другой нации, так и с возникающими опасениями по поводу возможной конкуренции в вопросах трудоустройства среди части молодежи. Эти противоречия также требуют определенной профилактической работы, направленной на формирование толерантности и принятия этих граждан.

Сознание молодежи начинает закладываться в образовательных учреждениях, и большую роль в этом процессе играют школы и вузы.

Образовательные учреждения играют большую роль в воспитании у обучающихся мировоззрения по поводу ценности человеческой жизни, закреплённой в ст. 2 Конституции Российской Федерации. Каждый человек должен понимать и осознавать, что жизнь человека – самое ценное, что есть в этом мире, поэтому стоит активно акцентировать свое внимание на развитии уважения к человеческой жизни среди молодежи.

Согласно судебной статистике Российской Федерации, с каждым годом наблюдается увеличение осужденных по статьям, устанавливающим наказание

за террористическую и экстремистскую деятельность в сети Интернет. Так, по ч. 2 ст. 280 Уголовного кодекса Российской Федерации «Публичные призывы к осуществлению экстремистской деятельности, совершенные с использованием средств массовой информации либо информационно-телекоммуникационных сетей, в том числе сети Интернет» наблюдается стремительный рост осужденных. По статистике Верховного суда Российской Федерации около 70 % совершаемых преступлений по данной статье с 2018 г. были зафиксированы в социальных сетях. Данные приведены в таблице 1 [1]:

Таблица 1

Динамика числа осужденных за экстремистскую деятельность

Год	Количество
2021	242
2020	135
2019	109
2018	83
2017	88
2016	89

Таким образом, профилактика экстремистских и террористических проявлений среди молодежи в информационной сети Интернет является одной из основных задач, стоящих перед человечеством. Экстремизм и терроризм являются наиболее опасными проявлениями преступных деяний во всем мире. Задача современного государства – сделать информационную среду свободной от радикально настроенных элементов.

Список литературы

1. Портал правовой статистики. URL: http://crimestat.ru/offenses_chart (дата обращения: 03.04.2022).
2. Смирнов А. А. Информационное противодействие терроризму и экстремизму // Научный портал МВД России. 2013. № 4 (24). URL: <https://cyberleninka.ru/article/n/informatsionnoe-protivodeystvie-terrorizmu-i-ekstremizmu>.
3. Шевко Н. Р. Актуальные проблемы обеспечения информационной безопасности современного общества / Н. Р. Шевко. Вестник Казанского юридического института МВД России. 2012. № 2 (8). С. 57–59.

Новиков А. В.¹,

курсант факультета подготовки

сотрудников для оперативных подразделений полиции

Московского университета МВД России имени В.Я. Кикотя

Научный руководитель:

Гончар В. В.,

начальник кафедры информационной безопасности

учебно-научного комплекса информационных технологий

Московского университета МВД России имени В.Я. Кикотя,

кандидат юридических наук, доцент

СОВРЕМЕННОЕ СОСТОЯНИЕ ЭКСТРЕМИЗМА И ТЕРРОРИЗМА В УСЛОВИЯХ РАЗВИТИЯ ЦИФРОВЫХ ТЕХНОЛОГИЙ

В настоящее время в современном обществе происходит борьба с одной из самых страшных проблем, вызывающей тревогу в мировом сообществе, с такой как экстремизм и терроризм. Данные явления возникают как правило из конфликтов и противоречий по религиозным, социальным, политическим и национальным мотивам. Процесс внедрения цифровых технологий в жизнь современных людей принес не только упрощение жизни человека, но и подверг огромному риску свое существование. Экстремисты и террористы для достижения своих целей используют метод принуждения, а в век современных технологий это стало реализовываться намного проще и масштабнее. Поэтому уголовно-правовое противодействие со стороны государства является главной прерогативой в предотвращении совершения экстремистской и террористической деятельности.

На данный момент происходит большой поток запрещенной информации через Интернет-ресурсы, такие как социальные сети и интернет-мессенджеры. Вконтакте, Инстаграмм, Телеграмм – являются на данный момент самыми популярными средствами для общения. Это вызывает огромный интерес среди преступников, так как такие площадки дают необъятный ресурс людской силы для вовлечения их в преступную деятельность. В основном с помощью данных интернет-ресурсов происходит подбор кандидатов посредством создания закрытых групп. В данных группах изначально не происходит подачи запрещенной информации, выкладываются посты с тематикой, косвенно подходящую под экстремистскую и террористическую деятельность. После этого преступники ждут заинтересованности со стороны пользователей.

Конечно, соответствующие службы производят мониторинг социальных сетей, но цифровые технологии развиваются с каждым годом и тем самым затрудняют выявление такой информации правоохранными органами. Появление таких технологий как VPN-адреса и прошивка сквозным шифрованием усложнили поимку преступников.

¹ © Новиков А. В., 2022.

Вся их особенность состоит в их работе. Вот, например, VPN-адрес. Затрудненность в отслеживании VPN-адресов заключается в расположении спутников передачи связи, т. е. над разными странами, к примеру, пользователь может находиться в России и пользоваться сигналом, исходящим из Англии. Тем самым шифруя свой настоящий адрес.

Прошивка сквозным шифрованием заключается в передаче данных между пользователем и участвующем в общении с ним лицом, тем самым третье лицо не может узнать или получить сведения, распространяемые в личном чате. Это привело к тому, что злоумышленники стали еще более скрытно осуществлять свою преступную деятельность.

Все более развиваясь, интернет-мессенджеры начинают использовать такие технологии, которые усугубляют положение государства в сфере контроля за экстремистской и террористической деятельностью. Был принят Федеральный закон от 22.09.2021 № 540 «О самоконтроле социальных сетей», согласно которому интернет-площадки обязаны выявлять и блокировать запрещенную информацию. Это как раз обусловлено значительными проблемами, возникающими в получении доступа к незаконной информации.

Также в стороне не остается всеми известный Darknet (черный Интернет). Данный Интернет обуславливает свое название, так как здесь происходит наибольшее скопление преступников. Darknet является для экстремистов и террористов основным источником внедрения в социум. Особенность этой сети заключается в практически полном отсутствии контроля со стороны государства. Здесь можно выкладывать напрямую посты, содержащие запрещенную информацию и это не будет никак санкционировано. Конечно, правоохранительные органы пытаются побороть данную проблему с помощью вступления в эти группы и выявления лиц, участвующих в них, но это не приводит к огромным успехам как в поимке этих лиц, так и в предотвращении распространения запрещенного контента в иные социальные сети.

Теперь хотелось бы обратиться к статистике. Согласно статистическим данным за период 2018–2021 гг. в 2018 г. по террористической направленности совершено 1679 преступлений, раскрыто из них 748, по экстремистской направленности – 1265 преступлений, из них раскрыто 1188. В 2019 г. по террористической направленности выявлено фактов преступлений 1806, раскрыто из них 844, по экстремистской направленности – 585, раскрыто из них 454 факта. В 2020 г. по террористической направленности совершено 2342 преступления, из них раскрыто – 910, по экстремистской направленности выявлено 833 факта, из них раскрыто – 677. В 2021 г. по террористической направленности выявлено фактов преступлений 2136, раскрыто из них 1094 факта, по экстремистской направленности совершено 1057 преступлений, раскрыто из них 908.

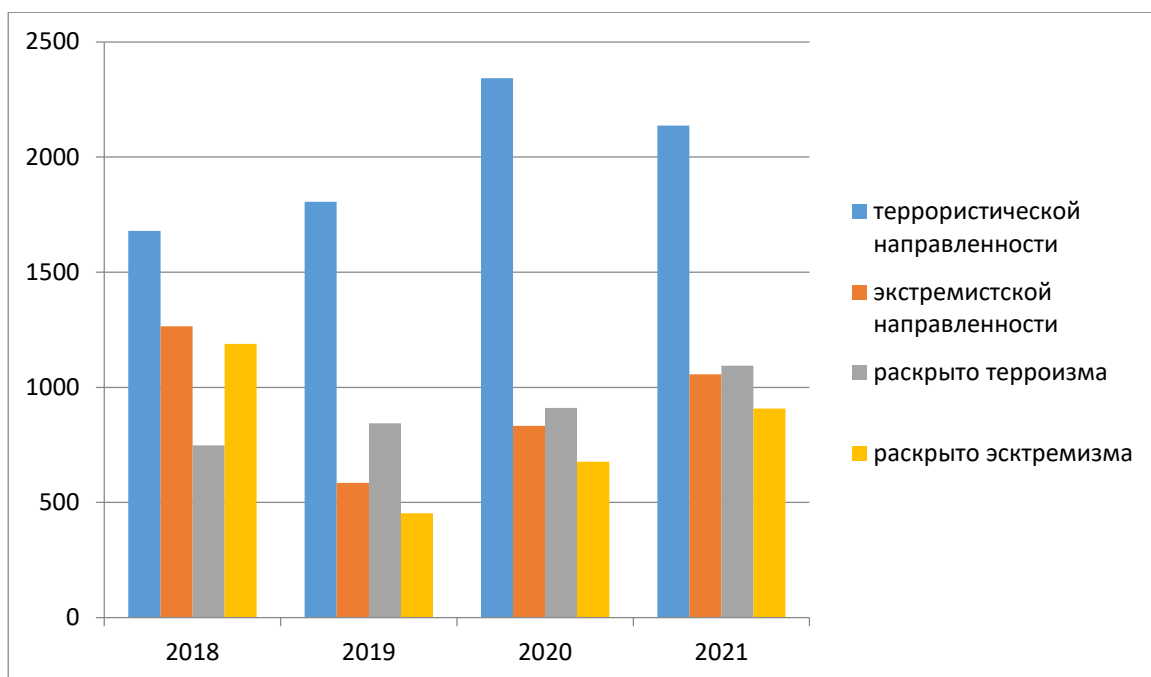


Рис. 1. Статистические данные

На основании приведенных статистических данных можно прийти к выводу, что происходит рост экстремистской и террористической деятельности. Незначительный рост показателей по экстремистской направленности обусловлен повышением значительного уровня латентности данных видов преступлений и из-за повышения уровня знаний и квалифицированности преступников в сфере цифровых технологий. Это, прежде всего, говорит нам о том, что необходимо принятие мер как уголовно-правового характера, так и ограничительных мер.

Изучая данную тематику и произведя анализ вышесказанного, можно подвести итоги, которые могут поспособствовать, прежде всего, в предотвращении совершения данных противоправных деяний:

1. Со стороны государства необходимы решительные меры по ограничению контента, распространяемого в Интернете, желательно установление контроля за социальными сетями, так как они являются основным источником распространения запрещенной информации.

2. Это ужесточение мер уголовной ответственности за экстремизм. Если за ст. 205 УК РФ «Террористический акт» предусмотрено максимальное наказание в виде лишения свободы сроком на 20 лет, то ст. 280 «Публичные призывы к осуществлению экстремистской деятельности» предусмотрено максимальное наказание в виде лишения свободы сроком до пяти лет. Здесь нужно рассмотреть более тщательно вопрос об увеличении срока наказания за данные противоправные действия.

3. Касательно новых цифровых технологий. В данном аспекте следует изучение их изначально, проще говоря, их «обкатки» государственными органами для выявления в них проблем и разработки методов борьбы с этими технологиями.

Список литературы

1. Пинкевич Т. В., Зубалова О. А. Современное состояние экстремизма и терроризма // ЮП. 2020. № 3 (94). URL: <https://cyberleninka.ru/article/n/sovremennoe-sostoyanie-ekstremizma-i-terrorizma-v-usloviyah-razvitiya-tsifrovyyh-tehnologiy>.
2. Пинкевич Т. В. Проблемы противодействия терроризму в условиях глобализации // Международно-правовые средства противодействия терроризму в условиях глобализации. Проблемы террористического наемничества среди молодежи и пути их преодоления: материалы Всероссийской научно-прак. конф. Ставрополь, 2016. (дата обращения: 05.04.2022).
3. Министерство внутренних дел Российской Федерации: официальный сайт. URL: <https://мвд.рф/> (дата обращения: 05.04.2022).
4. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 25.03.2022). URL: http://www.consultant.ru/document/cons_doc_LAW_10699/43942021d9206af7a0c78b6f65ba3665db940264/.

Маклаков Е. Д.¹,

слушатель факультета подготовки

специалистов в области информационной безопасности

Московского университета МВД России имени В.Я. Кикотя

Научный руководитель:

Овчинский А. С.,

профессор кафедры информационной безопасности

учебно-научного комплекса информационных технологий

Московского университета МВД России имени В.Я. Кикотя,

доктор технических наук, профессор, академик РАЕН

ЦИФРОВЫЕ ПЛАТФОРМЫ ОПЕРАТИВНО-РАЗЫСКНОЙ АНАЛИТИКИ В ПРОТИВОДЕЙСТВИИ ТЕРРОРИЗМУ И ЭКСТРЕМИЗМУ

Говоря о безопасности информационных сфер, о противодействии терроризму и экстремизму, выкристаллизовывается задача: не давать социальной деструкции зародиться и созреть в информационных сферах. Решаться эта задача может на основе современных и перспективных технологий контроля, воздействий и управления социальными процессами.

Автоматизация и последующая цифровизация открыли возможности накопления и обработки огромных объемов самых разнообразных данных. Их использование в раскрытии и профилактике преступлений опирается на новые направления оперативно-разыскной аналитики. Основной теоретической базой при этом остаются представления о триединстве реактивной, ресурсной и фоновой оперативно-разыскной информации. В условиях цифровой трансформации правоохранительных органов на основе алгоритмов оперативно-разыскной аналитики создаются цифровые платформы раскрытия и профилактики преступлений террористической и экстремистской направленности.

Цифровые платформы сегодня – это весьма емкое понятие, используемое в коммерции, логистике, военном деле, государственном управлении. Можно встретить описание программных, инфраструктурных, отраслевых платформ. Так, эксперты-футурологи представляют государство уже недалекого будущего в виде цифровой платформы, включающей алгоритмы автоматического управления экономикой, финансами, правовой системой, социальной сферой, внутренней и внешней безопасностью на основе возможностей искусственного интеллекта.

В ОРД речь может идти, в первую очередь, о закрытых цифровых платформах, настроенных на информационно-аналитическое сопровождение раскрытия и расследования преступлений, обеспечения антикриминальной безопасности. Создание этих платформ должно быть направлено на синтез таких алгоритмов обработки цифровых данных, которые отражают наиболее перспективные

¹ © Маклаков Е. Д., 2022.

направления оперативно-разыскной аналитики: инициативной, предиктивной, актуальной, ретроспективной, экспресс-аналитики.

Эти направления оперативно-разыскной аналитики выкристаллизовались на основе представлений о реактивной, ресурсной и фоновой составляющих оперативно-разыскной информации.

Инициативная аналитика в обеспечении антикриминальной безопасности стирает противоречие между непрерывным пополнением информационных оперативно-разыскных ресурсов и эпизодическим обращением к ним. Она направлена на превентивное выявление лиц, представляющих потенциальные угрозы общественному порядку и безопасности, требующих мер оперативно-разыскной профилактики. Инициативная аналитика показала свою эффективность при обеспечении безопасности таких крупнейших международных мероприятий, как Олимпийские и Параолимпийские игры (Сочи – 2014), Чемпионат мира по футболу 2018 г. Ее алгоритмы перспективны при целенаправленных территориальных исследованиях контингента лиц, от которых можно ожидать преступлений и правонарушений в городах и населенных пунктах с повышенной криминогенной обстановкой.

Экспресс-аналитика направлена на раскрытие преступлений по «горячим следам» – «не отходя от компьютера». Лица, подозреваемые в совершении преступления, устанавливаются на основе данных камер видеонаблюдения и фотографий, имеющихся в базах данных оперативно-разыскных ресурсов. Сведения из различных сегментов Интернета формируются в криминальные профили подозреваемых, устанавливаются их связи и возможные места нахождения. Использование данных о приобретенных билетах на авиа- и железнодорожный транспорт дает возможность организовать задержание выявленных вероятных преступников.

Ретроспективная аналитика направлена на раскрытие преступлений прошлых лет, розыск пропавших лиц, установление неопознанных погибших. Она опирается на специально организованные матричные информационные ресурсы, содержащие пустые элементы для недостающих сведений. Включает алгоритмы автоматического поиска данных и наполнение пустых элементов матрицы сведениями, требующимися для раскрытия преступлений прошлых лет.

Предиктивная аналитика направлена на профилактику преступлений, правонарушений и антисоциальных явлений. Она требует автоматизированных алгоритмов обращения к ресурсам оперативно-разыскной информации, использования нейросетей для обработки агентурных сообщений, оперативных сводок, Больших данных – фоновой информации, циркулирующей в сетевом эфире и социальных коммуникациях.

Фундаментальной теоретической базой применения предиктивной аналитики в профилактике преступлений является доказанное криминологическими исследованиями положение о том, что «нарастание незначительных отступлений от позитивного (в социальном и нравственном смысле) поведения может приводить человека к антиобщественным и общественно опасным поступкам».

Актуальная аналитика включает: оперативно-криминологическое прогнозирование условий, обстоятельств, места, времени, заказчиков и исполнителей преступлений; применение алгоритмов обработки накопленных и поступающих данных вместе с разработкой и использованием комплекса криминологических моделей; «выход» на возможного исполнителя или заказчика преступления с ориентировкой на его личностные и физические качества, вплоть до внешнего вида, особенностей характера и поведения.

Психолого-лингвистическая аналитика должна включать алгоритмы лингвистического анализа, позволяющие выявлять и ранжировать угрозы, содержащиеся в экстремистском и террористическом контекстах, а также алгоритмы психологического анализа, позволяющие получать максимально информативные цифровые профили о лицах, представляющих оперативный интерес.

Открытые цифровые платформы ОРД. Необходимо отметить, что наибольшие перспективы в управлении процессами декриминализации общественных отношений, в противодействии терроризму и экстремизму открывает создание открытых цифровых платформ. Открытые платформы наряду с алгоритмами накопления и обработки данных включают еще и коммуникационные серверы, построенные, например, по принципу социальных сетей.

Именно архитектура открытых цифровых платформ должна создать пространство для интерактивного общения, для формирования мировоззренческих позиций, идеологических установок, направленных на противодействие социальной деструкции. Коммуникационные алгоритмы открытых платформ должны включать механизмы целенаправленных воздействий на сознание людей, попадающих под влияние деструктивных идей, таких идей, которые побуждают к противоправным, насильственным действиям.

Целью обработки ресурсной и фоновой оперативно-разыскной информации, т. е. накопленных, поступающих и циркулирующих в Интернет-коммуникациях и массмедиа-данных, должны стать как проведение мероприятий по недопущению готовящихся преступлений, так и меры по криминологической профилактике, направленные на выявление и ликвидацию причин формирования криминальных потенциалов.

Основная функция открытых цифровых платформ противодействия терроризму и экстремизму – это информационные воздействия, включающие обще социальную профилактику, а по существу – формирование позитивного, патриотического, жизнеутверждающего фона в массовом сознании, в информационных сферах.

Список литературы

1. Овчинский А. С., Борзунов К. К., Чеботарева С. О. Информационные координаты. Управление. Противоборство. Безопасность. М. : Горячая линия. Телеком, 2018.
2. Овчинский А. С. Цифровые платформы оперативно-разыскной профилактики преступлений / Оперативно-разыскная деятельность в цифровом мире: сборник научных трудов / под ред. В. С. Овчинского. М. : Инфра–М, 2021.

Осипова А. А.¹,

заместитель командира взвода

факультета подготовки специалистов

в области информационной безопасности

Московского университета МВД России имени В.Я. Кикотя

Научный руководитель:

Клочкова Е. Н.,

доцент кафедры специальных информационных технологий

учебно-научного комплекса информационных технологий

Московского университета МВД России имени В.Я. Кикотя

СОВРЕМЕННЫЕ МЕТОДЫ И ТЕХНОЛОГИИ БОРЬБЫ С ЭКСТРЕМИСТСКИМИ ПРОЯВЛЕНИЯМИ В СЕТИ ИНТЕРНЕТ

Если обратиться в любой период истории, то можно заметить, что везде присутствуют ситуации, где люди, недовольные существующим политическим, социальным или же религиозным строем, собираются с целью применения насильственных действий. Насилие против государственной власти и ее представителей, посягательство на жизнь государственных или общественных деятелей, нарушение прав и свобод мирного населения, причинение вреда здоровью и имуществу либо создание и распространение печатных, аудио- и видео- материалов и т. д. – все это имеет общее понятие «экстремизм». В Федеральном законе от 25.07.2002 № 114 «О противодействии экстремистской деятельности» экстремистская деятельность подразумевает под собой следующее (рис.1):

ЭКСТРЕМИСТСКАЯ ДЕЯТЕЛЬНОСТЬ (ЭКСТРЕМИЗМ) Статья 1 Федерального закона № 114 от 25.07.2002 «О противодействии экстремистской деятельности»	
насильственное изменение основ конституционного строя или нарушение территориальной целостности РФ	пропаганда исключительности, превосходства либо неполноценности по признаку социальной, расовой, национальной, религиозной или языковой принадлежности
возбуждение социальной, расовой, национальной или религиозной розни	публичное оправдание терроризма и иная террористическая деятельность

¹ © Осипова А. А., 2022.

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
использование нацистской атрибутики или символики , либо атрибутики или символики, сходных с нацистской атрибутикой или символикой до степени смешения, либо атрибутики или символики экстремистских организаций	совершение преступлений по мотивам, указанным в пункте «е» части 1 статьи 63 УК РФ
публичное заведомо ложное обвинение лица, замещающего государственную должность РФ или субъекта РФ, в совершении им указанных деяний или деяний, являющихся преступлением в период исполнения своих должностных обязанностей	финансирование указанных деяний либо иное содействие в их организации, подготовке и осуществлении
организация и подготовка указанных деяний, а также подстрекательство к их осуществлению	публичные призывы к осуществлению указанных деяний либо массовое распространение заведомо экстремистских материалов, а равно их изготовление или хранение

Рис. 1. Основные понятия экстремизма

Противодействие, пресечение и профилактика экстремистской деятельности – одна из задач правоохранительных органов, но, чтобы решить ее, необходимо понять, где призывают людей к ее осуществлению. Самыми крупными средствами призыва, конечно же, являются сеть Интернет и социальные сети (ВКонтакте, Одноклассники, Facebook, YouTube и др.), где люди знакомятся, общаются, объединяются в группы, создают или присоединяются к сообществам и т. д.

Для достижения противоправных целей экстремизма на пользователей социальных сетей оказывают социально-психическое деструктивное воздействие. Проявление данной деятельности выражается в следующих признаках:

1. Нарушение баланса интересов, механизма социально-правового взаимодействия, идеалов общества и традиций.
2. Подмена и разрушение духовных и нравственных норм, т. е. аморальность.
3. Радикальность в действиях, направленных на достижение целей экстремизма.

Исходя из вышеперечисленных признаков сложно представить противодействие, которое могло бы распознать, раскрыть и пресечь экстремистскую деятельность, ведь помимо этого еще существуют такие проблемы как:

– сеть Интернет не имеет принадлежности к кому-либо и, например, на международном уровне касательно вопроса правового регулирования по борьбе с преступностью в Интернете регулирование отсутствует;

- постоянное совершенствование и использование современных информационных технологий (средства связи, технологии шифрования и кодирования, анонимизация пользователей Интернета) со стороны преступности;
- отсутствие правового регулирования по противодействию анонимности, а также технических возможностей;
- ограниченность действий и отсутствие опыта в информационной сфере правоохранительных органов, а также низкий уровень взаимодействия с техническими разработчиками социальных сетей.

И хотя количество преступлений экстремистской направленности ежегодно увеличивается, правоохранительные органы продолжают вести активную борьбу. На рисунке 2 представлена статистика преступлений экстремистской направленности, совершенных с использованием информационно-телекоммуникационных технологий.

СОСТОЯНИЕ ПРЕСТУПНОСТИ В РОССИИ

Преступления экстремистской направленности, совершенные с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации

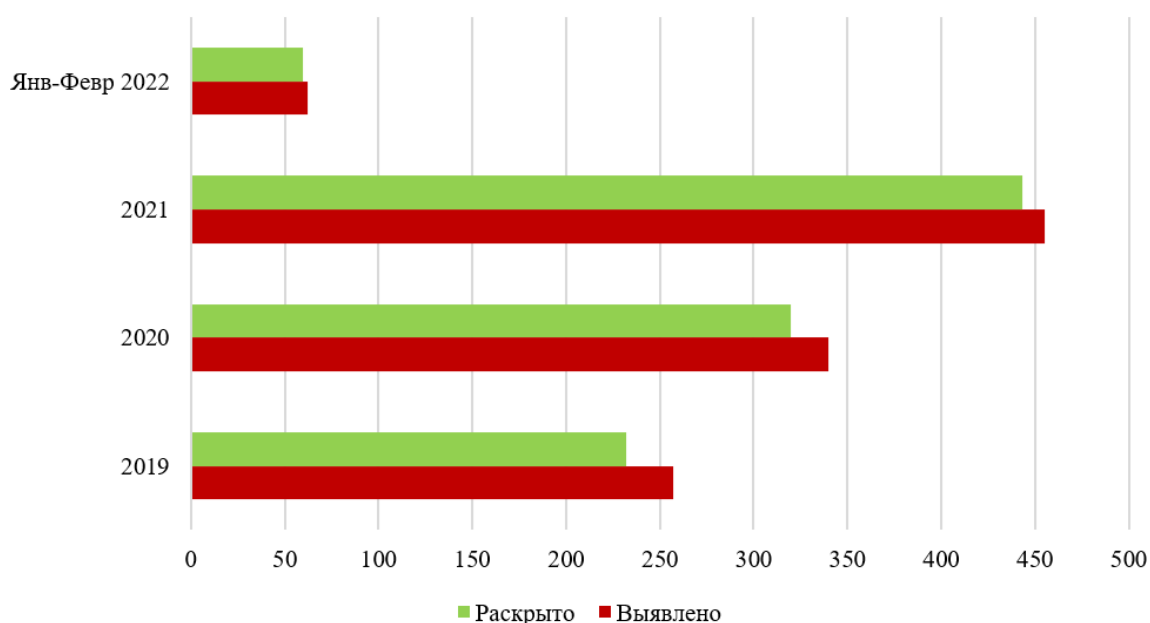


Рис. 2. Статистика преступлений экстремистской направленности

Справедливости ради необходимо отметить, что в борьбе с запрещенным контентом принимают участие не только правоохранительные органы, но различные государственные органы, общественные организации, простые граждане. Основными способами такой борьбы становятся:

1. Нормативно-правовое регулирование: Конституция Российской Федерации (статья 13), Уголовный кодекс Российской Федерации, Кодекс об административных правонарушениях Российской Федерации, Федеральный закон (далее – ФЗ) «О противодействии терроризму», ФЗ «О политических партиях», ФЗ «Об общественных объединениях», ФЗ «Об информации, информационных

технологиях и о защите информации», ФЗ «О связи», ФЗ «О средствах массовой информации», Указ Президента Российской Федерации «Об утверждении Стратегии противодействия экстремизму в Российской Федерации до 2025 года», «Концепция противодействия терроризму в Российской Федерации» и т. д.

2. Общественный надзор. Например, в 2011 г. была создана ассоциация «Лига безопасного Интернета», которая *«открыла свою горячую линию, пролоббировала законы о защите детей от вредной информации и о «черных списках» интернета, создала внушительную кибердружину из 20 тыс. человек и инициировала блокировки сотен сайтов»*.

3. Программное обеспечение (далее – ПО) для оперативных сотрудников. Разработка ПО для мониторинга социальных сетей (например, система «СЕУС», позволяющая мониторить площадки «Одноклассники», «Instagram» и «Telegram», или система «Демон Лапласа», с помощью которой изучаются публикации по ключевым словам, фразам, названиям или датам и выдается список аккаунтов, попавших под заданный критерий).

4. Мониторинг молодежи. Центр изучения и сетевого мониторинга молодежной среды (ЦИСМ), учрежденный в 2018 г., направлен на выявление и сбор информации, которая склоняет детей к опасным действиям, а также передача полученных данных МВД России, ФСБ России, Роспотребнадзору или Минпросвещению. Выявление осуществляется посредством чтения переписок и деанонимизации (т. е. частичного или полного раскрытия личности) пользователей социальных сетей

5. Гибридные технологии, т. е. оперативное решения задач возложить не только на информационные технологии, но и на человека, иными словами, на «человеко-машинные технологии». ЦИСМ заключает с регионами соглашения о сотрудничестве. Целью соглашения являются сбор и загрузка данных в систему об аккаунтах в социальных сетях школьников.

Если углубляться в мониторинг социальных сетей, то кроме чтения переписок и поиска по ключевым словам также можно выделить такие способы, как: изучение групп, сообществ и открытых страниц; анализ изображений и видеоматериалов, выложенных в социальные сети. Для решения данных задач могут использоваться следующие сервисы:

- интернет-ресурсы: snitch.name (поиск профилей), tagboard.com (поиск хештегов), sharedcount.com (число упоминаний в соцсетях), knowem.com (пробивание логина по соцсетям), Popsters (сервис для аналитики эффективности профилей в социальных сетях), Livedune и др.;

- утилиты: Сгееру (сбор геолокационной информации о пользователе на основе данных из его аккаунтов), GeoStalker (сбор информации по координатам, которые передал пользователю) и др.;

- операторы для строки поиска «ВКонтакте»: type:reply *ключевое слово* (поиск постов с комментариями), has:photo *ключевое слово* (поиск по фото с упоминанием запроса в описании или хештеге), has:doc *ключевое слово* (поиск по вложенным документам с поддержкой поиска по формату файла), has:poll *ключевое*

слово (поиск опросов с упоминанием запроса в тексте), *has:none* (поиск по публикациям без каких-то прикреплений и вложений), *near:координаты* (поиск постов по геолокации) и т. д.;

– сервисы для анализа фотографий: *29a.ch/photo-forensics* (поиск следов фотомонтажа), *regex.info/exif.cgi* (чтение метаданных), *newocr.com* (распознавание текста) и др.;

– сервисы со статистикой видеоканалов: *SocialBlade* (сервис для аналитики каналов на YouTube), *Whatstat*, *SeeZisLab* и т. д.

Основываясь на вышеизложенном, можно сделать вывод, что борьба с экстремистскими проявлениями в сети Интернет будет успешной только тогда, когда борьба будет вестись по всем направлениям.

Список литературы

1. Состояние преступности // МВД России. URL: <https://мвд.рф/reports/> (дата обращения: 05.04.2022).

2. Проскурникова К. В., Саутина С. А. Проявление экстремизма в сети интернет и формирование толерантного мышления // Сборник материалов круглого стола. Тверь : ФКУ НИИИТ ФСИН России, 2018. С. 247–253.

3. Шогенов Т. М. О некоторых вопросах противодействия экстремизму в сети Интернет // Пробелы в российском законодательстве. Юридический журнал. 2017. №3. С. 58–59.

4. Информационный экстремизм в сети Интернет – специфика воздействия на социум, опасность, противодействие // Pravo.Team URL: <https://pravo.team/uk-i-koap/gosudarstvennaya-bezopasnost/ekstrimizm/v-seti.html> (дата обращения: 05.04.2022).

5. Экстремизм в Интернете // Юристы России. URL: <https://yurist-rossiya.ru/novosti/ekstremizm-v-internete.html> (дата обращения: 05.04.2022).

*Полянская Е. П.¹,
преподаватель кафедры информационной безопасности
учебно-научного комплекса информационных технологий
Московского университета МВД России имени В.Я. Кикотя*

НЕКОТОРЫЕ ПРОБЛЕМЫ ДОКАЗЫВАНИЯ, ВОЗНИКАЮЩИЕ ПО УГОЛОВНЫМ ДЕЛАМ О ПРЕСТУПЛЕНИЯХ, СОВЕРШЕННЫХ ПО МОТИВАМ РАСОВОЙ, НАЦИОНАЛЬНОЙ, РЕЛИГИОЗНОЙ НЕНАВИСТИ ИЛИ ВРАЖДЫ

Борьба с противоправными деяниями экстремистской направленности является одним из приоритетных направлений деятельности органов внутренних дел.

Общественная опасность преступлений, совершенных по экстремистским мотивам обусловлена циничностью, агрессивностью, враждебностью поведения преступников, которые проявляют указанные действия в отношении людей, принадлежащих к определенной этнической группе, расе или религиозной конфессии.

Нередко у сотрудников правоохранительных органов, осуществляющих доследственную проверку, возникают сложности в разграничении смежных составов преступлений, в установлении субъективной стороны преступления, что осложняет формирование доказательственной базы.

При совершении преступлений экстремистской направленности действительными намерениями преступника являются в первую очередь не такие объекты, как жизнь или здоровье конкретного человека, и не материальные предметы или какое-либо имущество, а стремление ущемить, принизить расовое, национальное или религиозное достоинство и тем самым показать свое превосходство перед определенными общественными группами.

Сама по себе деятельность этнических преступных групп (организаций), состоящих из представителей какой-либо национальности, не может рассматриваться как характеризующий признак совершения преступления по рассматриваемому мотиву.

Преступления, совершаемые этническими преступными сообществами, могут совершаться не по мотиву ненависти к другому этносу, а в связи с делением сферы влияния в определенной экономической области, в криминальной сфере или определяться другими обстоятельствами, которые обусловили конфликт различных группировок.

Способ совершения преступления экстремистской направленности может быть различным. Экстремистские преступления, которым присущ физический характер, часто совершаются с особой жестокостью, в форме активных действий. Эти действия могут быть как физическими, например, направленными на умышленное причинение вреда здоровью, так и информационными, связанными с передачей сведений, способствующих возбуждению ненависти и вражды у других лиц, например, несовершеннолетних.

¹ © Полянская Е. В., 2022.

Действия информационного характера могут быть разнообразными (в зависимости от соответствующего состава преступления). К ним относятся: а) распространение и демонстрация агитационных материалов; б) выступление на массовых мероприятиях; в) издание, продажа, бесплатное распространение соответствующих брошюр, книг, статей, видео-, аудиозаписей, прочих источников; г) распространение инструкций, побуждающих к различным противоправным действиям против лиц другой национальности, вероисповедания, социальной группы и т. д.; д) предъявление определенных требований вышеуказанным лицами или группам в разных формах (устная, письменная, печатная, через различные средства массовой информации и социальные сети), например, «прочь из нашей страны, региона, города», «не появляйтесь в определенных местах» и т. д.), а также угрозы применения насилия в адрес определенных категорий лиц; е) выступление по радио, телевидению, в прессе, сети Интернет.

По каждому уголовному делу необходимо устанавливать содержание умысла, которое включает в себя желание совершить преступление именно в отношении указанных национальных, конфессиональных или иных социальных групп или их представителей. При этом лицо осознает, что в своем противоправном поведении оно проявляет соответствующие ненависть либо вражду и желает их продемонстрировать.

При совершении преступлений экстремистской направленности умысел направлен на совершение определенных общественно опасных действий либо угрозы их совершения в демонстративной манере с умышленным психологическим воздействием, вызывающим подавленность, страх.

Преступное деяние, которое описано в диспозиции статьи уголовного закона, само по себе может не указывать на его экстремистский характер.

Особенность предмета доказывания здесь состоит в точном определении субъективного отношения лица или лиц к совершенному деянию, в определении мотива, побудившего его к противоправным действиям.

Таким образом, для отграничения преступлений, совершаемых по признаку ненависти или вражды от смежных уголовно-противоправных деяний, необходимо определить мотив, который побуждает субъекта преступления к действиям. Это позволит не только правильно квалифицировать деяние, но и составить план проведения предварительного расследования и сбора необходимых доказательств.

По мнению А. П. Малаева, мотив национальной ненависти может быть как мнимым, так и истинным [2, с. 55–56].

Мнимым является мотив, при котором ущемление национальных чувств маскирует другие интересы – корысть, амбициозные психологические склонности личного превосходства, уничтожение политических или деловых конкурентов.

Пусть ущемление этнических, религиозных чувств, вред, причиняемый общественным ценностям, позволяет учитывать этот мотив для квалификации преступления или выделения обстоятельства, отягчающего наказание. Но для деятельности по предупреждению возможной в будущем преступной деятельности

необходимо понимать истинные мотивы, которые являются движущей силой при совершении лицом насильственных или иных преступлений.

Истинный мотив обусловлен целью причинения вреда лицу или группе лиц именно в связи с их этнической, социальной или религиозной принадлежностью. Субъект преступления стремится к реализации своего чувства, связанного с непримиримостью к определенной этнической группе или вероисповеданию. При этом вера в собственное превосходство и ущербность иной социальной группы может формироваться у лиц, являющихся вполне психически здоровыми, вменяемыми и признаваться вменяемыми.

Преступления с одним из признаков экстремистской направленности могут совершаться одним лицом, группой лиц или преступным сообществом (преступной организацией). При групповом совершении преступления необходимо изучить как личность каждого преступника в отдельности, так и определить связи между участниками группы.

Данные, полученные рядом авторов, свидетельствуют о том, что большая часть преступлений экстремистской направленности совершается лицами мужского пола (95,3 %), из которых третья часть – это несовершеннолетние лица в возрасте от 12 до 14 лет. Около 60 % деяний совершены лицами в возрасте от 17 до 25 лет. Взрослые люди совершают такие преступления реже (от 25 до 30 лет – 8 %, от 30 до 40 лет – 6 %, старше 40 лет – 5 %). Большая доля преступников является учащимися или выпускниками образовательных учреждений, которые по разным причинам не трудоустроены [1, с. 360–362].

Субъекты названных преступлений могут быть неоднородны по чертам своего характера и преследуемым целям, мотивам совершаемых ими действий. При этом можно выделить и некоторые общие черты, характеризующие личность преступников, например, такие как эмоциональная холодность и бесчувственность, неумение сопереживать и войти в положение другого человека и одновременно они могут проявлять противоположные чувства, например, чрезмерную чувствительность, ранимость, агрессивность и жестокость, неумение сдерживать свои негативные эмоции, злопамятность.

Лишь незначительная часть преступлений экстремистской направленности совершается в состоянии алкогольного опьянения.

К обстоятельствам, которые необходимо установить при получении показаний для доказывания экстремистского мотива, можно отнести личность допрашиваемого лица, его отношение к совершенному деянию и к участникам уголовного дела, взаимоотношения между ними.

Согласно постановлению Пленума Верховного Суда Российской Федерации от 28.06.2011 № 11 «О судебной практике по уголовным делам о преступлениях экстремистской направленности» для правильного установления мотива преступления следует учитывать, в частности, наличие конфликта между участниками события преступления, длительность межличностных отношений подозреваемого с потерпевшим, наличие с ним конфликтов, не связанных с национальными, религиозными, идеологическими, политическими взглядами, принадлежность к той или иной расе, социальной группе.

Для того, чтобы найти подтверждение тому, что мотив совершения преступления формировался определенный промежуток времени и побудил к активным действиям, необходимо выяснить, просматривались ли лицом, подозреваемым или обвиняемым в совершении преступления, в социальных сетях, среди друзей или в близком окружении изображения, картинки, музыка, видеозаписи экстремистского содержания, изучались ли графические изображения, комментарии, в которых содержится соответствующая информация.

Анализ материалов уголовных дел позволяет выявить типичную ошибку – в доказательствах не фиксируется информация о том, в отношении какой нации, расы выражены пренебрежение, агрессия. В материалах уголовного дела необходимо отображать сведения о потерпевших (национальная, этническая или расовая принадлежность, гражданство, возраст, род занятий, для иностранца – владение русским языком).

Часто вопрос о том, по отношению к какой национальной группе преступник проявляет ненависть или вражду, остается трудноразрешимым. В материалах уголовных дел можно встретить термины, которыми нельзя обозначить конкретную расовую принадлежность потерпевших, например, «лицо нерусской национальности», «неславянской национальности», «хачи», «кавказские фашисты» и т. п.

Поскольку следователь или дознаватель, проводящий проверку сообщения о рассматриваемых преступлениях либо расследование уголовного дела, обязаны устанавливать расу, национальность, религиозную принадлежность лица, то при невозможности самостоятельно решить этот вопрос могут быть привлечены специалисты. Смысловое понимание устных и письменных текстов исследуется в ходе производства лингвистических экспертиз.

Распространенность преступлений экстремистской направленности с каждым годом во всем мире приобретает угрожающие масштабы.

Состояние и динамика рассматриваемых преступлений определяют необходимость усиления мер, направленных на их предупреждение. Вместе с тем уголовное преследование лиц, совершивших преступления по мотивам расовой, национальной, религиозной ненависти или вражды, в настоящее время связано со значительными трудностями, поскольку существует множество проблем квалификации преступлений, особенно введенных в Уголовный кодекс Российской Федерации в последнее время, сложностей при формировании доказательственной базы, правильном применении инструментов доказывания, которые можно устранить путем правильного и грамотного толкования законодательства в этой сфере.

Список литературы

1. Адеянова М. А. Криминалистическая характеристика преступлений экстремистской направленности // Научный электронный журнал «Меридиан». № 2 (36). 2020. С. 360–362.
2. Малаев А. П. Мотив национальной ненависти или вражды: проблема юридической идентификации термина // Отечественная юриспруденция. № 7 (9). 2016. С. 55–56.

Шмарион П. В.¹,

*доцент кафедры КБ-12 «Правовое обеспечение
национальной безопасности»*

*Института кибербезопасности и цифровых технологий РТУ МИРЭА,
кандидат юридических наук*

СОВРЕМЕННЫЙ ТЕРРОРИЗМ: ОСОБЕННОСТИ, ТЕНДЕНЦИИ, МЕРЫ ПРОТИВОДЕЙСТВИЯ

В настоящее время можно говорить о терроризме как о новой форме ведения войны, когда боевые действия осуществляются без официального ее объявления, а значит, без четкого определения театра войны и театра военных действий, без знаков различия воюющих сторон и с нарушениями норм международного права, обеспечивающих защиту мирного населения и некомбатантов. Все чаще совершаются акты терроризма, в основе которых лежат нетерпимость, дискриминация отдельных социальных и этнических групп населения или даже народов, что подчеркивает его взаимосвязь с экстремизмом. Террористические организации выходят на уровень ведения регулярных боевых действий, контролируют целые города, страны, регионы. Вполне реальной становится возможность использования ими различных видов оружия массового поражения.

Террористы стремятся получить власть и доступ к финансовым ресурсам, используя слабости общественной и государственной систем в периоды экономической и социальной нестабильности, усложнения международной обстановки.

Современные террористические организации представляют собой разветвленные сети подпольных групп с жесткой иерархической структурой, состоящей из управляющего и оперативного звена, подразделений разведки, контрразведки, материально-технического обеспечения, боевых групп и прикрытия. Причем в качестве прикрытия используются специально созданные фирмы, фонды, финансовые организации. Существует надежная конспирация и агентура в правоохранительных и государственных органах, проводится тщательный отбор кадров, имеются учебные базы и полигоны. По данным международных организаций, хорошо оснащенные базы подготовки террористов расположены в более чем десяти странах мира (Иран, Ирак, Ливия, Куба, Северная Корея, Сирия, Сомали, Судан и др.). Кроме того, в последнее десятилетие произошло увеличение не только количества террористических группировок международного и транснационального уровня, но частоты взаимодействия между террористическими организациями (например, между чеченскими и арабскими), предпринимаются попытки оказания воздействия на ситуацию в мире (например, «Аль-Каида», «Исламское государство»). Все это говорит об организованном характере современного терроризма как о его специфике, активно проявляющейся в последнее время.

Террористы осваивают ранее недоступные им способы совершения насильственных акций, в том числе с использованием информационно-телекоммуникационных технологий. В социальных сетях и посредством сети Интернет активно

¹ © Шмарион П. В., 2022.

распространяются террористические и экстремистские идеи и материалы, даются предвзятые и заведомо ложные оценки политической ситуации и принимаемых официальной властью решений, преднамеренно неверно трактуются религиозные тексты, привлекаются финансовые активы. Под маской борцов с несправедливостью осуществляются попытки придать терроризму форму социального протеста с целью привлечения новых сторонников, особенно молодежи.

Информационные технологии используются не только для осуществления пропагандистской и вербовочной деятельности, но и для совершения кибератак в разведывательных целях, устрашения населения, взаимодействия и координации деятельности отдельных террористических групп и ячеек, что позволяет террористической угрозе становиться все более централизованной.

Учитывая высокую доходность отдельных сфер криминального бизнеса, террористические организации активно участвуют в преступной деятельности, включая незаконный оборот наркотиков, незаконную торговлю оружием, энергоносителями, похищение и торговлю людьми, «отмывание денег» и контрабанду ядерных и других потенциально смертоносных материалов.

Причинами перечисленных тенденций являются: разрастание кризисных явлений как на международной арене, так и на национальном уровне, неспособность официальных властей урегулировать сложные процессы в социальной и политической сферах, в том числе межнациональные и международные конфликты, быстрая смена систем общечеловеческих ценностей и идеалов, а также имеющиеся у террористов возможности манипулирования общественным сознанием посредством сети Интернет и в социальных сетях с помощью социальной инженерии.

Согласно данным МВД России за 2021 г. в стране было совершено 2136 преступления террористического характера, что на 8,8 % меньше по сравнению с 2020 г. Однако за последние 7 лет (с 2015 г.) динамика положительная, причем прирост составил 53 %, что не может не вызывать определенной тревоги [1].

В Российской Федерации в структуре преступлений террористического характера доминируют: организация деятельности террористической организации и участие в деятельности такой организации (ст. 205.5 УК РФ) – 22,75 %; содействие террористической деятельности (ст. 205.1 УК РФ) – 20,46 %; организация незаконного вооруженного формирования или участие в нем (ст. 208 УК РФ) – 20,6 %; публичные призывы к осуществлению террористической деятельности или публичное оправдание терроризма (ст. 205.2 УК РФ) – 18,40 %; несообщение о преступлении (ст. 205.6 УК РФ) – 5,81 %; прохождение обучения в целях осуществления террористической деятельности (ст. 205.3 УК РФ) – 5,24 %; террористический акт (ст. 205 УК РФ) – 1,92 %; организация террористического сообщества и участие в нем (ст. 205.4 УК РФ) – 1,69 % [2].

На национальном уровне основное внимание направлено на реализацию мероприятий, предусмотренных Комплексным планом противодействия идеологии терроризма в Российской Федерации на 2019–2023 гг. [3] и Стратегией противодействия экстремизму в Российской Федерации до 2025 года [4].

В результате проведенных мероприятий в 2021 г. на стадии приготовления предотвращено 65 преступлений террористической направленности, было задержано 312 боевиков и 821 пособник, пресечена деятельность 62 законспирированных ячеек международных террористических организаций, не допущен въезд на территорию страны 926 лиц, причастных к террористической деятельности, заблокированы финансовые активы около 3000 лиц, подозреваемых в причастности к преступлениям террористической и экстремистской направленности, на общую сумму свыше 100 млн руб. [5].

Кроме того, совместная деятельность Роскомнадзора и правоохранительных органов, направленная на защиту информационного пространства от пропаганды идеологии терроризма, привела к блокированию 6,5 тыс. и удалению около 50 тыс. пропагандистских террористических материалов в сети Интернет.

Наращиваются совместные усилия государственных структур, правоохранительных органов и общества по противодействию радикализации населения, прежде всего, молодежи, а также по профилактике нетерпимости и ксенофобии. Так, в 2021 г. около 15 млн человек приняли участие в проведении более 323 тыс. профилактических мероприятий в среде молодежи. В целях активизации работы по созданию контента, способствующего формированию антитеррористического сознания, Росмолодежью был проведен конкурс, в рамках которого было подготовлено 350 проектов в номинации «профилактика идеологии терроризма и экстремизма» [5].

Кроме того, в целях противодействия террористической угрозе необходимо продолжать работу по следующим направлениям:

- создание механизмов защиты информационного пространства от проникновения в сеть Интернет материалов, пропагандирующих и оправдывающих террористическую деятельность;
- снижение уровня радикализации различных групп населения, прежде всего, молодежи, а также повышение эффективности функционирования системы оказания на них профилактического воздействия, в том числе с целью формирования антитеррористического сознания;
- адресная профилактическая деятельность по сокращению числа россиян, покидающих страну с целью вступления в международные террористические организации и завербованных такими организациями;
- информационно-пропагандистская деятельность антитеррористической направленности;
- развитие организационных и иных мер, направленных на повышение результативности деятельности субъектов противодействия терроризму.

Таким образом, в Российской Федерации сформированы законодательные и организационные механизмы противодействия идеологии терроризма. Организовано распространение информационно-пропагандистских материалов антитеррористической направленности и предприняты меры, направленные на защиту информационного пространства. Однако, к сожалению, угроза терроризма во всем мире и в нашей стране будет сохраняться с учетом осложнения международной обстановки, дестабилизации социально-экономического состояния и

связанного с этим ухудшения социально-психологического климата. Поэтому важно продолжать развитие системы противодействия терроризму, используя самые современные технологические возможности.

Список литературы

1. Данные сайта МВД России. URL: <https://мвд.рф/> (дата обращения: 20.04.2022).
2. Данные Портала правовой статистики Генеральной прокуратуры Российской Федерации. URL: http://crimestat.ru/offenses_map (дата обращения: 20.04.2022).
3. Комплексный план противодействия идеологии терроризма в Российской Федерации на 2019-2023 годы / утвержден Президентом Российской Федерации 28 декабря 2018 г. № Пр-2665 // СПС «КонсультантПлюс». URL: <http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=EXP&n=510696&dst=100052#TcV5x3TglFrTEGvF2> (дата обращения: 20.04.2022).
4. Стратегия противодействия экстремизму в Российской Федерации до 2025 года / утверждена Президентом Российской Федерации 28.11.2014 № Пр-2753 (ред. от 29.05.2020) // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_194160/ (дата обращения: 20.04.2022).
5. Данные Национального антитеррористического комитета и Федерального оперативного штаба. URL: <http://nac.gov.ru/nak-prinimaet-resheniya/v-moskve-proshlo-itogovoe-zasedanie-nacionalnogo-0.html> (дата обращения: 20.04.2022).

Терехов М. Г.¹,

инспектор отдела международного сотрудничества

Московского университета МВД России имени В.Я. Кикотя

Научный руководитель:

Шаронов С. А.,

доктор юридических наук, доцент,

Почетный работник сферы образования Российской Федерации

ЗНАЧИМОСТЬ СТАНОВЛЕНИЯ ПРАВОВОГО РЕЖИМА ЦИФРОВЫХ АКТИВОВ В ОБЕСПЕЧЕНИИ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ (ПО ЛИНИИ ПРОТИВОДЕЙСТВИЯ ТЕРРОРИЗМУ И ЭКСТРЕМИЗМУ)

Как известно, для Российской Федерации стратегической задачей является обеспечение национальных интересов. Подчеркивается важность такой государственной позиции, тем, что деструктивные силы за рубежом и внутри государства предпринимают всевозможные попытки использования объективных социально-экономических трудностей государства в целях стимулирования негативных социальных процессов, обострения межнациональных и межконфессиональных конфликтов, манипулирования в информационной сфере, сети Интернет.

В свою очередь, международные террористические и экстремистские организации стремятся усилить пропагандистскую работу и работу по вербовке граждан, созданию на территории государства своих законспирированных ячеек, вовлечению в противоправную деятельность молодежи [3]. Для всех вышеизложенных явлений широко используются возможности сети Интернет, а также возможности децентрализованных финансовых инструментов по типу цифровых активов (криптовалют).

Объективная практика проявления в сети Интернет, находящейся под юрисдикцией государства, случаев противоправных действий с использованием цифровых активов (криптовалют), направленных на финансирование экстремизма и терроризма, целью которых является дестабилизация ситуации и нарушение суверенитета государственности, характеризуется как латентное, но распространенное и агрессивно влияющее на экономическую и общественную безопасность негативное явление.

Обуславливается такой вывод в свете последних событий, происходящих в юрисдикции члена организации ОДКБ – Республики Казахстан, которые в своем докладе на внеочередной сессии Совета коллективной безопасности ОДКБ также охарактеризовал Президент Российской Федерации В. В. Путин: «В Республике Казахстан можно было наблюдать агрессию международного терроризма, а боевики, которые участвовали в стычках, проходили подготовку за границей» [4].

Углубляясь в процессы подготовки и организации «гражданских революций», экономико-правовой аспект является наиболее выраженным и представляет наибольший интерес при исследовании произошедших событий.

¹ © Терехов М. Г., 2022.

Цель статьи охарактеризовать причины и условия складывающейся проблематики по отдельным существующим противоправным процессам с использованием цифровых активов и научные подходы к разрешению складывающейся проблематики.

Достижение поставленной цели представляется возможным посредством решения совокупности **задач**:

- 1) определить действующие нормативные правовые акты в исследуемой тематике;
- 2) определить мировые практики, отчеты ведущих финансовых организаций на тему оборота цифровых активов;
- 3) определить практический аспект оборота цифровых активов в противоправных целях, а также причины и условия, способствующие совершению противоправных действий;
- 4) дать предложения к разрешению складывающейся проблематики.

Методами исследования является анализ и синтез, исходя из полученной в ходе исследования информации и последующего анализа предлагается собственный подход к разрешению складывающейся проблематики.

Более подробно рассматривая на конкретном примере событий в начале 2022 г. в Республики Казахстан использование цифровых активов в противоправных целях, направленных на финансирование экстремизма и терроризма.

Первое, на что следует обратить особое внимание читателей – это использование цифровых активов в рассматриваемых событиях, что, резюмируя и забегаая вперед, является неотъемлемым экономическим элементом организации всей цепочки случившегося.

Предпосылками к объяснению такого вывода являются отдельные результаты исследования Кембриджского университета относительно процессов по созданию и развитию финансово-экономических процессов, связанных с оборотом цифровых активов (криптовалют) на территории Республики Казахстан.

Осенью 2021 г. Республика Казахстан заняла второе место в мире по добыче криптовалюты, говорится в исследовании Кембриджского университета. После того, как Китай признал майнинг нежелательной деятельностью на территории своего государства, Республика Казахстан достаточно быстро увеличила свою долю в мировом хэшрейте (совокупности операций) до 18 %. Его опередили лишь США с 35,4 % [5].

Изложенный факт и цифры говорят о том, что в Республике Казахстан произошел резкий финансово-экономический рост в цифровой среде (сети Интернет), что также отразилось естественным образом на всех традиционных экономических отношениях в обществе. Фактически появились дополнительные экономические блага в форме цифровых активов (в том числе выраженные криптовалютами), которые слабо контролируются в программно-техническом и гражданско-правовом регулировании во всей мировой практике государственного управления и национальной безопасности.

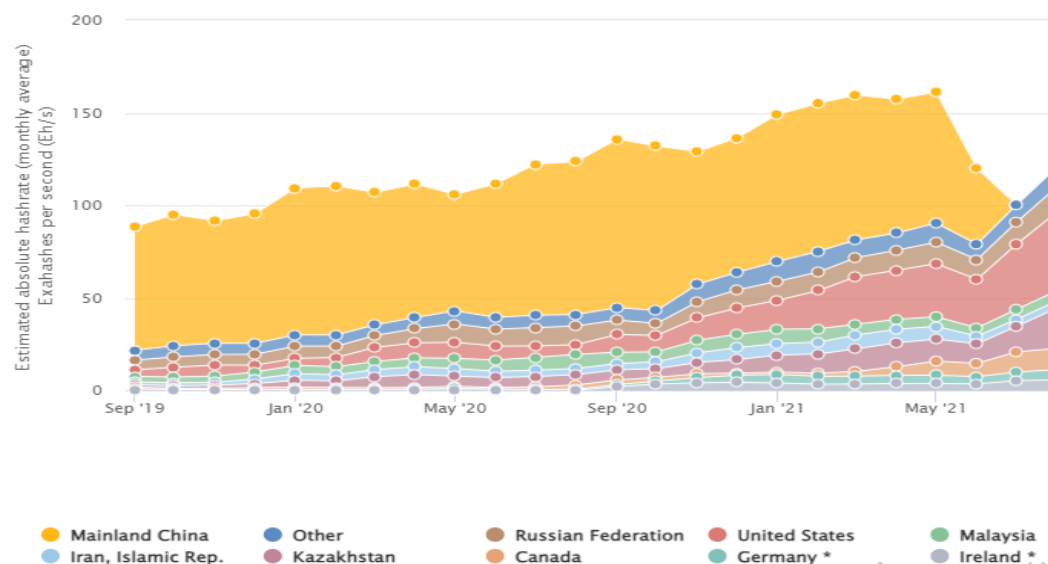


Рис. 1. Данные по анализу развития и изменений сетевого хешрейта за 2021 год [5]

Как следует из статистики за 2021 г., общий объем ВВП Республики Казахстан составил около 187,8 млрд долларов [6], а общий оборот за 2021 г. цифровых активов, выраженных криптовалютами, в мировой экономике составил свыше 3 трлн долларов.

Вышеприведенные данные свидетельствуют о том, что 18 % сетевого хешрейта пришедших в конце 2021 г. в экономику Республики Казахстан из общей суммы составляют 540 млрд долларов фактически зависят от вычислительных мощностей и энергии данного государства, а также значительно превышают ВВП Республики Казахстан.

Таким образом, фактически еще раз подтверждается мнение о критичности возможных последствий вхождения большого и нерегулируемого капитала цифровых активов, выраженных криптовалютой, в экономику государства, в частности, на рассматриваемом примере событий в Республике Казахстан.

Охарактеризовав тезисно общеизвестные причины и условия влияния финансово-экономического явления на складывающуюся проблематику по существующим противоправным процессам с использованием цифровых активов на примере событий в Республике Казахстан, представляется возможным в рамках причинно-следственной связи конкретизировать более частные аспекты причин и условий, которые проявились на фоне рассматриваемых событий в форме:

- терроризма;
- экстремизма.

Общие финансово-экономические явления спровоцировали более «острую» фазу событий – частные негативные явления внутри общества (на примере событий Республики Казахстан). Основными в более острой фазе происходящих событий стали беспорядки, которые охарактеризовали ряд поочередных противоправных действий, преследующих цели террористической и экстремистской направленности по дестабилизации суверенитета государства.

Из частных негативных явлений определяется второе негативное явление общего характера – миграционные процессы, которые не являются свойственными в том количестве, в котором происходили в период ноября–декабря 2021 г. и начале января 2022 г.

На фоне стабильного спада миграции на въезд в Республику Казахстан за последние 5 лет происходит резкий рост активности на въезд иностранных лиц из транзитных государств, которые имеют границы с государствами, где происходит смена государственной власти и иные явления. Вследствие чего и были спровоцированы частные рассматриваемые негативные явления в форме беспорядков на территории суверенного государства – Республики Казахстан.

Сопоставляя структуру элементов событий и явлений (общих и частных), необходимо сделать вывод о том, что в условиях финансово-экономического шока цифровой среды (сети Интернет) и традиционных институтов экономики от латентного входа достаточно большого количества финансового капитала на территорию государства, который имеет сложную программно-техническую, гражданско-правовую и экономическую природу:

1) сложным или почти невозможным становится для государственных органов, обеспечивающих национальную безопасность государства, процесс отслеживания транзакций криминально-подозрительных цифровых активов в местных криптовалютных обменниках и иных интернет-ресурсах, осуществляющих в той или иной форме оборот цифровых активов (криптовалют) среди цифровых активов на коммерческой основе, которые не являются криминальными;

2) становится невозможным предупредить описываемое негативное явление по линии обеспечения экономической и национальной безопасности (государственный аппарат до последнего не понимает масштаба возможных последствий, так как не обладает необходимой информацией о задействованных финансово-экономических ресурсах, вовлеченных в дестабилизацию национальной безопасности государства);

3) финансово-экономические ресурсы, направленные на дестабилизацию национальной безопасности государства, могут использоваться по трансграничной схеме (оплата цифровыми активами с территории соседних государств, подготовки беспорядков, экстремистов, террористических актов в различной форме). Данный процесс еще в большей степени затрудняет оперативно-служебную деятельность для правоохранительных органов государства, процесс определения, прогнозирования и предупреждения рассматриваемых событий на примере Республики Казахстан;

4) отсутствуют действующие гражданско-правовые режимы определения правового статуса, видов и свойств цифровых активов, а также нормативно-правовые акты, регулирующие отдельные сферы общественных отношений с использованием цифровых активов. Данный факт оказывает существенное влияние на последующее проведение следственных мероприятий, направленных на избличение как самих преступников, так и противоправных действий, совершаемых ими с использованием цифровых активов. В том числе, оказывает существенное

влияние на мероприятия после внесения судом возможных решений о привлечении к ответственности за такие противоправные деяния, чтобы устранить причины и условия, способствовавшие их свершению.

На основании вышеизложенного приходим к следующему промежуточному умозаключению о том, что к настоящему времени особенно важно уделять в своей деятельности пристальное внимание со стороны органов государственной безопасности таким инновационным и специфическим направлениям в экономическом секторе, как процесс оборота цифровых активов, выраженных в криптовалюте и иных формах.

Вышеизложенное уже более 5 лет активно прогрессирует, как глобальное, особо значимое, социальное, экономическое, программно-техническое и гражданско-правовое явление.

Для достижения второй части обозначенных целей в настоящей научной статье, следует перейти от характеристики к научным предложениям (подходам) по разрешению складывающейся проблематики. По его мнению, международное сообщество в условиях активных процессов цифровой глобализации имеют все инструменты для решения возникающих угроз национальной безопасности. Речь, в частности, идет и о уже действующих, например, в структуре ОДКБ мероприятиях, а также принятых нормативных правовых актах [2] в рамках инициирования таких мероприятий.

Безоговорочное внимание уделяется к настоящему времени вопросу подготовки высококвалифицированных специалистов в системе высшего образования и повышения квалификации, что достаточно логично, так как необходимость подготовленности по линии правоохранительной направленности в кадрах, которые имеют достаточные компетенции по расследованию подробно описываемых противоправных явлений с использованием цифровых активов (криптовалют), направленных на финансирование экстремизма и терроризма, на примере событий в Республике Казахстан – указывает на это.

Предпринятые шаги, которые уже сделаны, необходимо еще больше укреплять путем тесного взаимодействия государств по линии правоохранительных органов. В частности, существует потребность развивать такое научное направление как «цифровое право», которое по своей сущности является к настоящему времени фундаментальной наукой, изучающей феномен цифровизации общественных отношений по всем направлениям. Исследованием проблем, связанных с использованием и прогрессированием цифровых активов в различных проявлениях, например, в криптовалютах, является одним из неотъемлемых междисциплинарных институтов права, отнесенных к отрасли цифрового права.

Исходя из чего, ключ к решению проблем, обуславливающих использованием цифровых активов в противоправных целях, может быть успешно найден путем развития в науке на межгосударственном уровне вышеизложенных направлений цифрового права.

Впоследствии развитие перечисленных направлений станет серьезным катализатором роста создаваемых криминалистических, следственных методик по расследованию противоправных действий с использованием цифровых активов,

а также процесса установления гражданско-правового режима цифровых активов, который позволит осуществлять оборот цифровых активов в не криминальных целях законопослушным физическим и юридическим лицам.

Второй вывод, который относится к предложениям научного характера, в контексте большого оборота цифровых активов в цифровой среде (сети Интернет) обществом, неуклонно возрастает потребность в национальном регуляторе, который закрепит «рабочий» гражданско-правовой режим.

На основании чего предлагается на основе признаков, характеризующих ценностный и распорядительный характер для предметов оборота в цифровой среде (сети Интернет) в части цифровых активов (криптовалют), – выделять в национальном законодательстве более детально в обособленную категорию объектов гражданско-правового регулирования – «цифровое имущество», которое, с учетом значимых признаков, может «использоваться исключительно в цифровой среде (сети Интернет)».

Список литературы:

1. Решение Совета коллективной безопасности Организации Договора о коллективной безопасности от 14 октября 2016 г. «О Стратегии коллективной безопасности Организации Договора о коллективной безопасности на период до 2025 года». URL: https://odkb-csto.org/documents/statements/strategiya_kolletivnoy_bezopasnosti_organizatsii_dogovora_o_kollektivnoy_bezopasnosti_na_period_do_/.
2. Решение о базовой организации государств – участников Содружества Независимых Государств по подготовке кадров в сфере борьбы с преступлениями, совершаемыми с использованием информационных технологий, по образовательным программам высшего образования и дополнительным профессиональным программам от 5 апреля 2019 г.
3. О Стратегии национальной безопасности Российской Федерации: Указ Президента Российской Федерации от 02.07.2021 № 400 // Собрание законодательства Российской Федерации. 05.07.2021. № 27 (ч. 2). Ст. 5351.
4. Доклад Президента Российской Федерации В. В. Путина на внеочередной сессии Совета коллективной безопасности Организации Договора о коллективной безопасности. URL: <http://www.kremlin.ru/events/president/news/67568>.
5. Отчет Кембриджского центра альтернативных финансов (CCAF). URL: https://ccaf.io/cbeci/mining_map.
6. Официальная статистика ВВП за 2021 год в Республике Казахстан. URL: <https://www.gov.kz/memleket/entities/stat/press/news/details/242836>.
7. Санникова Л. В., Харитонов Ю. С. Цифровые активы: правовой анализ: монография. М. : 4 Принт, 2020.
8. Šmihula, Daniel. The waves of the technological innovations of the modern age and the present crisis as the end of the wave of the informational technological revolution. *Studia politica Slovaca*, – 1/2009. Bratislava, ISSN 1337-8163. P. 32–47.
9. Deutsche Bank Research / The Future of Payments: Part III. Digital Currencies: the Ultimate Hard Power Tool. 2019. P. 4–8.

10. Егорова М. А., Ефимова Л. Г. Понятие криптовалют в контексте совершенствования российского законодательства // Lex Russica. 2019. №7 (152). С. 130–139.
11. Ершов М. В. О некоторых проблемах цифровизации // Научные труды Вольного экономического общества России. 2019. № 6. С. 144–151.

Наумов Е. Е.¹,

курсант факультета подготовки

специалистов в области информационной безопасности

Московского университета МВД России имени В.Я. Кикотя

Пименова О. В.²,

доцент кафедры информационной безопасности

учебно-научного комплекса информационных технологий

Московского университета МВД России имени В.Я. Кикотя,

кандидат технических наук

АНАЛИЗ МЕТАДААННЫХ КАК СПОСОБ ИДЕНТИФИКАЦИИ ПРЕСТУПНИКА

Установление личности или идентификация преступника – это первоочередная задача в расследовании преступлений. Но часто правонарушитель не оставляет следов, которые явно указывают на его личность. Анализ метаданных файлов используется как один из способов идентификации преступника. Определим основные понятия.

Метаданные файлов – это данные, которые содержат информацию о самом файле. Как правило, в расследовании преступлений ценность для следствия имеют сведения об авторе, времени и дате создания файла, устройстве и особенно о географическом положении устройства при создании файла. Но помимо перечисленных данных, метаданные в себя включают также различную техническую информацию о файле.

Согласно Федеральному закону от 27.07.2006 № 149-ФЗ (ред. от 30.12.2021) «Об информации, информационных технологиях и о защите информации», *идентификация* – совокупность мероприятий по установлению сведений о лице и их проверке, осуществляемых в соответствии с федеральными законами и принимаемыми в соответствии с ними нормативными правовыми актами, и сопоставлению данных сведений с уникальным обозначением (уникальными обозначениями) сведений о лице, необходимым для определения такого лица [1].

С конца 1970-х гг. в штате Канзас орудовал серийный убийца ВТК (bind, torture, kill – «связывать, пытать, убивать»). Жертвами маньяка становились одинокие женщины и семьи. Желая обратить на себя внимание общественности, ВТК отправлял сообщения в полицию, газеты, радиостанции. В них он описывал различные обстоятельства и детали своих преступлений, прилагал доказательства (фотографии, личные вещи убитых). Однако полиция долгое время не могла найти убийцу. Доказательств, указывающих на конкретных людей, у следствия не было. Но в 2005 г. ВТК совершил свою первую серьезную ошибку: он подбросил коробку со своими сочинениями в машину на автомобильной парковке. Его действия и машину удалось записать на видеокамеру. Однако из видеозаписи удалось узнать только модель автомобиля: черный Jeep Grand Cherokee.

¹ © Наумов Е. Е., 2022.

² © Пименова О. В., 2022.

Через некоторое время убийца решил вести переписку с полицией в электронном формате. Он отправил в полицию дискету. Помимо послания маньяка следователи обнаружили удаленный файл Microsoft Word и восстановили его. Сам файл не содержал полезной для следствия информации. Но в метаданных документа упоминалась местная лютеранская церковь, а последние изменения внес автор по имени Деннис. Председателем церковного совета церкви оказался Деннис Рейдер, который владел черным Jeep Grand Cherokee. Последним доказательством его причастности стал анализ ДНК, полученный из других улик. Сейчас Деннис Линн Рейдер, отбывает 10 пожизненных сроков в тюрьме строгого режима Эль Дорадо в Канзасе [2; 3].

Приведенная история иллюстрирует то, каким образом метаданные файлов способны помочь следствию. Лицо, совершившее правонарушение, может различными способами скрывать свою личность, не оставляя правоохранным органам улик. В последние годы наиболее актуально в данном контексте рассматривать преступления, совершенные с использованием информационно-телекоммуникационных технологий. Используя средства анонимизации (VPN-подключения через иностранные сервера, Проху-сервера) и подставные авторизационные данные, преступники остаются неизвестными. Однако преступник во время общения с жертвой или правоохранными органами (в случаях с маньяками и прочими преступниками, желающими славы) может отправлять фотографии, видеозаписи, документы, которые хранят в себе различные данные о владельце или устройстве, на котором файл был создан или изменен. Несмотря на то, что эти данные не позволяют однозначно говорить о виновности или причастности лица к совершению преступления, они могут дать следствию дополнительные сведения о местоположении и личности преступника.

Изучение метаданных фотографий может помочь правоохранным бороться с преступлениями в «даркнете». Большинство продавцов на торговых площадках, занимающихся незаконной торговлей запрещенными товарами, не обладают достаточными знаниями в области информационной безопасности. По этой причине некоторые из них не знают про то, что их личность может быть раскрыта благодаря метаданным фотографий незаконного товара, которые они выкладывают на площадку. Например, 13 сентября 2016 г. студентами Гарвардского университета Майклом Роусом и Полом Лискером были опубликованы результаты проведенного ими исследования [4]. Они создали программу, изучающую фотографии проекта Black-Market Archives на предмет наличия в них метаданных, указывающих на личность создателя фотографии. Данный проект занимается хранением копий фотографий, опубликованных на различных незаконных торговых площадках даркнета. Данное исследование показало, что существует немало продавцов, которые загрузили на площадку фотографии своих товаров вместе с информацией о себе, в том числе координаты своего местоположения.

В ходе исследования было просканировано 7522284 фотографии. Из них было лишь 226471 уникальных изображений. Далее авторы исследования изу-

чили отобранные изображения на наличие в них геометок. Среди проанализированных изображений было найдено 2276 изображений, удовлетворявших условию. Правда, только 226 геометок были уникальными. Это говорит о том, что продавцы публиковали несколько фотографий, содержащих геометки одного и того же местоположения.

Данное исследование показало, что действительно есть возможность произвести идентификацию некоторых продавцов на незаконных площадках. Причиной этого является халатность при обеспечении анонимности. В этом виноваты, как сами продавцы, которые не удаляют свои геометки с фотографий, так и торговые площадки, которые не беспокоятся о защите личности своих клиентов. Однако сами авторы исследования отметили одну особенность. За время проведения исследования было замечено, что фотографии с одной площадки были заменены на такие же, но без геолокации. Как подмечают авторы, администрация скорее всего смогла обнаружить эту уязвимость и устранить.

За последние годы на подобных площадках стали чаще внедрять очищение атрибутов изображений автоматизировано, но и сами продавцы стали более осведомленными и осторожными. Оба эти факта обуславливают снижение результативности анализа метаданных фотографий на нелегальных торговых площадках даркнета. Однако 5 апреля 2022 г. прокуратура Франкфурта-на-Майне и Федеральное ведомство уголовной полиции Германии арестовали серверную инфраструктуру крупнейшей даркнет-площадки Hydra-Market, осуществляющей незаконную торговлю наркотическими и психотропными веществами, а также прочими товарами, продажа которых ограничена или запрещена на территории Российской Федерации [5]. 14 апреля 2022 г. Мещанский суд г. Москвы арестовал предполагаемого сооснователя площадки Дмитрия Павлова [6]. Данные события способствуют переходу продавцов на другие площадки, в том числе недавно созданные. Поэтому можно утверждать, что в ближайший год количество ошибок как со стороны сайтов, так и со стороны продавцов немного увеличится.

Идентификация преступников с помощью анализа метаданных файлов остается актуальной. Она неплохо может себя показать при расследовании преступлений, совершенных неопытными мошенниками.

Список литературы

i. Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 30.12.2021) «Об информации, информационных технологиях и о защите информации». Статья 2. Основные понятия, используемые в настоящем Федеральном законе // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_61798/c5051782233acca771e9adb35b47d3fb82c9ff1c/ (дата обращения: 20.04.2022).

2. The Grisly Story Of Dennis Rader, The Man No One Suspected Was The BTK Killer – Allthatsinteresting.com. URL: <https://allthatsinteresting.com/dennis-rader-btk-killer> (дата обращения: 20.04.2022).

3. Profile of a Serial Killer: Dennis Rader, the BTK Strangler – Owlcation URL: <https://owlcation.com/social-sciences/Profile-of-a-Serial-Killer-Part-5-Dennis-Rader-The-BTK-Killer> (дата обращения: 20.04.2022).

4. Illuminating the Dark Web. Searching for geotags in dark net markets. | Paul Lisker/Michael Rose | Medium. URL: <https://medium.com/@roselisker/illuminating-the-dark-web-d088a9c80240#.1d0ltbpny> (дата обращения: 22.04.2022).

5. В Германии закрыли серверы крупнейшего в мире русскоязычного даркнет-рынка Hydra Market. Коммерсантъ, 05.04.2022. URL: <https://www.kommersant.ru/doc/5294029> (дата обращения: 22.04.2022).

6. В Москве арестовали предполагаемого основателя даркнет-рынка «Гидра». РИА Новости, 14.04.2022. URL: <https://ria.ru/20220414/arrest-1783623004.html> (дата обращения: 22.04.2022).

Трухачев А. А.¹,

курсант факультета подготовки сотрудников

для оперативных подразделений полиции

Московского университета МВД России имени В.Я. Кикотя

Научный руководитель:

Гончар В. В.,

начальник кафедры информационной безопасности

учебно-научного комплекса информационных технологий

Московского университета МВД России имени В.Я. Кикотя,

кандидат юридических наук, доцент

СВЯЗЬ НЕЗАКОННОГО ОБОРОТА НАРКОТИКОВ С ТЕРРОРИЗМОМ В СОВРЕМЕННЫХ УСЛОВИЯХ

Доподлинно известно, что террористические организации нуждаются в своем финансировании. К источникам финансирования терроризма можно отнести большой перечень. В статье будет рассмотрен такой источник финансирования как выручка от незаконного оборота наркотиков. Для террористических организаций именно этот источник считается наиболее важным и приносящим колоссальное количество ресурсов.

Общественная опасность данных преступлений наиболее серьезно затрагивает общественные течения, связанные с безопасностью всего мира. С одной стороны, это террористические акты, с другой, незаконный оборот наркотиков. Значительная угроза миру заключается в том, что два этих элемента способствуют существованию друг друга. Террористские организации содействуют и организуют помощь в реализации наркопродукции. В свою очередь наркоторговцы предоставляют финансовые ресурсы на существование террористических организаций.

Примером финансирования терроризма может послужить приговор суда в отношении Мохаммеда, который сначала осуществил сбыт наркотической продукции, а затем купил ракетные комплексы для террористического движения «Талибан».

Также учитывая географию нахождения террористических организаций, то можно увидеть непосредственную связь с географией плантаций растительных наркотиков. Так, к примеру, Революционные вооруженные силы Колумбии располагаются вблизи плантаций наркобизнеса и имеют под своим контролем 25 % площади растительных наркотиков. Если детально рассмотреть сведения из Интерпола, то можно увидеть линии финансирования экстремистских организаций на Ближнем Востоке за счет средств, полученных от реализации наркотических веществ. Данные организации не только получали часть прибыли, но и участвовали в транспортировке поставок наркопродукции за рубеж.

¹ © Трухачев А. А., 2022.

Особую роль в финансировании террористических организаций занимает продажа наркотиков, используя информационные технологии, позволяющие реализовывать продукцию анонимно.

На сегодняшний день большое внимание уделяется борьбе с незаконным оборотом наркотиков, который организован на базе сетевых информационных ресурсов. Трудно не согласиться с мнением ученого О. П. Грибунова: «Ситуация с незаконным оборотом наркотиков в последнее время в нашем государстве остается предельно напряженной» [1, с. 19–28]. Связано это, прежде всего, с тем, что распространители наркотических средств активно используют и развивают технологии, позволяющие осуществлять сбыт продукции. Организаторы наркобизнеса используют сеть Интернет не только в качестве средства сбыта продукции, но и в качестве коммуникативной среды, позволяющей вербовать продавцов и курьеров.

Информационные технологии открывают возможности бесконтактной покупки наркотических средств, что значительно осложняют работу правоохранительных органов. Особое внимание стоит обратить на интернет-ресурс «DarkNet», данная информационная среда характеризуется наиболее высокой степенью анонимностью торговой операции. В Российской Федерации на данный момент существует интернет-ресурс, который обеспечивает реализацию деятельности наркоторговцев. Такой торговой площадкой признается «Гидра». С 2015 г. «Гидра» зарекомендовала себя как наиболее удобный сайт, позволяющий оптимально работать продавцам, а также сохраняющий анонимность покупателям.

Информационные ресурсы Интернета имеют огромные технические перспективы, что усложняет раскрытие преступлений, связанных с использованием межнациональной сети. Современные интернет-ресурсы обеспечивают наркоторговцам высокий уровень конспирации, а также открывают огромное поле шифрования связи.

МВД России рассматривает как одно из приоритетных направлений деятельности правоохранительных органов своевременное выявление, предупреждение, пресечение и раскрытие преступлений в сфере наркооборота и борьбу с последующим финансированием терроризма, в котором используются доходы от наркооборота.

Само по себе раскрытие преступлений, которые реализуются с помощью интернет-ресурсов, является весьма трудоемким процессом. Необходимой частью этого процесса является изучение той информационной сети, где обитает криминальная среда. Именно поэтому для раскрытия подобных преступлений, требуются особые навыки и знания в сфере информационных технологий [2, с. 119–122]. Камнем преткновения при раскрытии преступлений, связанных с информационными средствами коммуникации, оказывается определение электронных следов. Необходимо отметить, что использование электронных или «виртуальных» следов выступает обязательным условием решения оперативно-розыскных задач при раскрытии преступлений, связанных с незаконным оборотом наркотических средств в интернет-среде.

Таким образом, изложенное позволяет сформулировать вывод, что противодействие преступности в сфере оборота наркотиков и последующего финансирования террористических организаций, руководством страны отнесено к числу приоритетных направлений деятельности МВД России.

Список литературы

1. Грибунов О. П., Герасимов П. А., Косенко В. Н. Психоактивные вещества синтетического происхождения как предмет преступлений, связанных с незаконным оборотом наркотиков: некоторые аспекты противодействия их распространению / О. П. Грибунов, П. А. Герасимов, В. Н. Косенко // Вестник Восточно-Сибирского института МВД России. 2015. № 4 (75). С. 19–28.
2. Колычева А. Н., Васюков В. Ф. Отдельные аспекты судебной компьютерной экспертизы, назначаемой при расследовании преступлений, совершенных с использованием сети Интернет / А. Н. Колычева, В. Ф. Васюков // Расследование преступлений: проблемы и пути их решения. 2019. № 3 (25). С. 119–122.

Фарахиев Д. М.¹,

*слушатель факультета подготовки специалистов
по программам высшего образования
Казанского юридического института МВД России*

Минзянова Д. Ф.²,

*старший преподаватель кафедры
оперативно-разыскной деятельности
Казанского юридического института МВД России*

ИННОВАЦИОННЫЕ ТЕХНОЛОГИИ ПРОТИВОДЕЙСТВИЯ ТЕРРОРИЗМУ В ПРОЦЕССЕ ГЛОБАЛИЗАЦИИ

На современном этапе развития общества терроризм является наиболее опасным видом преступления. Согласно постановлению Пленума Верховного Суда Российской Федерации от 09.02.2012 № 1: «Терроризм представляет угрозу международному миру и безопасности, развитию дружественных отношений между государствами, сохранению территориальной целостности государств, их политической, экономической и социальной стабильности, а также осуществлению основных прав и свобод человека и гражданина, включая право на жизнь» [1]. В настоящее время в период экономических преобразований в России обостряется политическая борьба, усложняются международные отношения, снижается уровень жизни населения. В связи со снижением уровня заработной платы в правоохранительных органах значительно сокращается количество кадров, что ведет к ослаблению деятельности по предупреждению и противодействию преступлений, в том числе терроризма.

Терроризм на сегодняшний день является глобальной проблемой, признанной всеми цивилизованными государствами. Таким образом, поиск результативных средств противодействия и предупреждения терроризма является весьма актуальным вопросом.

Процесс глобализации, по нашему мнению, непосредственно воздействует на международный терроризм и кибертерроризм, который развивается и трансформирует способы своего распространения. Финансирование и техническая обеспеченность терроризма в настоящее время набирает обороты. В целях эффективной организации противодействия терроризму следует четко понимать детерминанты возникновения такого преступного явления. Анализируя ситуацию в мире, мы обнаруживаем, что происходит все большая популяризация религиозного экстремизма, национализма и сепаратизма. К сожалению, в разных странах продолжают вооруженные конфликты и боевые действия и вследствие этого возникает проблема беженцев, появившихся в результате фактического распада исторических государств Ближнего Востока, вызванного внешним вмешательством [2, с. 71]. Так, в 2016 г. мигранты, причастные к радикальным исламистским группировкам, совершили несколько терактов в городах Германии. И если

¹ © Фарахиев Д. М., 2022.

² © Минзянова Д. Ф., 2022.

уличная преступность усилиями полиции со временем пошла на спад, то тема террористических атак по-прежнему остается наиболее болезненной.

В то же время следует отметить, что противодействие терроризму может быть результативным лишь в случае применения системы взаимосвязанных мер политического, социально-экономического, организационного, идеологического и правового характера.

Информационно-аналитическое обеспечение противодействия терроризму можно выделить как одно из главнейших направлений взаимодействия между субъектами предупреждения. Основными его задачами являются:

- исследование основных детерминантов терроризма и анализ угроз террористического характера;
- расследование процессов, препятствующих усилиям по борьбе с терроризмом, и принятие результативных мер по противодействию;
- формирование условий качественного взаимодействия субъектов предупреждения;
- использование опыта зарубежных стран в борьбе с терроризмом;
- организация безопасного информационного пространства;
- организация повышения профессиональной подготовки кадрового потенциала в области аналитического обеспечения противодействия терроризму.

Последние годы интеграция цифровых технологий в повседневную жизнь в мире значительно возросла, особенно за счет использования социальных сетей. Хотя эта тенденция открывает широкий спектр возможностей для развития, свободы выражения мнений, участия в политической жизни и т. п., она также увеличивает риск того, что потенциально уязвимая часть населения – молодежь будет подвергаться воздействию террористического онлайн-контента, создаваемого террористическими и воинствующими экстремистскими группами в Интернете. Искусственный интеллект заслужил внимание во всем мире как инструмент, который может обрабатывать огромные объемы данных и обнаруживать закономерности и корреляции в данных, невидимых человеческому глазу, что значительно повышает эффективность и результативность анализа сложной информации, эти преимущества могут быть использованы и в области борьбы с терроризмом.

Тактически правильно при расследовании террористических актов использовать искусственные нейронные сети. Искусственные нейронные сети уже продемонстрировали свою эффективность в традиционной правовой сфере. Нейронные сети могут реализовывать важные тактические действия: распознавание, предсказание (прогнозирование), классификацию.

Рассмотрим каждое тактическое действие подробнее. Под распознаванием следует понимать необходимые признаки, например, идентификация внешности личности или государственных знаков транспортного средства. В данной ситуации системе предъявляется объект и она должна ответить только на один вопрос: «является ли данный объект искомым?». Так, к примеру, в Китае компания *Watrix* сформировала инновационную технологию на базе искусственного интел-

лекта, которая позволяет идентифицировать граждан по походке и телосложению. Данная технология дает возможность распознать, кто перед ним, даже если нет лица или в случае, когда гражданин отворачивается от камеры или надевает маску. Функционирование системы строится на анализе силуэта, роста, веса, скоростных и иных характеристик и идентификации их с данными имеющимися в базе [3].

Следующая возможность – это возможность прогнозировать преступное поведение террористического характера, устанавливать будущее состояние той или иной информационной системы или ее отдельных показателей. Например, в Соединенных Штатах Америки (далее – США), с 2012 по 2018 гг. функционировал проект под названием «Палантир» [4], собиравший сведения о жителях Нового Орлеана: их социальном окружении, трудовой деятельности, передвижениях, активности в социальных сетях и т. д. На основе этих сведений искусственный интеллект анализировал социальную картину и пытался определить лиц, склонных к совершению преступления.

Под возможностью классификации следует понимать разделение сведений по определенным видам (группам) в соответствии с параметрами, которые были заданы ранее. Виды классификации операций уже внедряются в деятельность правоохранительных органов нашей страны. К примеру, в рамках борьбы с терроризмом и экстремизмом в Федеральной службе войск национальной гвардии Российской Федерации разрабатываются системы криминалистического учета [5]. Следует отметить, что криминалистические учеты имеются и в других правоохранительных органах.

Конечно же, данным списком возможности системы искусственного интеллекта не ограничиваются. Огромное значение в процессе противодействия терроризму имеет и использование камер видеонаблюдения с функцией искусственного интеллекта. Так по мнению А. Фархади имеется возможность обучить искусственный интеллект распознавать признаки того, что человек вооружен и намерен совершить теракт [6]. Данная система должна сканировать видеозаписи с камер видеонаблюдения в *online*-режиме (рис. 1).



Рис. 1. Пример камеры видеонаблюдения, управляемой искусственным интеллектом

Ряд организаций на сегодняшний день внедрили подобные системы видеонаблюдения. Так, в одной из школ в Висконсине пользуется данными технологиями от компании *Actuate AI* [7]. Разработчики утверждают, что камеры обнаруживают оружие в течение 15 секунд и оповещают сотрудников полиции.

Основная проблема, которая может возникнуть, – это неправильное определение (к примеру, схожие предметы: оружие – дрель и др.). Также на неправильное определение оружия может повлиять недостаток света или переотражение света.

На сегодняшний день в нашей стране широко распространены «умные» видеокамеры, которые идентифицируют личность человека, который может оказаться потенциальным преступником или человеком, склонным к терроризму. В московских системах наблюдения применяются нейросети от компании *NtechLab* [8], которые идентифицируют лицо человека, сравнивая его внешность с фотографиями из базы данных. Если алгоритм считает, что выявил преступника, полиция получает уведомление с изображением, текущем местонахождением и личными данными.

Думается, если тактически правильно выстраивать расследование преступлений террористической направленности, то лица, совершившие данные преступления, понесут справедливое наказание. Справедливое наказание имеет для граждан очень важное превентивное значение [9]. Важно помнить, что терроризм можно одолеть лишь сообща. Российская история и весь мировой опыт говорят о том, что для эффективной борьбы с терроризмом нужна консолидация правоохранительных органов, ученых, общества и государства в целом.

Список литературы

1. О некоторых вопросах судебной практики по уголовным делам о преступлениях террористической направленности: постановление Пленума Верховного Суда Российской Федерации от 09.02.2012 № 1 (ред. от 03.11.2016) // СПС «КонсультантПлюс» (дата обращения: 20.04.2022).
2. Кобец П. Н. О природе терроризма, его причинах, условиях и основных детерминантах / П. Н. Кобец // Фундаментальные и прикладные исследования в современном мире. 2017. № 17-3. С. 71–72. EDN: YGGBZR.
3. В Китае камеры начали определять личность людей по походке. Да, даже круче, чем в «Черном зеркале». URL: <https://medialeaks.ru/0811jkr-you-are-how-you-walk> (дата обращения: 19.04.2022).
4. Саблинская И. Предсказать преступление: искусственный интеллект учится разыскивать бандитов. URL: <https://pravo.ru/news/200927> (дат обращения: 19.04.2022).
5. Предсказать преступление: искусственный интеллект учится разыскивать бандитов. URL: <https://pravo.ru/news/200927> (дата обращения: 19.04.2022).
6. Умное оружие и мониторинг соцсетей: сможет ли ИИ предотвращать теракты. URL: <https://trends.rbc.ru/trends/social/6169691a9a794774ed3f51d6> (дата обращения: 19.04.2022).

7. AI Gun Detection. URL: <https://actuate.ai/ai-security/gun-detection> (дата обращения: 19.04.2022).

8. Общественная безопасность. URL: <https://ntechlab.ru/solution/public-safety/> (дата обращения: 19.04.2022).

9. Суслин Э. В. Теоретико-правовые аспекты судейского усмотрения в уголовном процессе / Э. В. Суслин, С. В. Назаров // Вестник Томского государственного университета. Право. 2020. № 36. С. 115–125. EDN: NWUZUA.

Филимонова Ю. В.¹,

курсант факультета подготовки специалистов

в области информационной безопасности

Московского университета МВД России имени В.Я. Кикотя

Научный руководитель:

Клочкова Е. Н.,

доцент кафедры специальных информационных технологий

учебно-научного комплекса информационных технологий

Московского университета МВД России имени В.Я. Кикотя

ОСОБЕННОСТИ ПРОФИЛАКТИКИ И БОРЬБЫ С ПРОЯВЛЕНИЯМИ ЭКСТРЕМИЗМА И ТЕРРОРИЗМА СРЕДИ МОЛОДЕЖИ В СЕТИ ИНТЕРНЕТ

Современные реалии таковы, что под деструктивным влиянием различных факторов (социальных, экономических и политических), молодые люди оказались той частью общества, которая стала наиболее склонной к формированию радикальных взглядов и убеждений. Именно это, в первую очередь, способствует вовлечению молодых граждан в ряды экстремистских и террористических организаций, активно эксплуатирующих в своих политических интересах российскую молодежь.

В последние годы в России наблюдается резкий скачкообразный рост различных экстремистских организаций и движений, заинтересованных в вовлечении в свою деятельность молодых людей и подростков, т. е. тех, кто еще достаточно твердо не определился в своих идеологических приоритетах. Об этом свидетельствует анализ статистических данных за последние несколько лет – 80 % лиц из числа осужденных не достигли возраста 30 лет. Более того, членами неформальных молодежных организаций экстремистско-националистической направленности нередко являются несовершеннолетние лица в возрасте от 14 до 18 лет.

Криминологический анализ данного состава преступлений показывает, что чаще субъектами преступного посягательства выступают лица мужского пола, реже женского. В силу своего возраста, ряда социально-психологических, физиологических и демографических особенностей, будучи наиболее восприимчивыми к идеологическому воздействию, подверженными юношескому максимализму, а также радикальным направлениям, они составляют основу рядового состава бандформирований с целью осуществления террористических актов.

Можно выделить следующие основные особенности экстремизма в молодежной среде:

- формируется преимущественно в маргинальной среде, он постоянно подпитывается неопределенностью положения молодого человека и его неустановившимися взглядами на происходящее;

¹ © Филимонова Ю. В., 2022.

- чаще всего проявляется в системах и ситуациях, характерных отсутствием действующих нормативов, установок, ориентирующих на законопослушность, консенсус с государственными институтами;

- проявляется чаще в тех обществах и группах, где проявляется низкий уровень самоуважения или же условия способствуют игнорированию прав личности;

- данный феномен характерен для общностей не столько с так называемым «низким уровнем культуры», сколько с культурой разорванной, деформированной, не являющей собой целостности;

- экстремизм соответствует обществам и группам, принявшим идеологию насилия и проповедующим нравственную неразборчивость, особенно в средствах достижения целей [1].

Резко растущая информатизация общества вносит в деятельность террористических организаций свои коррективы, заключающиеся в возможности распространения своей идеологии и убеждений в различных интернет-ресурсах (блогах, форумах, чатах и т. д.). На площадках такого рода собирается аудитория, численность которой достигает цифр в несколько сотен тысяч активных пользователей. Легко трансформирующееся и несформировавшееся сознание молодежи дает экстремистам возможность осуществления всевозможных методов использования Интернета в террористических целях. К числу таких относятся:

- ведение активной пропаганды идеологии экстремизма и терроризма (вербовка, подстрекательство и радикализация);

- финансирование неформальных молодежных экстремистских группировок;

- подготовка террористов;

- навязывание своих ценностей и взглядов, заключающееся во внедрении собственных идеалов путем уничтожения исконных.

Для достижения своих целей используют наиболее популярные среди молодежи социальные сети, такие как «ВКонтакте», «Twitter», «Telegram». Нередко сайты содержат подробные инструкции по самостоятельному изготовлению взрывчатых устройств, совершению террористических актов и «националистических» убийств. Отсюда возникает резкая необходимость ответных действий со стороны правоохранительных органов, заключающихся в осуществлении ежедневного мониторинга интернет-ресурсов на предмет обнаружения экстремистских идей, призывов и взглядов, а также в оперативной проверке информации по фактам наличия в социальных сетях сведений о подготовке и совершении таких преступлений.

Существующая на сегодняшний день система законодательства Российской Федерации, освещающая правовую стратегию противодействия пропаганде терроризма и экстремизма в Интернете, а, в частности, в социальных сетях, по своей сущности обладает, если не исчерпывающим, то достаточно полным набором правовых норм.

В 2012 г. на территории Российской Федерации ввели постоянную цензуру на социальные сети. Практика применения уголовного законодательства свидетельствует о наиболее ходовых составах преступлений данной направленности, в число которых входят ст.ст. 280 и 282 УК РФ. По данным сравнительного обзора информационно-аналитического центра «Сова», осуществляющего мониторинг применения антиэкстремистского законодательства в России, наблюдается сильный рост числа осужденных за «экстремистские» высказывания в сети Интернет, преимущественно по ст. 282 УК РФ. Об этом свидетельствует статистика осужденных за публичные высказывания по ряду ходовых статей (ст.ст. 282, 280, 280.1, 205.2, 354.1, чч. 1, 2 ст. 148 УК РФ): в 2017 г. более 650, в 2018 г. – 731, в 2019 г. – 432, тогда как в начале десятилетия таковых насчитывалось менее двухсот ежегодно [2].

На 2021 г. пришелся новый этап ужесточения интернет-регулирования, в этом году 12 февраля было принято постановление, позволяющее Роскомнадзору замедлять трафик популярных платформ с целью ограничения доступа к информации, которая представляет угрозу безопасности страны, а к таковой относится и информация, запрещенная к распространению российскими законами. Эти меры в марте были применены к социальной сети Twitter, которая, по мнению российских властей, не удаляла в оперативном порядке запрещенный в России контент.

Кроме того, 24 февраля были подписаны поправки к Кодексу об административных правонарушениях (КоАП РФ), в которых устанавливалась административная ответственность для владельцев интернет-площадок за дискриминацию российских граждан по этническому, религиозному и иным признакам, за удаление «общественно значимой информации» и т. д. Таким образом, отстаивая интересы интернет-проектов российских СМИ, власти поставили перед онлайн-платформами фактически невыполнимые требования, в соответствии с которыми платформа не сможет удалять контент, нарушающий ее внутренние правила, но не запрещенный российским законодательством.

С целью противодействия распространению данной идеологии в сети Интернет создаются различные интернет-ресурсы, формирующие единые информационные антитеррористические пространства. К числу таких сайтов относится портал «Наука и образование против террора», целевая аудитория которого в основном обучающиеся и преподаватели образовательных организаций. Функционал портала позволяет ознакомиться как с актуальными новостями по данному вопросу, так и с различными материалами, направленными на недопущение формирования у пользователей идеологии экстремизма и терроризма. Также можно выделить сайт «Молодежь за Чистый Интернет», привлекающий в свои ряды политически активную часть населения России и других стран для поиска всевозможных решений проблематики идеологической борьбы с экстремизмом и терроризмом в современном мире.

Помимо этого, при поддержке Министерства науки и высшего образования Российской Федерации реализован проект Национальный центр информационного противодействия экстремизму и терроризму в образовательной сфере и сети

Интернет (далее – НЦПТИ) – диалоговая площадка, посредством которой осуществляется связь экспертов научной и педагогической среды с ведущими членами молодежных организаций и госструктурами, занимающимися вопросами противодействия экстремизму в сети Интернет и образовательной среде. Сайт оснащен рядом полезных функций: просмотр Интерактивной карты антитеррористической деятельности в образовательных организациях и научных учреждений Российской Федерации; возможность отправки информации о противоправных материалах через анонимную форму «Сообщить о противоправном контенте»; подборка проводимых мероприятий данной направленности (лекции, встречи, конференции и т. п.).

Согласно ст. 13 Федерального закона «О противодействии экстремистской деятельности» на территории Российской Федерации запрещено распространение экстремистских материалов, а также их производство или хранение в целях распространения. Существенная доля совершенных преступлений экстремистской направленности приходится именно на несовершеннолетних. Отсюда следует сделать вывод о целесообразности усиления профилактических работ среди молодежи, в том числе и несовершеннолетних, путем привлечения их к мероприятиям воспитательного характера, с целью контроля криминальной ситуации в данной сфере, а также пресечения экстремистской преступности в целом. К числу таких можно отнести уроки толерантности, просветительских проектов и лекций по вопросам толерантности, прививающие ее основы. Одним из таких примеров выступает Международный день толерантности, ежегодно отмечающийся в Российской Федерации 16 ноября, способствующий воспитанию толерантного мировоззрения и межнационального общения у молодежи.

Согласно ст. 5 Федерального закона от 25 июля 2002 г. № 114-ФЗ «О противодействии экстремистской деятельности» такого рода работа должна быть инициирована, в первую очередь, федеральными органами государственной власти, органами власти субъектов Российской Федерации, органов местного самоуправления, осуществляющими в пределах своей компетенции профилактические, воспитательные и пропагандистские меры с целью предупреждения угроз терроризма и экстремизма. Выявление на ранних этапах и оперативное принятие необходимых профилактических мер способствуют в значительной степени недопущению формирования у подростков девиантного поведения, проявляющегося в склонности к совершению противоправных действий.

Противодействие идеологии экстремизма и терроризма в социальных медиа – это информационная война современных реалий, где борьба ведется за умы и души подрастающего поколения. Осуществляющееся на регулярной основе противостояние экстремистской и террористической пропаганде – одно из важнейших направлений обеспечения национальной безопасности Российской Федерации.

Список литературы

1. Организация экстремистского сообщества: проблемы квалификации и доказывания: пособие / П. В. Агапов и др.; под ред. В. В. Меркурьева; Акад. Ген.

прокуратуры Российской Федерации. М., 2013.

2. Антиэкстремистская политика в России, Казахстане, Кыргызской Республике и Таджикистане. Сравнительный обзор. М. : Центр «Сова», 2020. URL: <https://www.sova-center.ru/files/books/wg-4-2020-rus.pdf> (дата обращения: 06.04.2022).

Хаярова Э. А.¹,
студентка КФ ФГБОУВО
«Российский государственный университет правосудия»

Эркаева С. А.²,
студентка КФ ФГБОУВО
«Российский государственный университет правосудия»

Научный руководитель:
Шевко Н. Р.,
доцент кафедры уголовно-правовых дисциплин
Казанский филиал ФГБОУВО «Российский
государственный университет правосудия»,
кандидат экономических наук, доцент

ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ ТЕРРОРИЗМУ В МОЛОДЕЖНОЙ СРЕДЕ

Характеризуя современное общество, нельзя не упомянуть об информационной среде, где молодое поколение проводит большую часть своего времени. Международные социальные сети, интернет-ресурсы востребованы среди молодежи, о чем свидетельствуют статистические показатели Федеральной службы государственной статистики (далее — РОССТАТ) по использованию сети Интернет возрастными группами населения за 2021 г. По данным РОССТАТ 38 % лиц, отнесенных к возрастной группе от 15 до 34 лет, используют Интернет до 8 часов каждый день [3].

Следует отметить, что информационная среда служит, как источником полезной информации, необходимой для учебного, рабочего процесса, так и средой, где часто распространяются ложные сведения о тех или иных явлениях, которые часто направлены на провокацию отдельных слоев населения [5]. Кроме того, зачастую в сети проявляются факты незаконной торговли оружием, запрещенными веществами, предлагаются различные схемы мошенничества, вербовка молодого поколения; размещение противоправных материалов пропагандистского характера подчеркивает необходимость правового регулирования деятельности в информационной среде.

Актуальность рассматриваемого вопроса проявляется в том, что в настоящее время в сети Интернет распространено большое количество ложной информации, не соответствующей действительности. В связи с распространением фейковой непроверенной, а часто и лживой информации в сети Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (далее — Роскомнадзор) обязала средства массовой информации (далее — СМИ) обращаться только к официальным российским источникам. С перечнем зарегистрированных СМИ можно ознакомиться на сайте Роскомнадзора [2].

¹ © Хаярова Э. А., 2022.

² © Эркаева С. А., 2022.

Кроме того, в связи с тем, что молодое поколение отличается своими социально-психологическими, физическими особенностями, неустойчивой психикой и мировоззрением, наиболее быстро поддается идеологическому воздействию и провокациям в других отраслях общественной жизни, именно молодые люди зачастую и становятся завербованными участниками международных террористических организаций, что, несомненно, является угрозой безопасности любого государства.

Для наиболее полного понимания затрагиваемой проблемы необходимо обратиться к понятиям. Под терроризмом законодательство подразумевает идеологию насилия или какое-либо воздействие на деятельность государственных органов власти, связанных с противоправными насильственными действиями [1]. Действия, связанные с организацией террористического акта, с подстрекательством к нему, относятся к террористической деятельности. Кроме того, к ней относятся вербовка, вооружение или же обучение-использование террористов, основную массу которых составляет молодежь.

Часто террористы с целью привлечения в свои ряды новых участников, как правило, молодые слои населения, используют метод пропаганды террористических идей, связанных с призывом к осуществлению насилия. Противодействие терроризму проявляется в его предупреждении, в выявлении террористического акта, раскрытии и расследовании преступных посягательств.

Федеральный закон «О противодействии терроризму» [1] позволяет Федеральной службе безопасности Российской Федерации (далее – ФСБ) привлекать для борьбы с терроризмом вооруженные силы, которые, в частности, могут использоваться для «пресечения полетов воздушных судов, используемых для совершения террористического акта либо захваченных террористами» — вплоть до их полного уничтожения. В том числе, по решению Президента Российской Федерации военные могут быть привлечены для нанесения ударов по базам террористов за рубежом.

Так, 6 сентября 2021 г. ФСБ России сообщила о задержании четырех сторонников ИГ (террористическая организация, запрещенная на территории России), готовивших нападение на сотрудников полиции в Ингушетии. По данным силовиков, они через Интернет связывались с другими членами организации и планировали теракты с использованием самодельных взрывных устройств и холодного оружия. Из мест проживания задержанных изъяли огнестрельное и холодное оружие, самодельные взрывные и зажигательные устройства, а также компоненты и инструменты для их изготовления. Кроме того, в их средствах связи была обнаружена переписка с членами ИГ, подтверждающая преступные намерения [4].

Терроризм представляет угрозу миру и безопасности, поэтому международное сообщество, осознавая опасность терроризма и стремясь выработать эффективные меры по его предупреждению, приняло ряд документов, к которым относятся конвенции Организации Объединенных Наций (например, Международная конвенция о борьбе с захватом заложников, Международная конвенция о

борьбе с бомбовым терроризмом, Международная конвенция о борьбе с финансированием терроризма), Шанхайская конвенция о борьбе с терроризмом, сепаратизмом и экстремизмом, Конвенция Совета Европы о предупреждении терроризма. В международных документах указывается, что терроризм ни при каких обстоятельствах не может быть оправдан соображениями политического, философского, идеологического, расового, этнического, религиозного или иного характера.

Обратившись к международной практике, можно вспомнить всем известные террористические организации (например, ИГИЛ), члены которых занимались активной пропагандой и вербовкой населения, в частности, молодежи. Для эффективного противодействия терроризму необходимо учесть особенности психологии потенциальных сторонников терроризма, которых могут подвергнуть вербовке. Террористы ищут среди молодежи новый ресурс, который мог бы усилить их деятельность. Например, тех, кто способен совершать террористические акты; тех, у кого есть образование в определенных сферах, как медицина, лингвистика, IT-индустрия (для осуществления кибератак и т. д.); тех, кто сам бы занимался вербовкой и привлекал бы новых членов в террористическую организацию; радикальных религиозных деятелей.

Террористы ищут всевозможные пути, чтобы вступать в дискуссии, отстаивать, навязывать свою идеологию, убеждения в информационной среде. Ознакомившись с социальным портретом преступности по возрастной категории, следует отметить, что более 50 % лиц, совершивших преступление, соответствует категории лиц от 14 до 35 лет [3]. Из этого следует вывод о необходимости совершенствования системы профилактики терроризма среди молодежи.

По нашему мнению, следует разработать эффективные технические средства для противодействия распространению идей терроризма в сети Интернет, укрепить международное сотрудничество и обмен передовым опытом по данному вопросу. Также необходимо пересмотреть нормативно-правовую базу на основе мониторинга зарубежного законодательства.

Список литературы

1. Федеральный закон от 06.03.2006 № 35-ФЗ (ред. от 26.05.2021) «О противодействии терроризму» // СПС «КонсультантПлюс» (дата обращения: 20.03.2022).
2. Официальный сайт Роскомнадзор. URL: <https://rkn.gov.ru/mass-communications/reestr/media/> (дата обращения: 20.04.2022).
3. Официальный сайт Федеральной службы государственной статистики (РОССТАТ). URL: <https://rosstat.gov.ru/folder/10705> (дата обращения: 30.03.2022).
4. ФСБ сообщила о задержании четырех сторонников ИГИЛ в Ингушетии. URL: <https://www.interfax-russia.ru/south-and-north-caucasus/main/fsb-soobshchila-o-zaderzhanii-chetyreh-storonnikov-igil-v-ingushetii> (дата обращения: 20.04.2022).

5. Шевко Н. Р. Актуальные проблемы обеспечения информационной безопасности современного общества / Н. Р. Шевко. Вестник Казанского юридического института МВД России. 2012. № 2 (8). С. 57–59.

Черкесова Д. А. ¹,

курсант факультета подготовки специалистов

в области информационной безопасности

Московского университета МВД России имени В.Я. Кикотя

Научный руководитель:

Клочкова Е. Н.,

доцент кафедры специальных информационных технологий

учебно-научного комплекса информационных технологий

Московского университета МВД России имени В.Я. Кикотя

ИНТЕРНЕТ, КАК ПЛАТФОРМА ДЛЯ ПРОПАГАНДЫ ЭКСТРЕМИЗМА И ТЕРРОРИЗМА

В последние годы в средствах массовой информации все чаще встречаются понятия терроризм, экстремизм. Во многих странах организации, занимающиеся такой деятельностью, классифицируются в зависимости от их склонности к насилию и политическим целям. Экстремистов, склонных достигать свои цели исключительно насильственным путем, принято называть террористами, поэтому смело можно сказать, что «экстремизм» – понятие более обширное и емкое, нежели «терроризм». Проблема борьбы с преступлениями данной направленности является весьма важной и актуальной, поскольку согласно ст. 2 Конституции Российской Федерации – соблюдение прав и свобод человека и гражданина входит в основные задачи, стоящие перед государством.

В соответствии с Федеральным законом от 25.07. 2002 № 144-ФЗ «О противодействии экстремистской деятельности», экстремистская деятельность (экстремизм) – это насильственное изменение основ конституционного строя или нарушение территориальной целостности Российской Федерации, за исключением проведения пограничных работ, демаркации и восстановления границы между Российской Федерацией и сопредельными странами (включая передачу части территории Российской Федерации). Кроме того, экстремизм, как достаточно широкое понятие с множеством определений, означает: публичное оправдание терроризма и иной террористической деятельности; возбуждение социальной, расовой, национальной или религиозной ненависти; пропаганду 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 и многое другое.

Согласно положениям Федерального закона от 06.03.2006 № 35-ФЗ (ред. от 26.05.2021) «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

¹ © Черкесова Д. А., 2022.

насильственных действий. С учетом этого, в соответствии с тем же нормативным актом, террористическая деятельность – деятельность, включающая в себя:

- а) организацию, планирование, подготовку, финансирование и реализацию террористического акта;
- б) подстрекательство к террористическому акту;
- в) организацию незаконного вооруженного формирования, преступного сообщества (преступной организации), организованной группы для реализации террористического акта, а равно участие в такой структуре;
- г) вербовку, вооружение, обучение и использование террористов;
- д) информационное или иное пособничество в планировании, подготовке или реализации террористического акта;
- е) пропаганду идей терроризма, распространение материалов или информации, призывающих к осуществлению террористической деятельности либо обосновывающих или оправдывающих необходимость осуществления такой деятельности.

Экстремистские и террористические акты могут выражаться в различных формах и видах преступного поведения. Согласно Уголовного кодекса Российской Федерации это и организация массовых беспорядков (ч. 1. ст. 212), и организация незаконного вооруженного формирования или участие в нем (ст. 208), и посягательство на жизнь государственного или общественного деятеля (ст. 277), и организация экстремистского сообщества (ст. 282.1), и террористические акты (ст. 205) и многие другие преступные действия и посягательства.

Развитие информационных технологий в последние несколько десятилетий привело к тому, что информационно-телекоммуникационные технологии стали играть достаточно важную роль в жизни человека, а компьютеры стали буквально неотъемлемой частью современного мира. Все это привело к тому, что и пропаганда идеологии экстремизма, терроризма также перешла в сеть Интернет и, преодолев тысячелетия, приспособилась к новым реалиям современного мира. На сегодняшний день в сети уже образовалась всемирная система исламистских ресурсов, доступных на разных языках и преследующих цель подготовки будущих членов террористических организаций.

История перехода пропаганды экстремизма и терроризма в глобальную сеть Интернете началась с создания организациями своих собственных веб-сайтов, но это было только начало, вскоре идеологи начали понимать возможности, которые им предоставляют новые информационные технологии и что нужно работать над расширением аудитории. Следующим этапом стал переход на различные форумы, где пропаганда могла надежно и безопасно распространяться. Такие группировки, как Аль-Каида (АК) и Аль-Шабаб, первыми увидели возможности, которые предоставлялись в набирающих популярность социальных сетях (Twitter, Facebook, ВКонтакте и т. д.), а также в центрах обмена файлами (YouTube).

Следующая трансформация произошла после увеличения давления со стороны правительства, как реакция на все более масштабные атаки, совершаемые членами и сторонниками ИГ. Корпорации социальных сетей и файлообменные

центры начали преследовать экстремистов, осуществляя цензуру аккаунтов с помощью специально разработанных алгоритмов. Все это привело к тому, что, несмотря на значительное сокращение, экосистема экстремистов не исчезла – она просто изменилась. Сообщество снова переменяло дислокацию, на этот раз это стали такие сервисы, как Telegram.

Гибридная платформа социальной сети оказалась идеальной для однорангового общения, групповых обсуждений и распространения пропаганды. К началу 2018 г. появились признаки того, что произойдет еще одна трансформация. Более двух лет на Telegram оказывалось всевозможное давление с целью очистить его от джихадистов. Но в то же время появляются и начинают бурно развиваться множество других зашифрованных и максимально обеспечивающих приватность платформ, таких как, например, Zello, Threema, Wickr и Surespot. И уже они начинают превращаться в онлайн-точки сбора.

Процесс привлечения новых сторонников к радикальным группировкам наиболее успешен через социальные сети. Профессиональные психологи запрещенной в Российской Федерации террористической группировки ИГИЛ для вербовки будущих сторонников используют популярные социальные сети Facebook, Twitter, Вконтакте и Одноклассники. Согласно текущей статистике, 84 % людей, которые участвовали в ИГИЛ, попали туда благодаря социальным сетям.

В настоящее время на территории России уже запретили деятельность американской кампании «Мета», которая владеет социальными сетями «Facebook» и «Instagram». Тверской районный суд признал компанию «Мета» экстремистской организацией, благодаря которой пользователи Facebook и Instagram в некоторых странах могли призывать к насилию против россиян или российских солдат в контексте вторжения на Украину. На данный момент социальная сеть разрешает некоторые сообщения, призывающие к смерти президентов Российской Федерации, Республики Беларусь. То есть компания «Мета» это отличный пример экстремистской организации в Интернете, ведь как еще можно назвать организацию, которая разрешила пользователям публиковать посты с призывами насилия над гражданами Российской Федерации, в частности российскими военными.

Директор Национального центра информационного противодействия терроризму и экстремизму в образовательной среде и сети Интернет С. А. Чурилов, в одном из своих выступлений отметил, что основными причинами использования глобальной сети в качестве инструмента пропаганды экстремистской и террористической деятельности стали: высокая скорость распространения информации через различные интернет-ресурсы, социальные сети, блоги; возможность анонимного ведения противоправной деятельности; а также возможность охвата достаточно широкой аудитории.

Целями такой пропаганды зачастую являются:

- запугивание и дезинформация общества;
- реклама террористической и экстремистской деятельности;
- продвижение террористической и экстремистской идеологии;

– поддержание взаимодействия террористических и экстремистских организаций.

Цели, которые преследуют сами «киберэкстремисты», связаны с вовлечением в свои ряды новых лиц, с созданием сообществ и блогов по обсуждению пограничных тем.

Проведенный нами анализ показывает, что чаще всего в сети Интернет встречаются материалы различных групп и обществ, побуждающие к насильственному изменению конституционного строя, отражающие пропаганду превосходства или неполноценности человечества по признакам отношения их к религиозной, социальной, расовой и другим принадлежностям. В последнее время увеличилось количество публикаций в социальных сетях («ВКонтакте», «Телеграмм»), демонстрирующих нацистскую символику, пропагандирующих идеологию нацизма, а также в связи с последними событиями текущего года осуществляющих антироссийскую пропаганду.

К сожалению, ввиду специфики развития современного общества, полностью устранить и избежать дальнейшее развитие терроризма и экстремизма в Интернете невозможно, однако в России, а точнее в ряде ее регионов, уже появились «Национальные центры информационного противодействия идеологии терроризма и экстремизма в образовательной среде и сети Интернет», где каждый доброволец может оставить сведения об обнаружении противоправного контента и тем самым посодействовать соответствующим органам своевременно отреагировать и пресечь противоправные действия данной направленности.

Список литература

1. Лапунова Ю. А. Распространение идеологии экстремизма и терроризма в киберпространстве: проблемы и пути их решения // Труды Академии управления МВД России. 2017. № 3 (43).
2. Мишин А. М. Проблемы противодействия экстремизму в сети Интернет // Евразийский юридический журнал. 2020. № 2 (141). С. 389–390.
3. Овчинский В. С. Основы борьбы с киберпреступностью и кибертерроризмом: хрестоматия. М., 2017.
4. Павлинова Е. Ю. Проблемы противодействия экстремизму в сети Интернет // Закон и власть. 2019. № 2. С. 50–53.

Чурин Р. А.¹,

*заместитель начальника отдела компьютерных
и радиотехнических экспертиз ЭКЦ МВД России*

Ращупкина В. А.²,

*научный сотрудник отдела научных
исследований по специальным видам экспертиз
и экспертно-криминалистического обеспечения
противодействия наркопреступности управления
научных исследований ЭКЦ МВД России*

СОВРЕМЕННОЕ СОСТОЯНИЕ КОМПЬЮТЕРНОЙ СУДЕБНОЙ ЭКСПЕРТИЗЫ В ЭКСПЕРТНО-КРИМИНАЛИСТИЧЕСКИХ ПОДРАЗДЕЛЕНИЯХ МВД РОССИИ

Значительное увеличение количества криминальных деяний, совершенных с использованием информационно-телекоммуникационных технологий, усиливает недоверие граждан к правоохранительным органам [1]. При этом лица, причастные к совершению таких преступлений, устанавливаются менее чем в каждом пятом случае (в 2019 г. – 44158, в 2021 г. – 86696).

Одновременно с этим возрастает потребность в проведении судебных экспертиз в ИТ-сфере, о чем свидетельствует увеличение зарегистрированных компьютерных экспертных исследований (+ 15,6 %). Их основной массив выполняется ведомственными экспертными подразделениями [2]. Так, например, экспертам системы МВД России в 2021 г. назначено более 27 тыс. компьютерных экспертиз и исследований.

Фактическая численность экспертов МВД России, имеющих право самостоятельного производства компьютерных экспертиз, составляет более 400 человек. За счет увеличения численности личного состава в экспертно-криминалистических подразделениях МВД России (далее также – ЭКП) появилась возможность специализировать сотрудников на определенном круге задач, например, вирусной аналитике, исследовании мобильных телефонов, накопителей данных, работе с поврежденными устройствами памяти и пр. Такое разделение по типу исследуемых объектов и специфике решаемых вопросов позволяет специалисту более глубоко изучать предметную область, концентрироваться на поставленной задаче, что, несомненно, положительно влияет на эффективность проводимых исследований.

Становится востребованным исследование так называемых больших данных – «Bigdata», в ходе которого изучаются и сопоставляются между собой массивы информации из различных источников (операторы сотовой связи, центры управления дорожным движением, органы, регистрирующие сведения о населении и его имуществе, социальные сети, компьютеры, мобильные телефоны и др.). Для анализа больших данных требуются значительные вычислительные мощности,

¹ © Чурин Р. А., 2022.

² © Ращупкина В. А., 2022.

поэтому создание столь масштабных проектов возможно только на общегосударственном уровне.

В ведомственных экспертных учреждениях по-прежнему остается недостаточным уровень обеспеченности аппаратно-программными средствами, необходимыми для производства компьютерных экспертиз и исследований. В текущем году актуализировалась проблема с материально-техническим обеспечением ЭКП, связанная с необходимостью использования импортного оборудования, не имеющего в настоящее время российских аналогов (особенно при исследовании мобильных устройств). На фоне антироссийских санкций это существенно осложняет приобретение современных аппаратных и программных средств, а также модернизацию и обновление имеющихся. Имеются случаи значительного роста цен, в том числе на отечественное программное обеспечение и аппаратные средства.

ЭКЦ МВД России активно проводит апробацию отечественных АПК, по результатам которой замечания и предложения направляют производителям. Развитие отечественных технических средств и программного обеспечения позволит в дальнейшем сократить расходы на их приобретение, минимизировать санкционные риски, а также исключить возможность утечки за рубеж информации, обрабатываемой в процессе исследований.

Также ЭКЦ МВД России на регулярной основе проводит мониторинг предлагаемых российскими разработчиками современных технических средств, которые могут быть использованы при производстве компьютерных экспертиз. Полученные результаты направляются в ЭКП. Проведен ряд опытно-конструкторских работ, направленных на создание инструментария для исследования объектов сферы высоких технологий, инициированы новые опытно-конструкторские работы, по итогам которых планируется создать новое, не имеющее аналогов оборудование для производства судебных компьютерных экспертиз.

Параллельно с изложенным прорабатывается вопрос закупки гражданских АПК для производства компьютерных экспертиз. Это позволит расширить комплектацию комплексов, закупать современные технические и программные решения, а также сэкономить бюджетные средства, затрачиваемые на проведение опытно-конструкторских работ.

Сотрудниками Центра смоделирован перспективный криминалистический комплекс типовой лаборатории для производства компьютерных экспертиз. Новый АПК будет построен на основе технологии аппаратной виртуализации. Такое архитектурное решение в первую очередь позволит повысить эффективность использования вычислительных мощностей ЭКП.

От совершенствования системы кадрового обеспечения в области информационной безопасности напрямую зависит укомплектованность ЭКП квалифицированными специалистами, осуществляющими противодействие преступлениям в сфере IT-технологий. В настоящее время подготовка кадров, специализирующихся на проведении компьютерных экспертиз и исследований, для экспертных

учреждений, помимо гражданских образовательных учреждений, осуществляется в двух ведомственных образовательных организациях МВД России.

ЭКЦ МВД России реализует мероприятия, направленные на увеличение количества обучающихся по программам высшего профессионального образования, повышения квалификации и профессиональной переподготовки для сотрудников подразделений МВД России, решающих задачи в области обеспечения информационной безопасности, а также противодействия преступлениям в сфере компьютерной информации. Регулярно проводятся стажировки и совещания в режиме видео-конференц-связи по актуальным проблемам производства экспертиз. ЭКЦ МВД России на протяжении нескольких лет каждое полугодие проводит рабочие совещания с экспертами экспертно-криминалистических подразделений в режиме видео-конференц-связи.

Экспертно-криминалистическим подразделениям системы МВД России в целях совершенствования своей деятельности перераспределяются штаты в сторону увеличения экспертов по направлению компьютерной экспертизы.

Необходимо отметить, что применяемые государственными экспертными учреждениями методы исследований в основном позволяют решать задачи, поставленные органами предварительного расследования. Имеющиеся в рассматриваемой сфере методики являются общими и дают возможность отвечать на вопросы, выносимые при расследовании преступлений, совершаемых в сфере информационно-телекоммуникационных технологий.

Наиболее длительные исследования при производстве компьютерных экспертиз связаны с диагностикой программного обеспечения. Для совершенствования подходов к производству компьютерных экспертиз (исследований) решается вопрос о создании информационного массива сведений об объектах компьютерной информации (в том числе относящихся к вредоносному), примененных при совершении преступных деяний, обнаруженных и исследованных в ходе производства судебных компьютерных экспертиз. Предлагаемая к хранению и обработке информация будет содержать характеристики файлов, позволяющие однозначно идентифицировать компьютерную информацию, сведения о шифровании, основных сигнатурах, адресах управления и характерной картине следообразования. Указанные данные могут быть использованы экспертами профильного направления при производстве исследований идентичных объектов, что позволит существенно сократить время их выполнения, а также сотрудниками оперативных и следственных подразделений при принятии решений о возбуждении и объединении уголовных дел.

Для повышения уровня автоматизации и качества организационно-управленческой и производственной деятельности ЭКП, в том числе в части оптимизации и перераспределения нагрузки при проведении компьютерных экспертиз, МВД России проводятся мероприятия по развитию сервиса единой автоматизированной информационной системы. В их рамках прорабатывается вопрос равномерного распределения нагрузки на профильных специалистов в целях ее выравнивания и сокращения очередей на производство экспертных исследований по уголовным делам, находящимся в производстве органов внутренних дел.

С учетом значимости экспертного сопровождения раскрытия и расследования преступлений, совершаемых с использованием интернет-технологий, необходимо на регулярной основе совершенствовать материально-техническое обеспечения ЭКП и научно-методическую базу производства компьютерных экспертных исследований, а также укреплять кадровый потенциал, что и является приоритетными направлениями в деятельности ЭКЦ МВД России.

Список литературы

1. Информационное письмо Генеральной прокуратуры и Министерства внутренних дел Российской Федерации от 08 февраля 2022 г. № 36-49-22/1/1322 «О практике рассмотрения сообщений о преступлениях, совершаемых с использованием информационно-коммуникационных технологий, и об иных проблемных вопросах».
2. Указ Президента Российской Федерации от 2 марта 2022 г. № 83, постановление Правительства Российской Федерации от 28 марта 2022 г. № 490, распоряжение Правительства Российской Федерации от 1 апреля 2022 г. № 714-р.

Лукина Е. В.¹,
студентка КФ ФГБОУВО
«Российский государственный университет правосудия»

Аматыч Э. Р.²,
студентка КФ ФГБОУВО
«Российский государственный университет правосудия»

Научный руководитель:
Шевко Н. Р.,
доцент кафедры уголовно-правовых дисциплин
Казанского филиала ФГБОУВО «Российский
государственный университет правосудия»,
кандидат экономических наук, доцент

ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ ПРОПАГАНДЕ ЭКСТРЕМИЗМА И ТЕРРОРИЗМА В СОЦИАЛЬНЫХ СЕТЯХ

Современный мир ежедневно подвергнут существенным изменениям. Обращая свое внимание на прошлые столетия, можно заметить, что тогда все силы были направлены на развитие промышленности, в нынешнее же время господствующее положение занимает информация, поскольку с каждым годом все больше видов деятельности человека осуществляется посредством информационных технологий. На данном этапе интерес всего человечества к сети Интернет растет в геометрической прогрессии. Российская Федерация одна из тех стран, которые активно используют Интернетом [1]. Так, на начало 2022 г. общая доля пользователей данной сети составила 85 % россиян.

Данные показатели свидетельствуют о том, что потребность в информационно-коммуникационной сети велика. Во многом это объясняется тем, что сеть представляет собой площадку, которая обеспечивает свободный доступ к различному роду информации, а также является основой процесса цифровизации в современных реалиях.

Как показывает практика, молодежь в силу своей неустойчивой психики, несформированного мировоззрения чаще других подвергается психологической атаке и более активно участвует в межэтнических конфликтах (до 90 %) [2]. На сегодняшний день, по словам экспертов, в социальных сетях действует более 10000 групп (в среднем около 7 млн подписчиков), вовлекающих подростков и молодежь в противозаконные действия, в том числе экстремистского и террористического характера [3].

Российское законодательство содержит ряд норм по противодействию распространению экстремистской идеологии и террористической деятельности. Со-

¹ © Лукина Е. В., 2022.

² © Аматыч Э. Р., 2022.

гласно ч. 3 ст. 29 Конституции Российской Федерации не допускаются пропаганда или агитация, возбуждающие социальную, расовую, национальную или религиозную ненависть и вражду [4].

26 апреля 2022 г. генпрокурор Игорь Краснов выступил в Совете Федерации с ежегодным докладом, где озвучил, что количество выявленных экстремистских преступлений выросло более чем на четверть в 2021 г., две трети из которых совершены в Интернете. Анализ результатов правоохранительной деятельности показывает, что при этом активно задействовались возможности социальных сетей и мессенджеров, прежде всего, Telegram, WhatsApp, «ВКонтакте», «Одноклассники», Instagram и Facebook. На данный момент последние два запрещены на территории Российской Федерации в связи с тем, что принадлежат корпорации Meta, которая признана в нашей стране экстремистской.

За последний год количество преступлений террористической направленности, совершенных с использованием сети Интернет, выросло на треть (576 преступлений террористической направленности против 428 в прошлом году). Медиасредства и цифровые технологии задействованы террористами, прежде всего, для вовлечения в террористическую деятельность, в том числе путем публичных призывов к ее осуществлению, публичного оправдания и пропаганды терроризма.

Одним из способов противодействия пропаганды экстремизма и терроризма в социальных сетях является блокировка деструктивных течений, признанных опасными для населения.

С каждым годом необходимость противодействия экстремизму и терроризму становится все более актуальной. Необходимо объединение всех стран и континентов для борьбы с этим наиболее опасным видом преступлений. За счет распространения в сети экстремизм и терроризм становятся транснациональными. Без всемерной поддержки со стороны правительств всех стран противодействие просто теряет смысл, становится неэффективным.

Список литературы

1. Шевко Н. Р. Кибербезопасность: состояние и перспективы / Н. Р. Шевко. М. : Всероссийский государственный университет юстиции (РПА Минюста России), 2021. С. 168–170.
2. Рубан Л. С. Дилемма XXI века: толерантность и конфликт. М., 2016.
3. Новое поколение интернет-пользователей: исследование привычек и поведения российской молодежи онлайн [Электронный ресурс]. URL: <https://www.thinkwithgoogle.com/intl/ru-ru/insights-trends/user-insights/novoe-pokolenie-internet-polzovatelei-issledovanieprivychek-i-povedeniia-rossiiskoi-molodezhi-onlain/> (дата обращения: 23.04.2022).
4. Конституция Российской Федерации: принята всенародным голосованием 12 декабря 1993 г. // Собрание законодательства Российской Федерации. 2014. № 31. Ст. 4398.

Рафикова Р. Р.¹,
студентка Казанского филиала ФГБОУВО
«Российский государственный университет правосудия»

Научный руководитель:
Шевко Н. Р.,
доцент кафедры уголовно-правовых дисциплин
Казанского филиала ФГБОУВО
«Российский государственный университет правосудия»,
кандидат экономических наук, доцент

КИБЕРТЕРРОРИЗМ – КОНВЕРГЕНЦИЯ ТЕРРОРИЗМА И КИБЕРПРОСТРАНСТВА

Современное общество характеризуется активным использованием информационных технологий. И, к сожалению, не только во благо. Эксперты в области информационных технологий и политические деятели подробно остановились на возможности проникновения кибертеррористов в правительственные учреждения, частные корпорации или нанесения ущерба технологической части вооруженных сил или службам и финансовым сферам глобального международного пространства. Насколько реальна эта угроза в нашем мире? Тревога, которую вызывает у людей тема «кибертерроризма», вызвана страхом перед возможной случайной и насильственной виктимизацией, что приводит к подозрительности и глубокому страху перед информационными технологиями.

Терроризм – это преднамеренное применение насилия в отношении людей для достижения своей цели. Террористы часто являются жестокими экстремистами, которые страстны и полны решимости достичь своих целей и готовы пожертвовать своей жизнью. Наиболее широко используемым оружием нападения во всем мире являются взрывчатые вещества.

В дополнение к войнам на суше, на море и в воздухе киберпространство стало новым полем битвы. Киберпространство – это безграничная и уникальная среда. Оно состоит из миллионов волоконно-оптических кабелей, соединяющих компьютеры, серверы, маршрутизаторы и шлюзы. Его безопасность является международной проблемой. Уровень сложности, необходимый для атаки на киберпространство, резко снизился.

Кибертерроризм часто определяется как любая преднамеренная, политически мотивированная атака на информационные системы, программы и данные, которая угрожает насилием или приводит к насилию. Определение иногда расширяется, чтобы включить любую кибератаку, которая запугивает или вызывает страх у целевой группы населения. Злоумышленники часто делают это, повреждая или разрушая критически важную инфраструктуру.

Кибертерроризм – это конвергенция терроризма и киберпространства. Это предполагает использование Интернета как средства содействия, так и меха-

¹ © Рафикова Р. Р., 2022.

низма поддержки. У него есть потенциал для создания постмодернистского состояния хаоса. Он использует компьютерные ресурсы для запугивания, нанесения вреда или разрушения критически важных инфраструктур, таких как электросети, транспорт, нефть и газ, банковское дело и финансы, водоснабжение и аварийные службы [5, с. 158].

Кибертерроризм обладает потенциалом создать постмодернистское состояние хаоса, которое может относиться к состоянию крайнего беспорядка и неразберихи. Кибертеррористы могут начать атаку на больницы, уничтожив жизни людей, их миротворцев и средства жизнеобеспечения. Они также могут атаковать военных, разрушая системы связи и нарушая обороноспособность. Чтобы преступление квалифицировалось как кибертерроризм, оно должно происходить в киберпространстве и использовать какую-либо компьютерную сеть для осуществления атаки [3, с. 85].

Террористы могут причинить вред, используя несколько тактик, таких как мошенничество, наводнения электронной почты, вирусы, трояны, черви, спам, фишинг, кража личных данных, шпионские программы и атаки типа «отказ в обслуживании».

Угроза кибертерроризма велика, как никогда. В 2021 г. по всему миру зафиксировано большое количество значительных кибератак.

Термином «кибертерроризм» часто злоупотребляют. Это пугающая проблема, которая вызывает страх: страх перед технологиями и страх перед терроризмом. Кибератаки усиливаются по мере того, как Интернет становится все более привлекательным для злоумышленников [4, с. 27].

Правительственные чиновники и другие специалисты часто утверждают, что мир не готов к кибертерроризму. Но что можно сделать, чтобы остановить это? Превентивные меры должны ограничивать ущерб, причиняемый сетевыми вторжениями. Они должны быть эффективными в блокировании многих форм кибертерроризма [7, с. 99]. Критически важные сети, такие как чувствительные военные системы и компьютерные сети МВД России и ФСБ России, физически не подключены к Интернету, что делает их невосприимчивыми к кибератакам.

С ростом его использования киберпреступность бросает вызов правоохранительным органам.

Хотя преступления неизбежны в современном мире, их можно свести к минимуму с помощью законов, нормативных актов, правоохранительных органов, международного сотрудничества и т. д. [6]. Однако законов, защищающих пользователей от кибератак, не существует. Поскольку нападения могут произойти в любой день с кем угодно, пользователи должны иметь базовую подготовку, чтобы защитить себя. Осведомленность – это, пожалуй, лучшая защита [1, с. 17]. Готовность должна начинаться на местном уровне, поскольку местные агенты, такие как полиция и военные базы, первыми прибывают на место нападения и реагируют на терроризм.

Должна существовать государственная образовательная программа, позволяющая людям быть осведомленными о киберугрозах. Программы повышения

осведомленности о безопасности служат эффективными мерами противодействия кибертерроризму.

Ключом к противодействию кибертерроризму является осуществление широких мер кибербезопасности и бдительность.

Кибертерроризм в основном нацелен на государственные структуры. Однако ситуация меняется, и предприятия также становятся мишенями. В результате предприятия и другие организации должны убедиться, что все устройства Интернета вещей защищены и недоступны через общедоступные сети. Для защиты от программ-вымогателей и подобных типов атак организации должны регулярно создавать резервные копии систем, внедрять методы непрерывного мониторинга и использовать брандмауэры, антивирусное программное обеспечение и средства защиты от вредоносных программ [2, с. 245].

Министерство по безопасности координирует свои действия с другими учреждениями государственного и частного сектора. В нем содержится информация о потенциальной террористической деятельности и о том, как защитить безопасность страны, а также о мерах по борьбе с терроризмом.

Кибертерроризм является серьезной проблемой. Однако кибертеррористов можно в какой-то степени сдержать. Мероприятия по сдерживанию могут снизить вероятность преступных проявлений. Есть основания для беспокойства, но не для паники. Борьба с кибертерроризмом – это непрерывная борьба.

Список литературы

1. Архипов Ю. А. Визуализация метрик защищенности для мониторинга безопасности и управления инцидентами. Солнечногорск: ТЕЛДА, 2018.
2. Барнс К. и др. Защита от хакеров беспроводных сетей. Пер. с англ. А. В. Семенова. М. : АйТи, ДМК пресс, 2019.
3. Батурин Ю. М., Жодзишский А. М. Компьютерная преступность и компьютерная безопасность. М. : Юридическая литература, 2021.
4. Кузнецов С. В. Конкурентная разведка через Интернет. Введение. Методические указания по результатам бизнес-тренингов. М. : 2020.
5. Мак-Клар Стюарт, Шах Саумил, Шах Шрирай. Хакинг в Web: атаки и защита. М. : Вильямс, 2018.
6. Шевко Н. Р. Актуальные проблемы обеспечения информационной безопасности современного общества / Н. Р. Шевко. Вестник Казанского юридического института МВД России. 2012. № 2 (8). С. 57–59.
7. Эриксон Джон. Хакинг: Искусство эксплойта. 2-е издание. СПб. : Питер, 2018.

*Андреянова Ю. М.¹,
студент Казанского филиала ФГБОУВО
«Российский государственный университет правосудия»*

*Научный руководитель:
Шевко Н. Р.,
доцент кафедры уголовно-правовых дисциплин
Казанского филиала ФГБОУВО «Российский
государственный университет правосудия»,
кандидат экономических наук, доцент*

ОСОБЕННОСТИ ПРОТИВОДЕЙСТВИЯ КИБЕРТЕРРОРИЗМУ В СОВРЕМЕННЫХ УСЛОВИЯХ

В современном мире информационные технологии достигли пика своего развития. Человек практически полностью перенес свою жизнь в виртуальное пространство. От перехода общества в мир новых технологий количество преступлений не только не снизилось, но и стремительно растет. К нарушениям закона в материальном мире добавились и преступления в информационном пространстве. К одним из самых опасных в этом роде относится кибертерроризм. Ученые и политики определяют его, как наиболее опасную форму терроризма.

В современном обществе наблюдается нарастающая активность международного терроризма, интегрированного в интернет-пространство. Кибертерроризм как особо опасный вид терроризма становится высокотехнологичным. За счет киберпространства он стирает все границы между странами и континентами, привлекая к себе внимание за мгновения миллиардов людей, позволяя злоумышленникам достичь поставленных целей за считанные доли секунды. Радикально настроенные граждане все чаще используют современные информационные технологии, компьютерные криптопрограммы по шифрованию, гаджеты, мобильные средства связи и пр.

На сегодняшний день в уголовном законодательстве нет четкого определения термину кибертерроризм. Как правило преступления в данной сфере классифицируют по ст. 205 Уголовного кодекса Российской Федерации «Террористический акт» [1]. Также не существует единого толкования термину «киберпреступление». Чаще всего под ним понимают преступления, совершаемые в интернет-пространстве или с помощью высоких технологий. То есть кибертерроризм – это особая совокупность деяний, совершаемых в информационном пространстве, которые несут в свою очередь террористический характер. Кибертерроризм преследует цель нанести информационный и телекоммуникационный вред государству, обществу или отдельному человеку с помощью информационной среды.

История развития кибертерроризма берет свое начало с момента информатизации общества и повсеместного распространения Интернета. В качестве ин-

¹ © Андреянова Ю. М., 2022.

струментов совершения терроризма в интернет-пространстве используются различные компьютерные программы. Можно привести примеры из наиболее известных, это:

- компьютерный код, который используется для угрозы или с целью нанесения физического или психологического вреда для структурных систем или людей;
- компьютерные вирусы, которые используются для несанкционированного удаленного доступа к различной информации, а также вывода из строя компьютерных систем и сетей;
- компьютерные вычислительные станции, предназначенные для совершения кибер-атак на различные информационные сервисы и ресурсы с их последующим выводом из строя [2].

В современном мире кибертерроризм занимает одну из лидирующих позиций в списке глобальных проблем. Решением вопроса по снижению угрозы кибертерроризма занимается все мировое сообщество. Каждая отдельная страна озабочена этой проблемой и ищет способы ее предотвращения и предупреждения.

Главной задачей кибертеррористов является угроза с помощью киберпространства. Посредством угрозы они добиваются определенных решений в социальной, экономической и политической сферах. Самое главное, что под действия кибертеррористов может попасть кто угодно, как обычный человек, так и целое государство.

На сегодняшний день отдельные государства по одиночке не в силах противостоять кибертерроризму, поэтому странам необходимо объединять свои усилия для борьбы в этой сфере. Ведущая роль в координации достижения целей противоборству кибертерроризма возлагается на международные организации – ООН и, прежде всего, ее главные органы – Совет Безопасности и Генеральная Ассамблея.

У кибертерроризма есть определенные особенности, которые отличают его от других форм терроризма. С одной стороны, он обладает всеми признаками терроризма, а с другой – киберпреступления, вбирая в себя все преимущества использования информационных технологий. Во-первых, кибертерроризм – информационное оружие, в основе своей опирающееся на современные информационные технологии. Во-вторых, как и любое киберпреступление он носит трансграничный характер (преступники обычно находятся в одной стране, а их жертвы – на другом конце земного шара). Следовательно, с наименьшими затратами кибертерроризм достигает своих преступных целей, нанося максимальный ущерб, охватывая огромные массы пользователей сети, оставляя минимум следов и улик.

В связи с этим можно выделить и особенности кибертеррористических актов. Прежде всего, это зависимость от информационно-телекоммуникационных технологий, удаленный доступ к любой точке земного шара за считанные секунды, привлечение огромного количества интернет-пользователей, доступность большинства информационных ресурсов и данных, трансграничность, анонимность, высокая скорость.

В целях противодействия распространению терроризма и экстремизма в виртуальном пространстве были приняты законодательные акты, в том числе и международные (например, Конвенция ООН «О киберпреступности»), по борьбе с ними. В соответствии с Конвенцией помимо создания правовых условий международного сотрудничества и противодействия киберпреступности интернет-провайдеры еще должны осуществлять сбор, обработку, анализ и запись или перехват необходимой информации с помощью доступных технических средств и помогать в этом правоохранительным органам.

Таким образом, на современном этапе развития общества применение чисто технических средств защиты не представляется надежным противодействием киберпреступлениям. Необходим комплексный подход как к вопросу обеспечения информационной безопасности на всех уровнях (законодательном, организационном, техническом, методологическом и др.), так и к вопросу международного сотрудничества по данной проблеме.

Список литературы

1. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 25.03.2022) // Собрание законодательства Российской Федерации. 1996. № 25. ст. 2954.
2. Антонян Е. А. Блокчейн-технологии в противодействии кибертерроризму: монография. М., 2019.

Шаруха И. А.¹,

соискатель факультета подготовки

научно-педагогических и научных кадров

по кафедре криминологии

Московского университета МВД России имени В.Я. Кикотя

ПРАКТИКА ПРИМЕНЕНИЯ ЗАКОНОДАТЕЛЬСТВА ОБ ОТВЕТСТВЕННОСТИ ЗА ПРЕСТУПЛЕНИЯ, ПОСЯГАЮЩИЕ НА СВОБОДУ СОВЕСТИ И ВЕРОИСПОВЕДАНИЯ

Уголовно-правовая охрана общественных отношений, обеспечивающих беспрепятственную реализацию каждым человеком и гражданином своего конституционного права на свободу совести и вероисповедания, в настоящее время осуществляется с помощью ряда статей Уголовного кодекса Российской Федерации (далее – УК РФ), среди которых, на наш взгляд, в первую очередь следует выделить те, что предусматривают ответственность за публичные действия, совершаемые в целях оскорбления религиозных чувств верующих, а равно действия, направленные на воспрепятствование функционированию религиозных организаций, осуществлению богослужений или иных религиозных обрядов и церемоний (ст. 148 УК РФ), создание некоммерческой организации, посягающей на личность и права граждан, и участие в деятельности такой организации (ст. 239 УК РФ), организацию деятельности экстремистской организации, вовлечение в деятельность такой организации либо участие в ее деятельности (ст. 282² УК РФ).

Среди указанных уголовно-правовых норм наиболее применяемой на практике является ст. 282² УК РФ, при этом в последние пять лет наблюдается положительная динамика числа осужденных за предусмотренные в ней преступления. Так, в 2017 г. по ст. 282² УК РФ по основной и дополнительной квалификации было осуждено 11 лиц, в 2018 г. – 41 лицо, в 2019 г. – 67 лиц, в 2020 г. – 100 лиц и в 2021 г. – 138 лиц [1]. Закономерным является то, что наибольшее число таких лиц было осуждено по ч. 2 ст. 282² УК РФ – за участие в деятельности экстремистской организации (например, в 2021 г. виновными в совершении этого деяния были признаны 93 лица – 67,39 % от всех лиц, осужденных по данной уголовно-правовой норме в целом).

На формирование практики применения ст. 282² УК РФ большое влияние оказывают разъяснения Пленума Верховного Суда Российской Федерации, содержащиеся в его постановлении от 28 июня 2011 г. № 11 (ред. от 28.10.2022) «О судебной практике по уголовным делам о преступлениях экстремистской направленности» [2]. В свою очередь, складывающаяся правоприменительная практика выявляет актуальные проблемы реализации ответственности по ст. 282² УК РФ, для разрешения которых требуются новые разъяснения Пленума Верховного Суда Российской Федерации [3].

Обнаружению данных проблем и привлечению к ним внимания Верховного Суда Российской Федерации способствуют не только нижестоящие суды, но и

¹ © Шаруха И. А., 2022.

органы прокуратуры, сотрудники различных правоохранительных органов, ученые и представители общественности. В частности, по результатам заседания Совета при Президенте Российской Федерации по развитию гражданского общества и правам человека, проходившего 10 декабря 2020 г., был утвержден Перечень поручений Президента Российской Федерации, в подп. «а» п. 8 которого Верховному Суду Российской Федерации было рекомендовано подготовить разъяснения по итогам обобщения судебной практики по делам, связанным с нарушениями законодательства о свободе совести, свободе вероисповедания и религиозных объединениях [4]. Итогом выполнения этого поручения стало принятие в конце октября 2021 г. постановления Пленума Верховного Суда Российской Федерации, содержащего, в частности, разъяснения, касающиеся выявленных проблемных вопросов применения ст. 282² УК РФ.

Наиболее важными из них, по нашему мнению, являются позиции Пленума, согласно которым, во-первых, по уголовным делам об участии в экстремистской организации необходимо установить, в каких конкретных общественно опасных действиях выразилось такое участие, каково их значение для возобновления или продолжения деятельности соответствующей запрещенной организации, а также исключить случаи привлечения к уголовной ответственности за действия, состоящие исключительно в реализации лицом своего конституционного права на свободу совести и вероисповедания (например, проведение богослужений или иных религиозных обрядов, церемоний); во-вторых, действия организационного характера, наказуемые по ч. 1 ст. 282² УК РФ, охватывают случаи вовлечения других лиц в деятельность соответствующей запрещенной организации [6].

Отметим, что указанные разъяснения Пленума Верховного Суда Российской Федерации основаны на результатах обобщения уже сложившейся судебной практики и направлены на ее закрепление для обеспечения единообразных подходов к юридической оценке противоправных действий, связанных с функционированием экстремистских организаций.

Так, по одному из уголовных дел об организации деятельности экстремистской организации (ч. 1 ст. 282² УК РФ) было установлено, что у П., являвшейся «специальным пионером» религиозной организации «Управленческий центр Свидетелей Иеговы в России» и осведомленной о вступившем в законную силу решении суда о ликвидации и запрете деятельности этой организации, в связи с неоднократным распространением и хранением в целях массового распространения литературы, признанной экстремистскими материалами, возник преступный умысел на возобновление и продолжение деятельности местной религиозной организации Свидетелей Иеговы, а также на участие в ней. Для реализации этого умысла П., в частности, совершила действия по вовлечению других лиц в состав участников (членов, последователей) указанной запрещенной организации. В этих целях П. прошла обучение в различных филиалах указанной религиозной организации, изучила специальную литературу, в результате чего овладела психологическими приемами воздействия на других людей для их вовлечения в деятельность экстремистской организации. О результатах своей преступной де-

тельности П. ежемесячно готовила отчеты, включавшие сведения об «обработанной» ею территории с указанием количества жителей, национального состава и других особенностей, о проводимых на регулярной основе собраниях в ее квартире, о количестве жителей, посещающих такие собрания. При этом П., осознавая незаконность своих действий, принимала меры конспирации, в том числе инструктировала лиц, присутствовавших на закрытых «религиозных» собраниях, о необходимости сохранения такой деятельности в тайне [7].

Из этого примера видно, что суд еще до внесения указанных выше изменений в постановление Пленума Верховного Суда Российской Федерации от 28 июня 2011 г. № 11 пришел к выводу о включении вербовки новых участников экстремистской организации в содержание объективной стороны состава преступления, предусмотренного ч. 1 ст. 282² УК РФ. Кроме того, по этому уголовному делу принято еще одно важное решение в части квалификации содеянного: суд расценил действия подсудимой, сочетавшие в себе признаки организации деятельности экстремистской организации и участия в ее деятельности, в качестве одного преступления, наказуемого по ч. 1 ст. 282² УК РФ. Между тем в указанном постановлении Пленума Верховного Суда Российской Федерации соответствующее правило квалификации до настоящего времени не закреплено, что, на наш взгляд, является пробелом в формировании единообразной практики применения статей 282¹ и 282² УК РФ. В данном случае следует обратить внимание на разъяснение, содержащееся в абз. 4 п. 22⁷ постановления Пленума Верховного Суда Российской Федерации от 9 февраля 2012 г. № 1 (в ред. от 03.11.2016) «О некоторых вопросах судебной практики по уголовным делам о преступлениях террористической направленности» [8], согласно которому действия лица, не только организовавшего деятельность террористической организации, но и участвовавшего в данной деятельности, охватываются ч. 1 ст. 205⁵ УК РФ и не требуют дополнительной квалификации по ч. 2 этой уголовно-правовой нормы [9]. Полагаем, что аналогичное разъяснение необходимо закрепить и для целей квалификации сочетания таких же общественно опасных действий по ст.ст. 205⁴, 282¹ и 282² УК РФ.

Относительно ст. 148 УК РФ отметим, что на практике применяются только первые ее две части, предусматривающие ответственность за публичные действия, выражающие явное неуважение к обществу, совершенные в целях оскорбления религиозных чувств верующих, тогда как чч. 3, 4 данной уголовно-правовой нормы об ответственности за незаконное воспрепятствование деятельности религиозных организаций, проведению богослужений или иных религиозных обрядов и церемоний фактически не действуют. Так, за период с 2017 по 2021 гг. включительно по чч. 1, 2 ст. 148 УК РФ по основной и дополнительной квалификации было осуждено 39 лиц, при этом более 41 % таких лиц признаны виновными в оскорблении чувств верующих в течение 2021 г. При этом преобладают факты совершения соответствующих действий с использованием сети Интернет, где виновные размещают фото-, видео- и иные материалы, форма и содержание которых способны оскорбить религиозные чувства верующих (например, в слу-

чае размещения фотографий с изображением неприличных действий на фоне религиозных святынь, храмов). То есть публичность такие действия нередко приобретают не во время их непосредственного осуществления вблизи зданий и иных объектов, имеющих значение для верующих, а только в момент размещения соответствующих файлов на личной странице в социальной сети либо на сайте в сети Интернет. Данная особенность характерна и для ряда других уголовно наказуемых деяний, совершаемых с использованием информационно-коммуникационных технологий, в том числе для преступлений экстремистской направленности [10].

Например, несовершеннолетний М. был осужден по ч. 2 ст. 148 УК РФ за публичные действия, выражающие явное неуважение к обществу, совершенные в целях оскорбления религиозных чувств верующих, в местах, специально предназначенных для проведения богослужений, других религиозных обрядов и церемоний. По делу установлено, что М., находясь в помещении кафедрального собора имени Казанской Божией Матери, пренебрежительно относясь к христианским святыням, символам и ценностям, обесценивая христианские каноны и нормы поведения, осознавая противоправность своих действий, предвидя неизбежность наступления общественно опасных последствий в виде оскорбления чувств православных верующих, прикурил сигарету от зажженной свечи, установленной на подставке для свечей, а также курил сигарету в помещении собора, то есть в месте, специально предназначенном для проведения богослужений, религиозных обрядов и церемоний. Продолжая свои преступные действия, М. разместил в своем аккаунте в социальной сети видеозапись указанных противоправных действий с голосовым комментарием, содержащим нецензурную лексику. При этом согласно показаниям семи свидетелей, находившихся в храме во время указанных действий, очевидцем совершения последних никто из них не являлся, большинство свидетелей о правонарушении узнали от органов следствия или из средств массовой информации, после чего они просмотрели видеозапись, которую оценили как оскорбляющую чувства верующих [11].

Изучение практики применения чч. 1, 2 ст. 148 УК РФ показало, что основные трудности связаны с толкованием признаков состава преступления и его отграничением от смежных преступлений и сходных административных правонарушений. В частности, возникают вопросы относительно того, что понимать под выражением явного неуважения к обществу, когда соответствующие действия направлены только против одной социальной группы – верующих; как отличить такие действия от оскорбления, умышленного публичного осквернения религиозной или богослужебной литературы, предметов религиозного почитания, знаков или эмблем мировоззренческой символики и атрибутики либо их порчи или уничтожения, унижения человеческого достоинства по признаку отношения к религии и мелкого хулиганства, являющихся административными правонарушениями, а равно от уголовно наказуемого хулиганства, одним из криминообразующих признаков которого выступает указанное выражение явного неуважения к обществу наряду с мотивом религиозной ненависти либо вражды. Представляется, что на эти и другие вопросы должен ответить Пленум Верховного Суда

Российской Федерации, разъяснения которого относительно практики применения ст. 148 УК РФ в настоящее время отсутствуют.

По нашему мнению, также востребованными на практике являются и разъяснения Пленума Верховного Суда Российской Федерации по вопросам применения ст. 239 УК РФ. Данная уголовно-правовая норма содержит три самостоятельных состава преступления, при этом первые два из них связаны с созданием религиозных или общественных объединений, различных некоммерческих организаций, включая те, что исполняют функции иностранного агента, их структурных подразделений, деятельность которых сопряжена с насилием над гражданами, причинением вреда их здоровью или побуждением к отказу выполнять свои гражданские обязанности. Третий состав преступления предусмотрен ч. 3 ст. 239 УК РФ и заключается в участии в деятельности некоммерческой организации, указанной в чч. 1, 2 данной статьи. Статья 239 УК РФ редко применяется на практике: за указанный выше пятилетний период по ней было осуждено всего 25 лиц, при этом большинство из них (свыше 50 %) – по ч. 3 этой статьи. При этом действия организаторов и (или) иных участников соответствующих некоммерческих организаций, сопряженных с противоправной деятельностью, нередко дополнительно квалифицируются по статьям главы 16 УК РФ о преступлениях против жизни и здоровья человека.

Например, К. был осужден по ч. 1 ст. 239 и п. «б» ч. 2 ст. 111 УК РФ. По делу установлено, что К. создал религиозное объединение «Возрождение XXI век г. Омск», деятельность которого была сопряжена с насилием над гражданами, руководил этим объединением, а также умышленно причинил тяжкий вред здоровью двух и более лиц, повлекший их психическое расстройство. Более трех лет К. еженедельно проводил воскресные богослужения, в ходе которых применял психологическое насилие к гражданам, помимо их воли используя технологии психологического воздействия, в том числе гипнотические техники, вводил участников богослужения в состояние измененного сознания (транса), внушал им необходимость посещать богослужения и совершать пожертвования, желая таким образом достигнуть имевшуюся у него цель – получать доход от пожертвований граждан. В результате систематического применения К. технологий психологического воздействия у шести потерпевших развилось психическое расстройство (синдром психической зависимости), что было квалифицировано как умышленное причинение тяжкого вреда здоровью [12].

Деятельность таких псевдорелигиозных, религиозных или общественных объединений, а равно иных некоммерческих организаций связана с вовлечением в их орбиту большого числа граждан, которые подвергаются насилию, обману, а равно иному противоправному воздействию, при этом они нередко утрачивают все свое имущество либо его значительную часть, а их психическому и физическому здоровью наносится ощутимый урон. В связи с этим при применении ст. 239 УК РФ на практике возникает необходимость разрешения ряда сложных вопросов квалификации содеянного, в том числе касающихся правильного определения видов преступлений, образующих их совокупность, и ограничения от

смежных составов преступлений и сходных административных правонарушений.

Таким образом, изучение практики реализации уголовной ответственности за деяния, предусмотренные ст.ст. 148, 239 и 282² УК РФ, показало, что ряд вопросов нуждается в разъяснениях Пленума Верховного Суда Российской Федерации, при подготовке которых важно учитывать общие принципы уголовной ответственности, а также необходимость научно обоснованного решения проблем, связанных с толкованием соответствующих законоположений и их последующим применением.

Список литературы

1. Здесь и далее приводятся статистические данные Судебного департамента при Верховном Суде Российской Федерации: URL: <http://www.cdep.ru/index.php?id=79> (дата обращения: 27.04.2022).
2. Сайт Верховного Суда Российской Федерации: URL: <http://www.vsrf.ru/> (дата обращения: 27.04.2022).
3. Иванцов С. В., Борисов С. В. Организованные формы экстремистской и террористической деятельности: регламентация и реализация ответственности // Общество и право. 2016. № 2. С. 91–97.
4. Перечень поручений Президента Российской Федерации от 28 января 2021 года № Пр-133 по итогам заседания Совета при Президенте Российской Федерации по развитию гражданского общества и правам человека, проходившего 10 декабря 2020 г. (подпункт «а» пункта 8) // Сайт Президента Российской Федерации: URL: <http://www.kremlin.ru/acts/assignments/orders/64952> (дата обращения: 27.04.2022).
5. Постановление Пленума Верховного Суда Российской Федерации от 28 октября 2021 г. № 32 «О внесении изменений в некоторые постановления Пленума Верховного Суда Российской Федерации по уголовным делам» // Российская газета. 2021. 12 ноября.
6. Пейсикова Е. В., Борисов С. В. Новые позиции Пленума Верховного Суда Российской Федерации об освобождении от наказания и уголовной ответственности // Уголовный процесс. 2022. № 2. С. 68–74.
7. Приговор Горномарийского районного суда Республики Марий Эл от 31.05.2021 по делу № 1-1-5/2021 // СПС «КонсультантПлюс».
8. Сайт Верховного Суда Российской Федерации: URL: <http://www.vsrf.ru/> (дата обращения: 27.04.2022).
9. Иванцов С. В., Узембаева Г. И. Противодействие преступлениям экстремистской направленности, совершаемым с использованием средств массовой информации либо информационно-телекоммуникационных сетей: уголовно-правовые и криминологические аспекты: монография / под ред. С. В. Иванцова. М., Юрлитинформ, 2018. С. 4
10. Иванцов С.В., Узембаева Г.И., Музычук Т.Л., Тищенко Ю.Ю. Актуальные проблемы совершенствования системы мер криминологического предупре-

ждения преступлений экстремистской направленности, совершаемых с использованием информационно-телекоммуникационных сетей // Всероссийский криминологический журнал. 2018. Т. 12. № 16. С. 776–784.

11. Приговор мирового судьи судебного участка № 54 Центрального судебного района суда г. Читы от 3 марта 2021 г. // Архив Забайкальского краевого суда за 2021 год.

12. Приговор Куйбышевского районного суда г. Омска от 24 декабря 2018 г. // Архив Омского областного суда за 2018 год.

Гринберг С. А.¹,

адъюнкт факультета подготовки

научно-педагогических и научных кадров по кафедре криминологии

Московского университета МВД России имени В.Я. Кикотя

КРИМИНОЛОГИЧЕСКИ ЗНАЧИМЫЕ ОСОБЕННОСТИ ПРЕВЕНТИВНОГО ВОЗДЕЙСТВИЯ НА ОРГАНИЗОВАННЫЕ ФОРМЫ ПРОФЕССИОНАЛЬНОЙ ПРЕСТУПНОСТИ

Деятельность по противодействию преступности должна осуществляться на основе объективной криминологической информации об объекте превентивного воздействия, как о состоянии преступности, так и о превентивном потенциале субъектов данной деятельности. Для эффективной реализации мер по выявлению, устранению, нейтрализации факторов детерминации преступности либо минимизации их воздействия, а также по недопущению совершения преступлений на разных стадиях преступного поведения необходимо, прежде всего, учитывать криминологически значимые характеристики конкретного вида преступной деятельности, выступающего в качестве объекта превентивного воздействия.

Противодействие организованным формам профессиональной преступности в условиях современного мегаполиса должно осуществляться с учетом криминологической сущности данного вида преступности. Особенности превентивного воздействия в отношении данного вида преступной деятельности обусловлены рядом субъективных и объективных факторов.

Прежде всего, следует учитывать то, что превентивное воздействие направлено на организованную преступную деятельность, т. е. деятельность субъектов, организовавших для совместной преступной деятельности в форме организованных групп, а также преступных сообществ (преступных организаций). Соответственно, превентивное воздействие должно осуществляться на основе всего выработанного наукой и практикой арсенала методов и средств противодействия организованной преступности [1].

При осуществлении превентивного воздействия в отношении организованных форм профессиональной преступности в условиях современного мегаполиса следует учитывать наличие у лиц, осуществляющих преступную деятельность (в первую очередь у преступников-профессионалов, как ключевого, системообразующего элемента указанных форм организованной преступной деятельности), криминального опыта, что определяет как общественную опасность преступников и уровень их профессионализма, так и криминальную специализацию и направленность преступной деятельности.

Существенное криминологическое значение имеет наличие криминального опыта лиц, осуществляющих преступную деятельность, поскольку данный критерий определяет, как общественную опасность преступников и уровень их про-

¹ © Гринберг С. А., 2022.

фессионализма, так и криминальную специализацию, и направленность преступной деятельности. В то же время, установление факта уголовно-правового рецидива имеет существенное оперативно-разыскное значение, поскольку позволяет установить характеристику личности преступника и его предыдущей преступной деятельности, выявить криминальные связи и пр. [2, с. 62–66].

Также следует учитывать и такой субъективный фактор, как профессиональная основа преступной деятельности, т. е. обладание организованными субъектами преступной деятельности соответствующей криминальной специализацией и криминальной квалификацией.

При осуществлении превентивного воздействия в отношении организованных форм профессиональной преступности в условиях современного мегаполиса следует учитывать потенциально неоднородный профессиональный состав их участников.

Соответственно, превентивное воздействие следует дифференцировать относительно профессиональной преступной деятельности организованных групп и преступных сообществ:

- 1) состоящих из преступников-профессионалов;
- 2) состоящих из преступников-профессионалов и иных лиц, выполняющих различного рода «вспомогательные» функции и обеспечение преступной деятельности организованной группы (преступного сообщества);
- 3) состоящих из членов организованной группы (преступного сообщества) и привлеченных преступников-профессионалов (как правило, имеет место в случае привлечения представителями организованной преступности различных преступников, так называемых «суперпрофессионалов», как для выполнения узкоспециализированных функций по обеспечению деятельности преступного сообщества, так и для совершения конкретных, сложных с точки зрения способа совершения преступлений).

Превентивное воздействие также требует дифференциации в зависимости криминальной специализации организованных форм профессиональной преступной деятельности. Так, организованные группы и преступные сообщества могут специализироваться на:

- 1) обороте оружия;
- 2) обороте наркотиков;
- 3) организации проституции;
- 4) торговле людьми и рабском труде;
- 5) миграции;
- 6) обороте предметов искусства и антиквариата;
- 7) угоне и торговле автомобилями;
- 8) мошенничестве;
- 9) хищениях (карманные кражи, кражи из жилища и пр.);
- 10) трансплантации органов и тканей человека;
- 11) заказных убийствах;
- 12) фальшивомонетничестве;

13) незаконных операциях с недвижимостью (рейдерство, «черные риелторы» и пр.);

14) криминальном использовании информационных технологий и пр.

Не только криминальная специализация, но и избираемые способы достижения криминальных целей, среди которых наибольшую общественную опасность представляет насилие [3, с. 157–168], определяют характер и степень общественной опасности организованных форм преступной деятельности. Поэтому методы и средства превентивного воздействия должны дифференцироваться в зависимости от насильственной либо ненасильственной направленности организованных форм профессиональной преступной деятельности.

В соответствии с уровнем криминальной квалификации особое внимание в качестве объекта превентивной деятельности требует преступная активность таких участников организованных форм преступной деятельности, как преступники-суперпрофессионалы. Если профессиональная преступность, аккумулируя в себе криминальный опыт, выступает «венцом» и одновременно источником криминальной эволюции [4, с. 181–186], то преступники-суперпрофессионалы являются вершиной эволюции преступного профессионализма. Именно их преступная деятельность представляет наибольшую общественную опасность, поскольку, как личность преступника-суперпрофессионала представляет собой один из наиболее опасных типов личности преступника, так организованные формы преступной деятельности преступников-суперпрофессионалов представляют собой наиболее опасный вид организованной преступности.

В качестве объективных факторов, определяющих особенности превентивного воздействия в отношении организованных форм профессиональной преступности в условиях современного мегаполиса, следует учитывать именно факторы, связанные с обстановкой и условиями современного мегаполиса, выступающего специфической социально-правовой реальностью.

Многие, объективно присущие современному мегаполису характеристики определяют условия и обстановку, выступающие криминогенным фактором организованных форм профессиональной преступной деятельности.

Современный мегаполис, как один из наиболее сложных и высокоразвитых видов людских поселений, является центром социальной, финансовой, политической активности и культурной жизни региона или всей страны, центром концентрации больших масс населения, что сопряжено с колоссальными разноплановыми (по видам и уровням) миграционными нагрузками, центром концентрации значительных интеллектуальных и экономических ресурсов, разнопрофильным рынком труда (включающим нелегальные и полуполигальные сектора трудоустройства), обладает развитой социальной и транспортной инфраструктурой и рядом иных специфических характеристик.

Противодействие преступности в условиях современного мегаполиса определяет необходимость учета криминологических параметров его географических и функционально-топографических характеристик [6, с. 145–146]. Именно топографические особенности и неоднородность городского пространства, специфика его планирования и проектирования, социально-функциональный контекст

городского пространства, а также географическое и геополитическое положение современного мегаполиса на территории страны во многом определяют специфику криминогенной обстановки на данной территории.

Социально-территориальные и производственно-территориальные комплексы и их компоненты, а также транспортная инфраструктура современного мегаполиса требуют особого внимания, как с точки зрения выявления их криминогенности, так и с точки зрения обеспечения их безопасности.

Социально-демографические характеристики и специфика организация социальной жизни современного мегаполиса обуславливают наличие специфических социально-психологически факторов, выступающих детерминантами организованных форм профессиональной преступной деятельности. К данным факторам, в частности, следует отнести: поликомпонентный состав населения, высокую мобильность населения, повышенный ритм жизни и повышенные психологические нагрузки, стрессогенность и конфликтогенность, повышенную частоту межгрупповых, межличностных контактов, анонимность социальных контактов и поведения, социальную отчужденность, закрытость и психоэмоциональную индифферентность окружающих и пр.

Таким образом, организованность и профессиональный характер преступной деятельности, а также указанные особенности современного мегаполиса определяют криминологически значимые особенности, которые должны учитываться при реализации превентивного воздействия в отношении организованных форм профессиональной преступности в условиях современного мегаполиса.

Список литературы

1. Иванцов С. В. Обеспечение органами внутренних дел системного подхода в изучении и предупреждении организованной преступности: монография / С. В. Иванцов; под ред. С. Я. Лебедев. Москва: ЮНИТИ-ДАНА, 2017.
2. Иванцов С. В. Особенности предупреждения рецидивной и профессиональной преступности органами внутренних дел // Российский криминологический взгляд. 2011. № 4 (28). С. 62–66.
3. Игнатов А. Н. Стратегия противодействия криминальному насилию в современном обществе // Библиотека криминалиста. Научный журнал. 2015. № 6 (23). С. 157–168.
4. Иванцов С. В. Криминальный профессионализм в системе российской организованной преступности и вопросы его предупреждения органами внутренних дел // Человек: преступление и наказание. 2008. № 3 (62). С. 181–186.
5. Игнатов А. Н., Пахомов С. В. Влияние качественно-пространственных особенностей местности на выбор и реализацию способа совершения преступления // Общество и право. 2016. № 3 (57). С. 143–147.