



ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ КАЗЕННОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ УНИВЕРСИТЕТ МИНИСТЕРСТВА ВНУТРЕННИХ ДЕЛ
РОССИЙСКОЙ ФЕДЕРАЦИИ ИМЕНИ В.Я. КИКОТЯ»

ПРОТИВОДЕЙСТВИЕ ТЕРРОРИЗМУ И ЭКСТРЕМИЗМУ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

**Сборник научных статей Всероссийской конференции
17 декабря 2020 г.**

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

Научное электронное издание

Москва
2020

© Московский университет МВД России
имени В.Я. Кикотя, 2020
ISBN 978-5-9694-0920-0

Рецензенты:

Начальник кафедры информационно-компьютерных технологий в деятельности органов внутренних дел Белгородского юридического института МВД России имени И.Д. Путилина кандидат технических наук, доцент **А. Н. Прокопенко**;
врио начальника УВД по Северо-восточному административному округу ГУ МВД России по г. Москве полковник полиции **А. Ю. Андрющенко**

Противодействие терроризму и экстремизму в информационных системах : сборник научных статей Всероссийской конференции – М. : Московский университет МВД России имени В.Я. Кикотя, 2020. – 253 с. – 1 электронный оптический диск (CD-R). – Системные требования: CUP 1,5 ГЦ ; RAM 512 Мб ; Windows XP SP3 ; 1 Гб свободного места на жестком диске.

ISBN 978-5-9694-0920-0

В сборнике публикуются статьи авторов – участников Всероссийской конференции «Противодействие экстремизму и терроризму в информационных системах», прошедшей в Московском университете МВД России имени В.Я. Кикотя 17 декабря 2020 года.

В статьях авторов рассматриваются основные аспекты распространения экстремизма и терроризма 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.

Статьи публикуются в авторской редакции. Сборник предназначен для научных и практических работников, участвующих в борьбе с преступностью.

Научное электронное издание

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

Номер государственной регистрации обязательного федерального экземпляра
электронного издания – 0000000000

© Московский университет МВД России
имени В.Я. Кикотя, 2020

Издание подготовлено
с помощью программного обеспечения Microsoft Word

Редактор *Калинин М. А.*
Корректор *Калинин М. А.*
Компьютерная верстка *Калинин М. А.*

Подписано к изданию дд.мм.2020
Объем издания: 5,14 Мб
1 электронный оптический диск (CD-R)



Московский университет МВД России имени В.Я. Кикотя
117437, г. Москва, ул. Академика Волгина, д. 12
<http://www.mosu.mvd.ru>, e-mail: support_mosu@mvd.ru

СОДЕРЖАНИЕ

<i>И. Ю. Сундиев, А. А. Смирнов</i>	
Экстремистский контент в сети «Интернет» и его влияние на радикализацию молодежи	8
<i>Н. А. Дош</i>	
Глобальные тренды в сфере киберпреступности	14
<i>А. А. Смирнов</i>	
Троллинг как метод контрпропаганды в области борьбы с терроризмом и экстремизмом	23
<i>Ю. В. Берладир</i>	
К вопросу о понятии и причинах одиночного терроризма	28
<i>А. В. Манойло</i>	
Информационные войны и психологические операции: игры, в которые играют специальные службы и профессора политологии.....	34
<i>А. С. Попович</i>	
Технология преступления. Криптовалюта – предмет, искусство или способ?	43
<i>В. А. Минаев, В. Ю. Федорович</i>	
Моделирование информационного противоборства в социальных медиа: от теории к практике	54
<i>А. А. Рыженко</i>	
Модель вложенной пирамиды системы управления безопасностью информационного пространства госкорпорации	65
<i>А. С. Овчинский, А. Ю. Андрющенко</i>	
Информационные сферы как поля сражений	70
<i>И. В. Лягушкин</i>	
Сакрально-географическая карта России как поле информационного противоборства	76
<i>Н. Р. Шевко</i>	
Интернет-технологии против терроризма	80
<i>В. В. Гончар, И. С. Акиншин</i>	
Особенности расследования киберпреступлений террористической и экстремистской направленности	83
<i>К. К. Борзунов, П. Д. Лопатин</i>	
Киберразведка в выявлении террористических и экстремистских угроз	89
<i>В. Н. Цимбал</i>	
Особенности противодействия идеологии экстремизма в средствах массовой информации	95
<i>Е. Н. Клочкова</i>	
Кибертерроризм как одна из форм проявления современного терроризма	100
<i>А. А. Гущина, М. Ю. Пакляченко</i>	
К вопросу терроризации медиа-контента	103

В. И. Лустин

**Отдельные аспекты противодействия терроризму
в информационном пространстве.....** 106

И. А. Архипова, А. В. Шаров

**Вопросы взаимодействия при проведении контртеррористических
операций.....** 109

П. В. Коратаев, М. Ю. Пакляченко

**Стандартизация понятий и основных положений по вопросам работы
с компьютерными атаками как с формами проявления терроризма
в информационных системах.....** 113

Д. Е. Некрасов

**Духовно-нравственный компонент в личности расово-этнического
экстремиста и воздействие на него ресурсов
информационно-телекоммуникационной сети «Интернет».....** 118

А. Н. Гулевский

О ненасильственных методах борьбы с терроризмом..... 123

М. Г. Левандовская

**Вовлечение в террористическую деятельность с использованием
социальных сетей** 128

О. И. Федосеева

**Пропаганда традиционных духовно-нравственных ценностей
как основа противодействия информационному воздействию** 135

Д. Х. Носова , В. И. Давлетов

**Направление противодействия проявлениям терроризма и экстремизма
в сети «Интернет».....** 139

Е. С. Шалюгина

Информационный терроризм – манипуляция сознанием большинства... 145

В. Р. Гурьянова

Стратегия антитеррористической деятельности в условиях пандемии... 149

А. В. Еськов , В. М. Кальницкая

**Профилактика экстремизма и терроризма в молодежной среде
как актуальная проблема в информационно-коммуникационном
пространстве.....** 151

А. В. Еськов, В. А. Сергеева

**Правовое обеспечение деятельности органов внутренних дел
в сфере противодействия проявлениям экстремизма
в информационных системах.....** 155

А. А. Агеенков

**Особенности проведения оперативно-разыскных мероприятий
в информационно-коммуникационной среде в период действия
правового режима контртеррористической операции** 158

И. И. Желнов, А. Ю. Голубев, Н. Г. Агнистов

**Классификация спецслужб, контролирующих Интернет
(на примере США).....** 162

И. И. Желнов, В. А. Харьков

Анализ используемых зарубежными странами технических средств контроля Интернета (на примере США)..... 166

Е. А. Охонько

Применение массовых информационных технологий экстремистскими организациями..... 170

А. Г. Карпова, В. В. Гончар

Особенности расследования преступлений, совершаемых с использованием криптовалюты..... 173

А. В. Луханина, В. В. Гончар

Противодействие использованию криптовалюты в экстремистской и террористической деятельности..... 177

И. О. Трушина, Е. Н. Ярмонова

К вопросу об определении понятия персональных данных, используемых в профилактической деятельности сотрудников органов внутренних дел... 181

Л. Э. Абдуразакова, В. В. Гончар

Совершенствование противодействия террористическим и экстремистским киберпреступлениям..... 186

Д. Р. Ахмедов, В. В. Гончар

Особенности правового воздействия на террористические проявления в сфере информационных технологий..... 190

А. Р. Баргаринов, И. В. Тишутина

О некоторых вопросах организации расследования транснациональных преступлений экстремистского характера в Республике Казахстан..... 194

К. В. Алдушина, Т. А. Прудникова

Борьба с экстремизмом и терроризмом в Российской Федерации и пути ее совершенствования..... 200

А. А. Дуваа, А. С. Овчинский

Использование больших данных в выявлении террористических угроз ... 204

А. А. Осипова, В. Н. Цимбал

Использование технологии Big Data в деятельности органов внутренних дел..... 210

Е. М. Плохих, А. С. Овчинский

Направления информационно-аналитического противодействия терроризму..... 215

М. С. Курбатова, Е. Н. Клочкова

Кибертерроризм как угроза современному информационному обществу ... 220

С. Н. Попова, В. Н. Цимбал

Применение систем биометрической идентификации в противодействии терроризму..... 223

Н. К. Рудакова, Е. Н. Клочкова

Вопросы противодействия распространению экстремистской деятельности в сети «Интернет»..... 229

Т. Э. Тараканова, К. К. Борзунов

Алгоритмы моделирования террористической активности..... 233

И. С. Жданов, А. С. Овчинский

Инициативная аналитика в предупреждении преступлений, связанных с террористическими угрозами 236

Н. А. Анфиногенова, И. Д. Котов, О. В. Пименова

Технология распознавания лица: перспектива применения в деятельности правоохранительных органов..... 241

А. Л. Суворов, Е. Н. Клочкова

Установление личности пользователя мессенджера Telegram как инструмент борьбы с экстремистской деятельностью 246

К. М. Шарова, Е. Н. Клочкова

Основные направления противодействия кибертерроризму как разновидности международного терроризма 250

Сундиев И. Ю.¹,

главный научный сотрудник НИЦ № 2

ВНИИ МВД России,

доктор философских наук, профессор;

Смирнов А. А.²,

ответственный секретарь научно-консультативного совета

при Антитеррористическом центре Государств-участников СНГ,

кандидат юридических наук

ЭКСТРЕМИСТСКИЙ КОНТЕНТ В СЕТИ «ИНТЕРНЕТ» И ЕГО ВЛИЯНИЕ НА РАДИКАЛИЗАЦИЮ МОЛОДЕЖИ

Интенсивное развитие информационно-телекоммуникационных технологий, наряду с позитивными изменениями в жизни общества, создает новые вызовы, содержит в себе риски деструктивного влияния на детей и молодежь. По данным ООН, более миллиона детей и подростков в мире ежегодно подвергаются различным формам противоправных посягательств, в том числе совершаемых с использованием информационно-телекоммуникационных технологий.

В условиях пандемической и постпандемической реальности социальные сети и новые масс-медиа приобретают особую значимость для всех групп населения как основные источники жизненно важной информации. При этом уровень доверия к этим источникам у молодежи максимален [1].

Об угрозе радикализации детей и молодежи через информационно-телекоммуникационную сеть Интернет (далее – Интернет) заявил Генеральный секретарь ООН А. Гутерреш. Он отметил, что в условиях пандемии ситуация значительно ухудшилась: свыше 1,5 млрд. детей в мире из-за распространения нового коронавируса не ходят в школу и много времени проводят в Интернете, что увеличивает риск их радикализации и вербовки экстремистскими группировками. «Мы уже видим, что [экстремистские] группы пользуются карантинными мерами и активизируют усилия по пропаганде через социальные сети и привлечению на свою сторону молодых людей, которые все больше времени проводят дома и сидят в Интернете»[2], – подчеркнул Генеральный секретарь ООН. Тем самым, информационная война в условиях пандемии не только не стихает, но и приобретает новые, более изощренные формы.

Информационные каналы в сети «Интернет» благодаря техническим возможностям наращивают скорость подачи и объемы информации. У потребителей информации отсутствует возможность сформировать свою версию происходящих событий: человек начинает жить в рамках навязанных ему интерпретаций.

Деструктивное информационное влияние на интернет-аудиторию оказывает распространение «токсичного» контента. Под «токсичным» контентом мы понимаем различные виды негативной информации, оказывающей деструктивное психологическое воздействие на личность, социальные группы и общество в целом.

¹ © Сундиев И. Ю., 2020.

² © Смирнов А. А., 2020.

Термин «токсичный» изначально имеет значение «ядовитый» и определяется как способность некоторых химических или биологических веществ нарушать нормальные физиологические функции организма человека, животных или растений, вызывая его отравление (интоксикацию), а при тяжелых поражениях – гибель[3].

Однако в последнее время данный термин стал использоваться в иных предметных контекстах. Стало принято говорить о токсичных отношениях, людях, культурах. В 2018 г. Оксфордский словарь выбрал его словом года[4].

Используя данный термин в своей статье, мы исходим из возможности контента оказывать отравляющее воздействие на индивидуальное и групповое сознание и бессознательное.

В научной литературе и правовых актах выделяют множество видов негативного контента. Например, В. Н. Лопатыным в качестве «вредной» информации идентифицированы: информация, возбуждающая социальную, расовую, национальную или религиозную ненависть и вражду; призывы к войне; пропаганда ненависти, вражды и превосходства; порнография; посягательство на честь, доброе имя и деловую репутацию людей; реклама (недобросовестная, недостоверная, неэтичная, заведомо ложная, скрытая); информация, оказывающая деструктивное воздействие на психику людей.

В аналитическом докладе «Фильтрация контента в Интернете. Анализ мировой практики» 2013 г. назывались следующие категории интернет-контента, которые подвергаются фильтрации в разных странах мира [5]:

- 1) политический контент (сайты оппозиционных и правозащитных движений, религиозных движений и сект, информация об этнических меньшинствах);
- 2) социально опасная информация (порнография, ЛГБТ-пропаганда, разжигание национальной и религиозной розни, призывы к насилию);
- 3) контент, связанный с национальной безопасностью (сайты террористических и экстремистских организаций, ресурсы военных противников, ресурсы с конфиденциальными данными и др.);
- 4) сайты и сервисы, нарушающие экономические интересы (файлообменные сайты и торрент-трекеры);
- 5) специализированные интернет-инструменты и социальные сервисы (поисковые сервисы, социальные сети, онлайн-переводчики).

В методологическом плане решение задачи определения видов контента, который идентифицируется как токсичный (негативный, вредный, опасный), и составление его общего перечня может осуществляться несколькими способами. Основным из них является аналитический метод, предполагающий вычленение и указание видов негативного контента, закрепленных в международных договорах и национальном законодательстве. Для этого используется сравнительно-правовой метод исследования.

Вместе с тем существует и другой возможный подход, который можно обозначить как *сущностный метод*. Он предполагает выделение и обоснование критериев вредоносности контента, на основе применения которых динамически выявляется и корректируется перечень деструктивной информации. В определенном смысле его можно сравнить с проактивным принципом работы антиви-

русских программ, отличающимся от традиционного сигнатурного тем, что вирус обнаруживается не путем сравнения его с эталонным перечнем, а посредством описания и детекции признаков вредоносности. В рамках сущностного метода требуется установить и доказать деструктивность того или иного контента на основе определенной процедуры.

Одним из наиболее опасных видов токсичного контента в Сети выступает *экстремистский контент* – информация, возбуждающая социальную, расовую, национальную или религиозную ненависть и вражду и стимулирующая насилие.

Потребление экстремистского контента может побудить человека к вступлению в радикальные сообщества или способствовать его саморадикализации. В обоих случаях результатом может быть совершение террористического акта или нападения по мотивам ненависти или вражды к определенным группам.

Специалистами неоднократно отмечалось, что Интернет выступает подходящей средой для формирования различных групп девиантной направленности. Я. Костюковский так описывает данный процесс: *«Человек, который интересовался чем-то и имел вполне девиантное увлечение, но никогда особо не задумывался над этим, вдруг встречает не только информацию, точно совпадающую с его интересами, но получает теоретические и практические сведения, точный диагноз и название этих интересов, возможность общаться с коллегами, и наконец, встречаться с ними не только в виртуальном мире»*.

Описанный механизм четко прослеживается на примере экстремистских виртуальных сообществ. Д. Гартенстайн-Росс подчеркивает, что «в Интернете, независимо от того, во что вы верите, и как далеко заходите в своих убеждениях, легко найти тех, кто разделяет ваши взгляды. Интернет позволяет стать частью сообщества единомышленников, даже если объединяющие идеи являются экстремистскими – будь то радикальный исламизм, белый национализм, неонацизм или радикализм сторонников освобождения животных. Люди, высказывающие в сети радикальные взгляды, могут найти тех, кто задается аналогичными вопросами, придерживается таких же крайних представлений о мире или же стремится обратить в свою веру новых сторонников» [6].

В составе террористических и экстремистских организаций действуют опытные вербовщики, которые могут самостоятельно отыскивать потенциальных кандидатов и проводить вербовочные мероприятия. «Классической» можно считать схему вовлечения, состоящую из двух этапов.

На *первом этапе* общения в социальных сетях потенциальные объекты для вовлечения в экстремистские и террористические организации подвергаются убеждающей коммуникации и навязыванию им (отдельным реципиентам и группам) специфической системы ценностей через контент общения. Общий контекст такого воздействия выстраивается на продвижении стереотипов, предубеждений и предрассудков, разделяющих людей на «своих» и «чужих». Под воздействием такого рода коммуникации реципиенты постепенно меняют свои установки и поведение. Под воздействием массовой пропаганды они становятся последователями продвигаемого деструктивным сообществом идей и начинают действовать в соответствии с нормами и моделями поведения, принятыми в данных деструктивных сообществах.

На *последующем этапе* происходит селекция: реципиенты, проявившие высокую восприимчивость к предлагаемым идеям и ценностям и обладающие необходимыми способностями, вовлекаются в данные сообщества и становятся его членами. Их сознание подвергается насильственному изменению, запускается механизм контроля сознания членов лидерами этих подгрупп. Деструктивные сообщества через современные информационно-коммуникационные технологии воздействуют на сознание молодых людей, трансформируют их мировоззрение и установки, изменяют их личность, превращая их в орудие для реализации различных деструктивных целей и задач сообщества. Реципиенты с выраженной психопатологией, психологически неустойчивые, с низким уровнем социально-нравственного развития становятся объектами бесструктурного и бесконтактного воздействия и подготавливаются *для акций насыщающего террора*.

Что касается процесса саморадикализации, то он предполагает самостоятельный поиск и потребление контента террористической и экстремистской направленности, в результате чего лицо усваивает экстремистскую идеологию и психологически готовится к совершению теракта или насильственного преступления.

Основным каналом саморадикализации в современном мире выступают интернет-ресурсы – интернет-сайты, видеохостинги, социальные сети и мессенджеры. Содержащийся в них контент можно условно разбить на две большие группы – пропагандистские и новостные материалы, подготовленные основными медиацентрами террористических организаций, и продукция индивидуальной сетевой активности сторонников экстремизма. Во втором случае идет речь о текстовых и голосовых сообщениях, которые распространяют участники многочисленных радикальных чатов и форумов, функционирующих на базе мессенджеров (Telegram, WhatsApp, Skype) и имиджбордов (4chan, 8chan, Gab).

Очевидно, что заходящий на тематические ресурсы или подписывающийся на соответствующий канал индивид делает это не случайно, а уже имея определенный первичный интерес, который может быть детерминирован разными причинами (любопытство, состояние депрессии или озлобленности, решение проблем статуса в молодежной группе). В дальнейшем, потребляя экстремистский контент и активно обсуждая радикальные идеи в виртуальных форумах, индивид может радикализироваться и начать подготовку террористического акта. Параметры протекания данного процесса будут во многом зависеть от его индивидуальных психологических особенностей.

Отдельным направлением радикализации выступает вовлечение широких масс в противоправные публичные акции. Социальные сети и мессенджеры стали основным каналом мобилизации массовых протестных мероприятий. В качестве последнего примера можно привести Республику Беларусь, в которой основным информационным каналом для стимулирования радикализации стал телеграм-канал Nexhta, имеющий «зеркала» (дубли) на других платформах.

По мере совершенствования технологий коммуникации возникают новые способы организации протестной деятельности. Например, весной 2020 г. в нашей стране были проведены «виртуальные митинги» с использованием «Яндекс-навигатора»[7]. Митинги, в которых люди участвовали, не выходя из дома, прокатились по стране в последние дни апреля. Первыми подобную ак-

цию провели жители Ростова-на-Дону. Визуальное пространство карты перед зданием администрации региона заполнилось метками-комментариями с помощью сервисов «Яндекс.Карты» и «Яндекс.Навигатор» и их элемента для текстовых комментариев – сервиса «Разговорчики». Акция начиналась как флэшмоб граждан, недовольных плохой организацией выдачи пропусков в «режиме повышенной готовности», а затем перешла в «виртуальный» митинг с политическими и экономическими требованиями.

Таким образом, можно констатировать, что формы политической активности (митинги, демонстрации, пикеты и т. д.) успешно переходят в онлайн-формы в цифровой среде и при дальнейшем развитии технических и сценарно-структурных элементов могут стать не менее значимыми, чем «классические».

Мировой опыт противодействия токсичному контенту в Интернете показывает, что оно включает в ряд направлений:

- 1) мониторинг интернет-пространства в целях выявления токсичного контента;
- 2) уголовное или административное преследование либо привлечение к гражданской ответственности лиц и организаций, создающих и распространяющих негативных контент;
- 3) удаление или ограничение доступа к токсичному контенту в Сети;
- 4) информационно-просветительская и контрпропагандистская работа в Сети.

Широко используемый способ блокировки запрещенных материалов имеет ограниченную эффективность, поскольку зачастую способствует перемещению противоправного контента на другую веб-платформу или уходу в теневой Интернет (DarkNet). Тем не менее этот метод работает, особенно если к данному процессу активно подключается администрация самих социальных сетей и мессенджеров. Например, в мессенджере Telegram создан канал ISIS Watch, который в ежедневном режиме публикует данные о блокировке каналов распространения террористического контента и используемых для этих целей ботов.

Решение указанных проблем предопределяет необходимость комплексного подхода, включающего в себя как использование адекватных инновационных технических средств выявления, мониторинга и пресечения асоциального контента, так и широкого внедрения в онлайн-среду специально подготовленных сил реагирования (киберполицейских не только с техническим, но и психологическим, педагогическим, историческим, иным гуманитарным образованием). С учетом того, что в настоящее время киберпреступность становится ядром современной преступности, представляется необходимым экстенсивное наращивание полицейского присутствия в Интернет- и онлайн-среде с одновременной интенсификацией антиэкстремистской деятельности при дополнительной гуманитарной поддержке (социальный онлайн-мониторинг) подростков и молодежи, склонных к радикальным проявлениям.

Эффективно противодействовать негативному контенту, способствующему вовлечению молодежи в деструктивную деятельность посредством масс-медиа и сети Интернет, необходимо комплексно, в первую очередь, с помощью организационно-правовых, информационных и оперативно-разыскных мер. Приоритетное внимание необходимо уделять контрпропагандистской работе, направленной на нейтрализацию экстремистской и иной деструктивной деятельности[8].

Библиографический список

1. Марков А. Информационная безопасность в условиях пандемии COVID-19 // Российский совет по международным делам. 9 апреля 2020 г. URL : https://russiancouncil.ru/analytics-and-comments/analytics/informatsionnaya-bezopasnost-v-usloviyakh-pandemii-covid-19/?sphrase_id=35369216 (дата обращения : 05.05.2020).
2. Гуттериш объявил об угрозе радикализации через Интернет более 1,5 млрд. детей // ТАСС. Информационное агентство [электронный ресурс]. (27 апреля 2020 г.) URL : <https://tass.ru/obschestvo/8347533> (дата обращения : 10.06.2020)
3. Уткин Ю. Н. Токсичный // Большая российская энциклопедия [электронный ресурс]. URL : <https://bigenc.ru/chemistry/text/4195484> (дата обращения : 12.10.2020).
4. Оксфордский словарь выбрал слово года – «токсичный» // Медуза [электронный ресурс]. URL : <https://meduza.io/feature/2018/11/15/oksfordskiy-slovar-vybral-slovo-goda-toksichnyy-eto-ne-tolko-pro-yady-est-toksichnaya-maskulinnost-i-toksichnye-otnosheniya> (дата обращения : 12.10.2020).
5. Филтрация контента в Интернете. Анализ мировой практики : аналитический доклад [электронный ресурс] // Фонд развития гражданского общества. URL : http://civilfund.ru/Filtraciya_Kontenta_V_Internete_Analiz_Mirovoy_Praktiki.pdf
6. Радикализация и насилие в интернете // Российский совет по международным делам. 14 июня 2013 г. URL : https://russiancouncil.ru/analytics-and-comments/interview/radikalizatsiya-i-nasilie-v-internete/?sphrase_id=37561508 (дата обращения : 10.06.2020).
7. В городах России прошли виртуальные митинги против режима самоизоляции // Медуза [электронный ресурс]. URL : <https://meduza.io/feature/2020/04/20/v-gorodah-rossii-proshli-virtualnye-mitingi-protiv-rezhima-samoizolyatsii-protestuyushchie-ispolzovali-servisy-yandeksa> (дата обращения : 29.05.2020).
8. Смирнов А. А. Организация контрпропаганды в области борьбы с терроризмом и экстремизмом : науч.-практ. пособие / под ред. А. П. Новикова. М. : АТЦ СНГ, 2020.

*Дош Н. А.¹,
директор по рискам Ассоциации участников Мастеркард*

ГЛОБАЛЬНЫЕ ТРЕНДЫ В СФЕРЕ КИБЕРПРЕСТУПНОСТИ

Злоумышленники постоянно 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 распространения новой коронавирусной инфекции в мире преступники разработали и используют множество новых либо хорошо забытых старых схем, направленных на получение выгоды от их совершения.

Такой вид атак на устройства самообслуживания как «скимминг» (копирование данных на магнитной полосе банковской карты) для Российской Федерации по объективным причинам стремится к нулю, но в других странах этот метод активно используется криминальными группами для кражи денежных средств. В последнее время интерес для мошенников представляют не только банкоматы, но и другие устройства самообслуживания, где используются банковские карты. «Скимминговые» устройства были выявлены в автомате по продаже железнодорожных билетов и на автоматической заправочной станции (рис. 1).



Рис. 1. Атаки на банкоматы / скимминг

¹ © Дош Н.А., 2020

Еще один негативный зарубежный тренд, 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 неполный 2020 год на территории этой страны зафиксировано более 400 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 (рис. 2).



Рис. 2. Атаки на банкоматы/Подрыв

Несмотря на большое количество подрывов банкоматов в Европе и попытки правительств некоторых стран повлиять на текущую ситуацию с целью снижения количества инцидентов, производитель детских игрушек и конструкторов LEGO отказался снимать с производства так называемый «стартовый набор» конструктора со всеми необходимыми комплектующими, где в игровой форме моделируется взлом и подрыв банкомата (рис. 3).

Атаки на банкоматы от ЛЕГО.... « the starter set »



Рис. 3. Набор LEGO Starter Set (иллюстрации с упаковки)

Пандемия, без сомнения, стала очень хорошим поводом для криминальных групп, которые за очень короткий срок переработали все свои мошеннические схемы под сложившиеся обстоятельства. Пользуясь в первые месяцы пандемии паникой, связанной с нехваткой профилактических средств, мошенники создавали фиктивные предложения по реализации масок, антисептиков, тестов и после получения предоплаты за товар исчезали. Жертвами таких схем становились не только простые граждане, но и как показано на слайде выше, государственные компании. В марте 2020 года немецкая компания получила около 15 млн. евро из федерального бюджета на закупку средств индивидуальной защиты для работников социальной сферы. Заплатив за необходимый товар около 2 млн. евро двум якобы фирмам-поставщикам, находящимся в разных странах, позже представители компании выяснили, что мошенники, используя реальные реквизиты существующих компаний, вели от их имени переписку и указывали свои банковские реквизиты для перевода денежных средств.



Рис. 4. Схема мошенничества по отношению к физическим лицам во время пандемии COVID-19

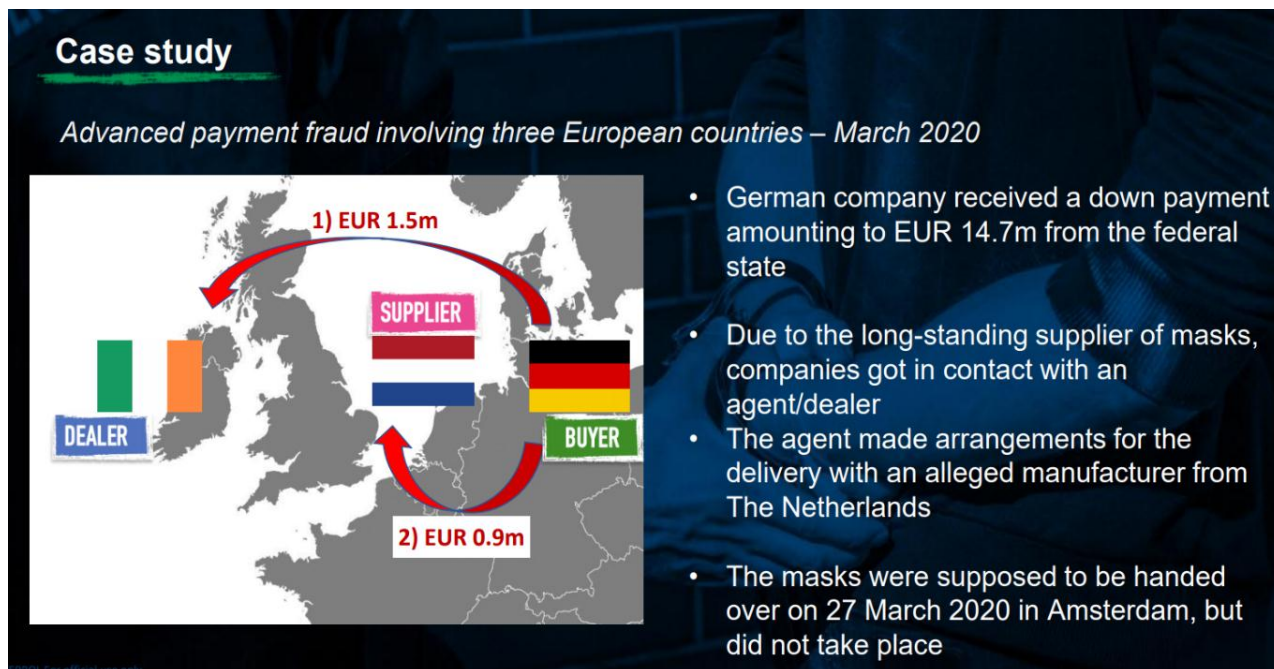


Рис. 5. Схема мошенничества по отношению к компаниям во время пандемии COVID-19

Мошенники организовали огромное количество фальшивых интернет-ресурсов, связанных с пожертвованиями для пострадавших от пандемии (пример схемы данного вида мошенничества дан на рис. 6). Среди подобных стоит выделить пример мошеннического обращения от имени ВОЗ (рис. 7).



Рис. 6. Пример мошеннической схемы пожертвований для пострадавших от пандемии COVID-19



Рис. 7. Пример мошеннического обращения от имени Всемирной организации здравоохранения

Пользуясь ситуацией, мошенники организовывали звонки жертвам якобы от имени департаментов здравоохранения или лечащих врачей с целью получения персональной информации (рис. 8) и рассылали по электронной почте и мессенджерам ссылки на якобы особую информацию про COVID19, ведущую на вредоносное ПО (рис. 9).

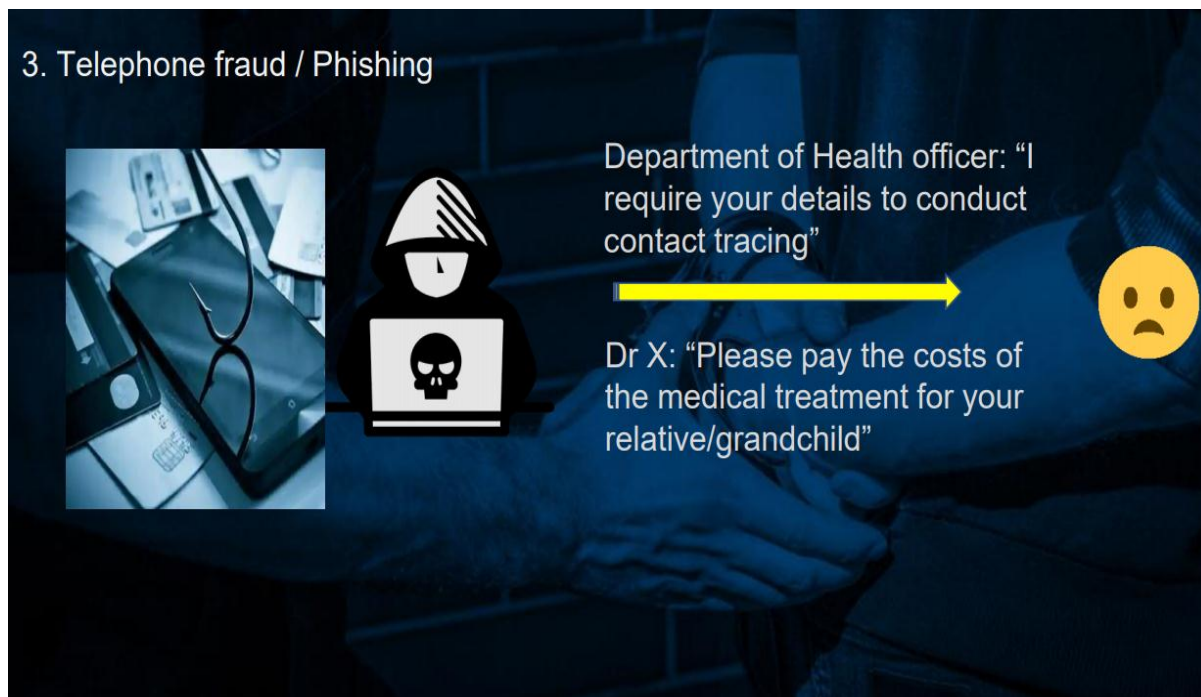


Рис 8. Схема звонка мошенника от имени врача



Рис. 9. Информационный слайд о телефонном и интернет-мошенничестве в период пандемии COVID-19

Получая доступ к информации о зараженных вирусом родственниках, мошенники предлагали членам семьи купить якобы готовую вакцину (рис. 10).

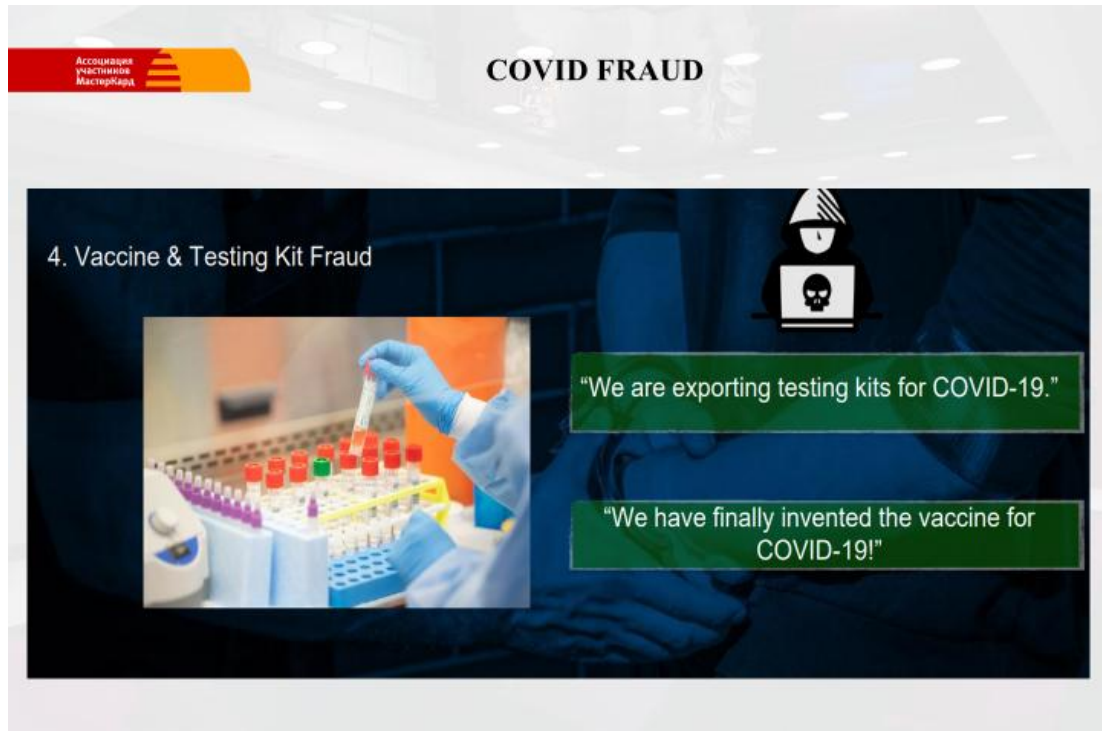


Рис. 10. Схема мошенничества с предложением вакцины от COVID-19

Взламывая рабочие электронные ящики компаний, криминальные элементы получили возможность отправлять электронные письма от имени руководителей своим подчиненным с измененными вводными, объясняя изменения пандемией. Один из примеров – «Из-за пандемии мы вынуждены отправить денежные средства на другой счет прямо сейчас» (рис. 11).

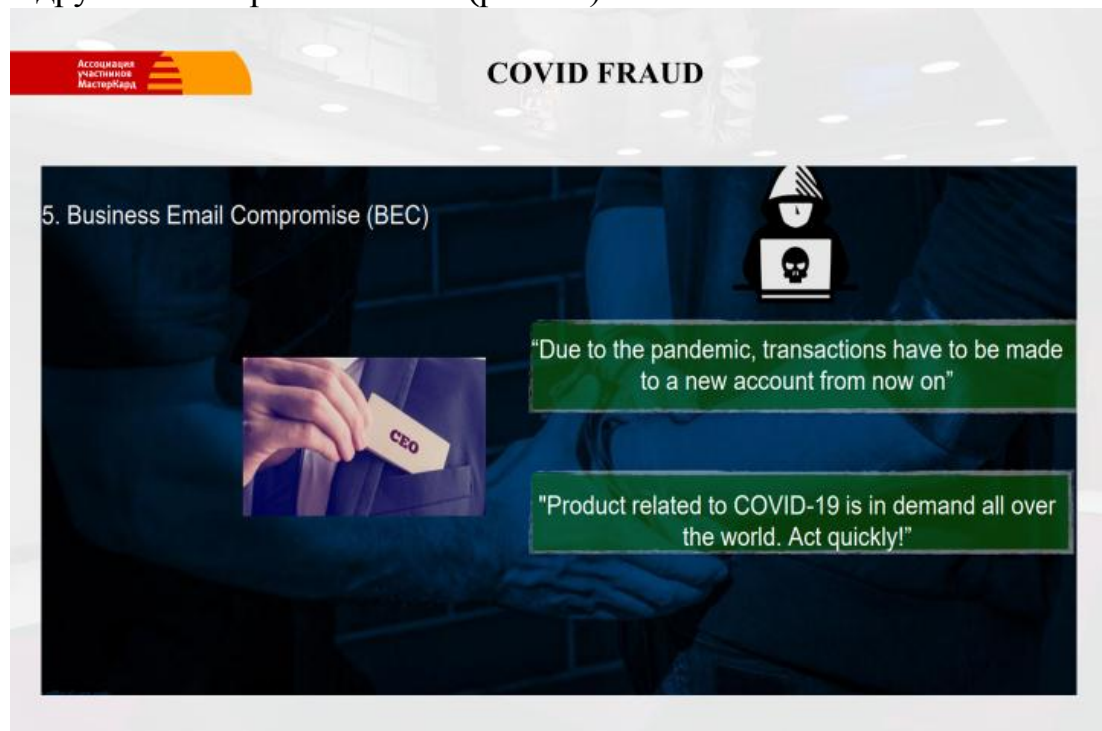


Рис. 11. Схема мошенничества от имени руководителей жертвы

Удаленные рабочие места в период пандемии стали для некоторых организаций практически единственной возможностью сохранить работоспособность и эффективность. К сожалению, безопасность такого рода рабочих мест зачастую отсутствовала, что стало одной из причин взлома криминальными кибергруппами корпоративных сетей и использованием техники, связанной с вымогательством огромных сумм у представителей компании. Преступники при этом скачивают огромный массив данных организации, после чего шифруют все устройства (сервера, рабочие станции). Такая атака несет в себе разрушительные последствия при ее осуществлении на информационную инфраструктуру государственного ресурса или объекта критической инфраструктуры (рис 12).

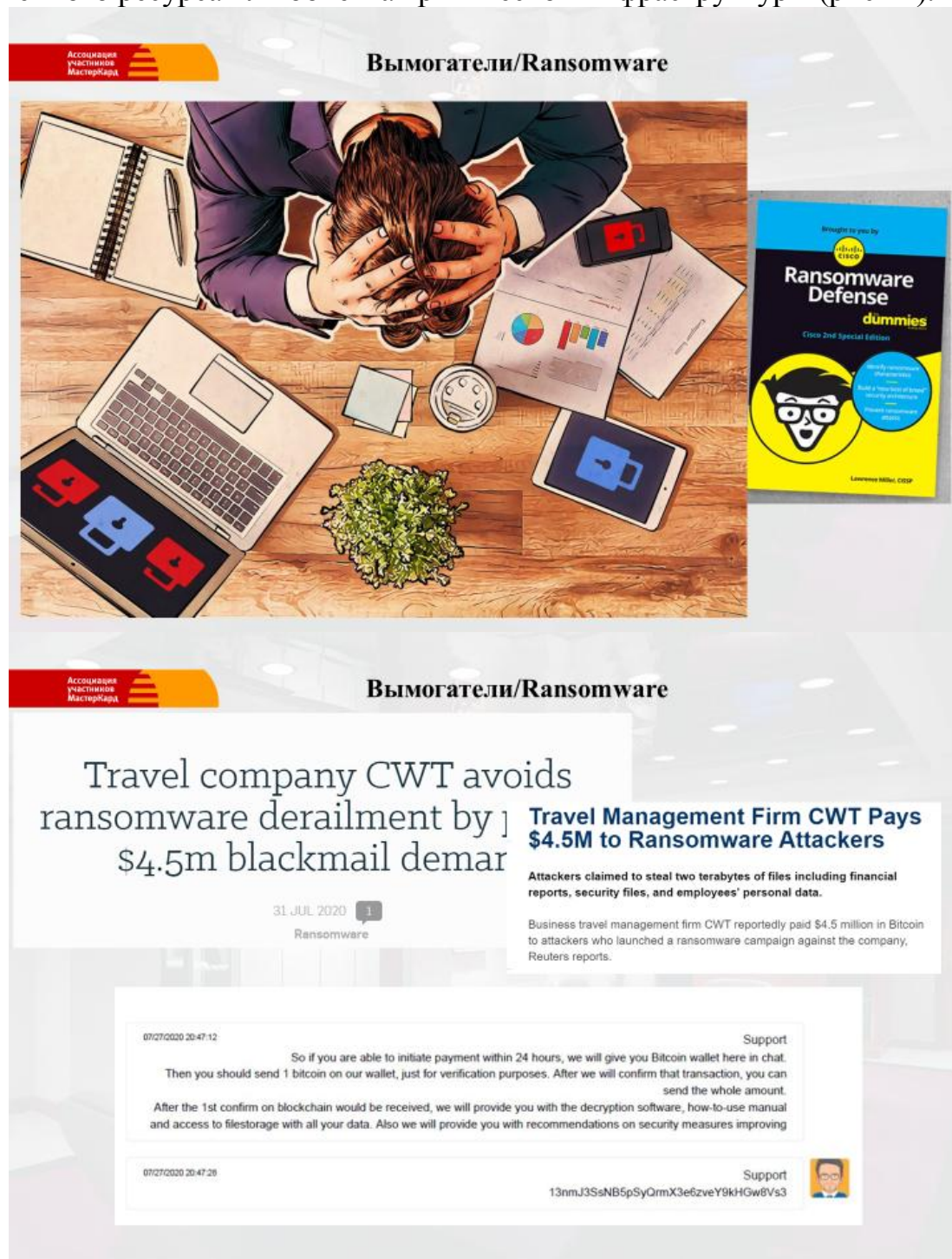


Рис. 12. Примеры вымогательства и его последствий

На сегодняшний день социальная инженерия это проблема номер один в сфере противодействия киберпреступлениям. В большинстве случаев мошенники общаются с потенциальной жертвой по телефону и заставляют ее совершить самостоятельно различного рода действия, которые приводят к переводу денежных средств на криминальные счета. Такого рода звонки поступают из оборудованных колл-центров, которые находятся на территории соседнего государства. Текущая политическая ситуация не позволяет плотно вести с ним диалог в сфере противодействия преступности в том числе и по данному направлению.

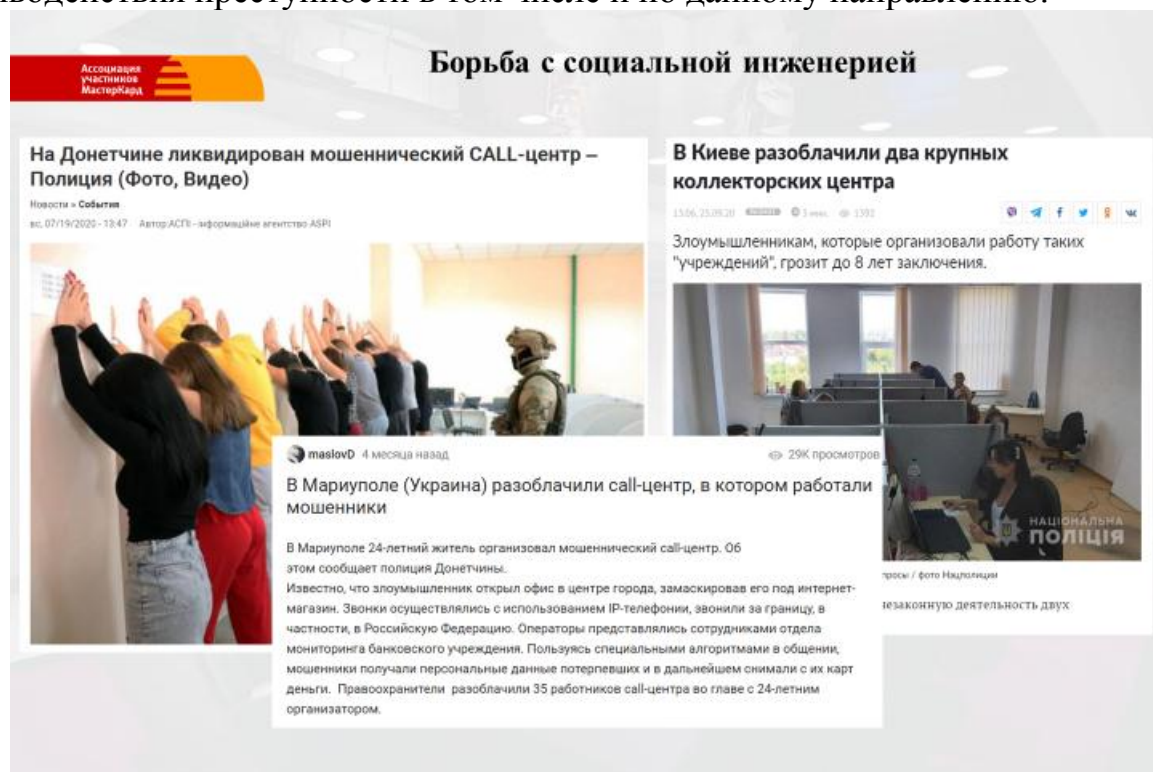


Рис. 13. Подборка новостей о пресечении деятельности мошенников на территории Украины

Смирнов А. А.¹,

*ответственный секретарь Научно-консультативного совета
при Антитеррористическом центре государств-участников СНГ,
кандидат юридических наук, доцент*

ТРОЛЛИНГ КАК МЕТОД КОНТРПРОПАГАНДЫ В ОБЛАСТИ БОРЬБЫ С ТЕРРОРИЗМОМ И ЭКСТРЕМИЗМОМ

Контрпропагандистская работа является относительно новым направлением противодействия терроризму и экстремизму. Повышение его значимости на современном этапе обусловлено комплексом следующих факторов:

1) возросшей активностью пропагандистской и вербовочной деятельности террористических и экстремистских организаций в информационном пространстве, прежде всего в сети «Интернет»;

2) ограниченной эффективностью традиционных мер противодействия: уголовное и административное преследование, блокировка интернет-ресурсов;

3) невозможностью нейтрализации самих радикальных идей, лежащих в основе экстремистской идеологии, запретительными или репрессивными мерами.

В Концепции Сотрудничества государств – участников СНГ в борьбе с терроризмом и иными насильственными проявлениями экстремизма от 26 августа 2005 г. противодействие пропаганде терроризма и экстремизма определено в качестве одного из основных направлений сотрудничества в борьбе с терроризмом и экстремизмом (пункт 12 раздела III).

Контрпропаганда в области борьбы с терроризмом и экстремизмом определяется нами как деятельность по оказанию информационно-психологического воздействия на людей и социальные группы в целях нейтрализации террористической и экстремистской пропаганды [10, с. 22].

Основной целью контрпропагандистской работы в области борьбы с терроризмом и экстремизмом является нейтрализация пропагандистской активности лиц и организаций, направленной на распространение идеологии экстремизма и вовлечение лиц в террористическую и экстремистскую деятельность.

Контрпропагандистская работа в области борьбы с терроризмом и экстремизмом включает три основных направления [10, с. 27]:

1) создание и распространение контента контрпропагандистской направленности (плакатов, баннеров, памяток, видеороликов, художественных и документальных фильмов и т. д.);

2) осуществление коммуникаций антиэкстремистской направленности (профилактических бесед, дискуссий в социальных сетях и форумах);

3) организация и проведение мероприятий контрпропагандистской направленности (групповых встреч, массовых публичных акций, флешмобов, фестивалей и т. д.).

В контрпропаганде в области борьбы с терроризмом и экстремизмом используются различные методы, включая идеологическое развенчание, дезинформирование, дискредитация, устрашение, зашумление и др. Одним из наиболее дей-

¹ © Смирнов А. А., 2020.

ственных методов контрпропаганды также выступает троллинг, направленный на снижение популярности экстремистской идеологии и ее последователей, а также нейтрализацию транслируемых ими мыслей и идей путем их осмеяния и выставления в глупом (нелепом) виде.

Под «троллингом» обычно понимают «использование в сетевом диалоге провокационных, часто оскорбительных реплик, отвлекающих от главной темы, направленных на создание конфликтной ситуации и в конечном счете на разрушение общения» [9, с. 133]. Как видно, в таком подходе троллинг рассматривается как вид провокативной коммуникации в Интернете.

В настоящем докладе мы будем использовать данный термин в более широком значении как *обозначение группы методов психологического воздействия, в основе которых лежат юмор, сатира и провокации*. В данном значении троллинг будет охватывать все три составляющих контрпропагандистской работы в области борьбы с терроризмом и экстремизмом: контент, мероприятия, коммуникации.

Применение таких методов в контрпропагандистской работе не является чем-то новым. В вводной статье тематического выпуска журнала *per Concordiam*, посвященного борьбе с экстремистской идеологией, эксперт центра Маршалла С. Маллинс упоминает о троллинге среди прочих подходов, используемых в мировой практике: «Еще один набирающий популярность метод – это высмеивание террористов и превращение их в объект для издевок» [6, с. 8]. В качестве примера он приводит онлайн-кампании с использованием фотошопа, где на рисунке бойцы ИГИЛ представлены как резиновые утки.

С. Г. Кара-Мурза в своей книге «Манипуляция сознанием» писал о применении юмора в манипулятивных целях: «Сильным средством разрушения психологической защиты против манипуляции сознанием является осмеяние, идеологизированное остроумие. Особенно идеологически нагруженным бывает смех, имеющий своим объектом именно скрепляющие общество символы. Фрейд в монографии «Остроумие и его отношение к бессознательному» писал о важных социальных функциях тенденциозных остроумий, о том, что они служат «оружием атаки на великое, достойное и могущественное, внешне и внутренне защищенное от открытого пренебрежения им» [4, с. 214]. Феномен «народной смеховой культуры» подробно изучен в работе М. М. Бахтина [1].

К воздействию юмора и сатиры могут быть особенно чувствительны террористические и экстремистские организации, которые основаны на жестком идейном базисе (религиозные и квазирелигиозные секты, исламистские организации). Хотя они могут быть использованы и против радикальных организаций, формируемых вокруг харизматического лидера, прежде всего, для подрыва авторитета последнего.

Одним из широко известных форм использования юмора в информационном противоборстве являются карикатуры. В статье, посвященной деятельности группы выдающихся советских художников-карикатуристов «Кукрыниксы» в годы Великой Отечественной войны, так характеризуется роль карикатур: «Политическая карикатура в военные годы стала не только частью пропаганды, но и предстала как настоящее оружие. С помощью рисунков талантливых художни-

ков страшный враг превращался в жалкое уродливое существо. Карикатура вызывала улыбку и у суровых воинов, и у тружеников тыла. А улыбка очень была нужна советским людям, принявшим на себя все тяготы войны» [7].

Также к формам сатиры и юмора, которые традиционно применялись в пропаганде, относятся: анекдоты, шутки, сатирические рассказы, песни, фильмы, картины и т. п. В современных условиях к этому списку добавляются: демотиваторы, фотожабы, смешные картинки и фотографии, другие формы «приколов». Для обозначения информации как забавной в сленге молодежной интернет-аудитории используется междометие «лол», образованное от английской аббревиатуры lol, интерпретируемой как «громко смеюсь» или «много смеха», а для обозначения самого вызываемого чувства удовольствия и веселья – существительное «лулзы» (от англ. lulz) [9, с. 63–66]. «Я сделал это ради лулзов» – известный лозунг троллей.

Нужно выделить такую многомерную форму современной смеховой культуры, как «*интернет-мем*» (также встречаются такие сленговые обозначения, как «мемас», «мемчик»). Исследователь С. А. Шомова определяет интернет-мем как «специфический тип сообщений в Сети, объединяющий разножанровые и многообразные по своей семиотической природе краткие высказывания на актуальные для сетевого сообщества темы и обладающий при этом – благодаря яркости, броскости смыслового содержания и/или визуальной «упаковки» – вирусной природой» [11, с. 18].

Несмотря на свою преимущественно юмористическую природу, интернет-мемы представляют собой чрезвычайно мощный инструмент воздействия на общественное сознание, в связи с чем они являются объектом пристального внимания специалистов по информационным войнам [2].

Интернет-мемы обладают вирусной природой, способностью самокопирования и распространения в медийном пространстве. При этом при тиражировании мема происходит его постоянная трансформация, состоящая в обрастании дополнительными смыслами, коннотациями или вписывании в новые предметные контексты.

Использование интернет-мемов в контрпропагандистской работе в сфере борьбы с терроризмом и экстремизмом представляется нам весьма перспективным направлением. Оно включает в себя как самостоятельное создание мемов, так и использование существующих в нужном контексте. Очевидно, что второе направление является гораздо более простым, поскольку нужно обладать большим умением для конструирования нового мема и прилагать определенные усилия для его раскрутки на первоначальном этапе.

В интернете существуют специальные платформы, именуемые имиджбордами, где публикуются разнообразные мемы (наиболее известными из них в России выступают MDK, Двач, 4ch и др.). В связи с этим полагаем возможным создание и администрирование специализированных пабликов и сообществ, где также будут публиковаться интернет-мемы с позитивным и антиэкстремистским контентом.

В этом плане представляет интерес функционирование популярного российского анонимного *интернет-ресурса* «Д//ихад» (каналы в Twitter, Telegram и

ВКонтакте). В нем осуществляется активный троллинг представителей радикальных исламистских движений, нередко в весьма провокативной манере [12]. Администраторы ресурса обладают необходимыми знаниями в области ислама, языка и культуры мусульманских стран, а также глубоко осведомлены о формах и методах виртуальной активности террористов и экстремистов. Используя данные знания в сочетании с юмором и интернет-мемами, они создают большое количество тематического контента, в котором умело и тонко высмеивают членов радикальных организаций и их сторонников. Этот ресурс не только популярен среди широкой российской аудитории телеграм-каналов, но и находит читателя среди самих джихадистов. Об этом свидетельствуют многочисленные скриншоты из чатов последних, которые периодически публикует «Д///ихад».

Сам рассматриваемый интернет-ресурс вряд ли можно оценить как положительный, однако нельзя не признать, что некоторые применяемые его авторами приемы антиэкстремистского троллинга являются весьма эффективными.

Вернемся к изначальному, узкому пониманию троллинга как провокационной коммуникации в сети. Троллинг интересует нас не как социальный феномен, а как метод психологического воздействия.

В коммуникативном процессе троллинг обоснованно рассматривается в качестве *формы речевой агрессии* – целенаправленного, мотивированного, конфликтного речевого поведения, в основе которого лежит негативное эмоциональное воздействие на адресата [3, с. 110]. Троллинг направлен на внесение раздора в процесс коммуникации, например, путем перевода фокуса внимания с обсуждения серьезной темы на перепалку с переходом на личности [5, с. 291-292]. По словам Г. Почепцова, троллинг осуществляется посредством провоцирования объекта атаки на эмоциональную реакцию [8].

Т.А. Воронцова выделяет две основные техники троллинга [3, с. 112-113]:

1) *шоковая техника* – представляет собой агрессивное опровержение общего мнения. Как правило, при общей положительной тональности комментариев тролль «вбрасывает» сообщение с резко отрицательной оценкой, что вызывает возмущение остальных участников;

2) *переход на личности* – предполагает высказывание, содержащее резко негативную оценку кого-либо из участников коммуникации (оценка может касаться его личных качеств, компетентности по отношению к обсуждаемой проблеме или коммуникативной компетентности) либо его высказывания (указание на умышленную ложь или сознательное искажение фактов, негативная оценка содержания и стиля высказывания).

Весьма близкими по значению выступают понятия «флейм» («флейминг») и «флуд», обозначающие схожие проявления «разрушающей коммуникации».

Флейм (от англ. flame – пламя) определяется как «спор с оскорблениями, коммуникативный конфликт, агрессивная полемика в Интернете» [9, с. 152-153]. Флейминг представляет собой агрессивное речевое взаимодействие (взаимный троллинг), смыслом которого является сам полемический процесс, т. е. спор ради спора, в котором все средства хороши. В ходе этого процесса предмет обсуждения часто уходит на второй план и для участников коммуникации становится важнее «кто кого» [9, с. 113-114].

Флуд (от англ. flood – наводнение») означает многочисленные сообщения, не связанные с темой диалога и отвлекающие от ее обсуждения. Как правило, имеет целью создание помех для коммуникации [9, с. 153-154].

В контрпропагандистской работе в области борьбы с терроризмом и экстремизмом троллинг, равно как флейминг и флуд, возможно использовать в онлайн-новых коммуникациях на различных форумах радикальных движений (на платформах в ВКонтакте, Telegram, WhatsApp и др.) для нарушения дискуссий, дискредитации их активных участников и внесения разногласий между ними. Также троллинг может применяться и при комментировании публикаций на интернет-сайтах, в блогах, пабликах и сообществах для нейтрализации определенных комментариев и дискредитации их авторов.

Библиографический список

1. Бахтин, М. М. Творчество Франсуа Рабле и народная культура средневековья и Ренессанса. М., 1990.
2. Виловатых, А. В. Меметика как инструмент современного информационного противоборства // Проблемы национальной стратегии. – 2018. – № 5. – С. 141–154.
3. Воронцова, Т. А. Троллинг и флейминг: речевая агрессия в интернет-коммуникации // Вестник Удмуртского университета. – 2016. – Т. 26, вып. 2. – С. 109–115.
4. Кара-Мурза, С. Г. Манипуляция сознанием : учебное пособие. – М.: Алгоритм, 2004.
5. Ксенофонтова, И. В. Специфика коммуникации в условиях анонимности: меметика, имиджборды, троллинг // Интернет и фольклор : сборник статей. М. : Государственный республиканский центр русского фольклора, 2009. С. 291–292.
6. Маллинс, С. Важность идеологии // Per Concordiam. – 2016. – № 4, т. 7.
7. Павлов, В. Кукрыниксы – художники Победы // ИСТОРИЯ.РФ. 2 мая 2019 г. URL: <https://histrf.ru/biblioteka/b/kukryniksy-khudozhniki-pobiedy> (дата обращения: 20.08.2019).
8. Почепцов, Г. Троллинг: незванный гость в твоём доме // Media Sapience. 8 июля 2017 г. URL: https://ms.detector.media/trends/1411978127/trolling_nezvanyu_gost_v_tvoem_dome. (дата обращения: 20.07.2019).
9. Словарь языка интернета.ru / под ред. М. А. Кронгауза. – М. : АСТ-ПРЕСС КНИГА, 2016.
10. Смирнов, А. А. Организация контрпропаганды в области борьбы с терроризмом и экстремизмом : научно-практическое пособие / А. А. Смирнов; под ред. А. П. Новикова. – М. : АТЦ СНГ, 2020.
11. Шомова, С. А. Мемы как они есть : учебное пособие. – М.: Аспект Пресс, 2018.
12. «Диванные муджахиды грозились отрезать нам головы». Амир «Д//ИХАД» о диванных муджахидях, пленительных гуриях и взрывных лулзах // Лента.ру. 30 июня 2016 г. URL: https://lenta.ru/articles/2016/06/30/sochnie_babahi/ (дата обращения: 30.07.2019).

Берладир Ю. В.¹,

*начальник группы анализа обстановки отдела
ситуационного анализа, мониторинга угроз
и подготовки проектов решений Антитеррористического
центра государств – участников СНГ,
кандидат юридических наук, доцент*

К ВОПРОСУ О ПОНЯТИИ И ПРИЧИНАХ ОДИНОЧНОГО ТЕРРОРИЗМА

Большая часть научных и аналитических исследований проблем терроризма посвящена деятельности международных террористических организаций. Однако одним из аспектов усиления террористических угроз в последнее десятилетие является рост террористических актов, совершаемых террористами-одиночками. Как отмечается исследователями феномена террористов-одиночек, большая часть террористических актов (до 70 %), произошедших в Европе с 2006 г., совершалась террористами-одиночками – так называемыми «одинокими волками» (остальные – не идентифицированы или осуществлены группами более трех человек)[1].

В настоящее время в научной литературе можно встретить несколько определений понятия «террорист-одиночка», в рамках которых данный феномен приобретает различные, иногда противоположные, сущностные черты. Исходя из предмета данной статьи, предлагается уточнить исходное понятие термина «террорист-одиночка» на основе общих признаков данного явления, наиболее полно раскрывающих его сущность и отличия, выделенных из имеющихся определений², а также с учетом результатов анализа практики деятельности правоохранительных органов в данной сфере.

Так, под *террористом-одиночкой* в терминологии, употребляемой Контртеррористическим комитетом Совета Безопасности ООН, понимается «*индивид, совершающий преступный акт насилия в политических целях, действуя независимо, без явной связи с руководством террористической организации и/или вне организационной иерархии*»[2].

В свою очередь в международном междисциплинарном исследовании, подготовленном под эгидой британского Королевского объединенного института оборонных исследований (RUSI) под терактом, совершаемым в одиночку, понимается «угроза или применение насилия *отдельным злоумышленником* (или небольшой ячейкой), чьи действия движимы не чисто личными, материальными причинами, а *преследуют цель оказания влияния на значительную группу лиц*, также предпринимаемые *без непосредственной* посторонней поддержки в планировании, подготовке и осуществлении нападения, наконец, чье решение приступить к действиям *не обусловлено указаниями со стороны* какой-либо группы или других индивидов (притом, что *может быть ими инспирировано*)».

¹ © Берладир Ю. В., 2020.

² Обоснованность и допустимость самих определений не является предметом данного исследования.

В литературе по данной теме можно найти и иные определения, например:

– «*индивид, совершающий предумышленный насильственный акт, скрытно следующий утвердившейся идеологии, исповедуемой организацией. Одиноким волк может иметь **неустойчивые связи** с формально признанной террористической организацией, или группой ненависти, но может действовать и вне связи с кем-либо*» [2];

– «*лицо, формально не входящее в состав ячейки террористической организации и самостоятельно совершающее террористический акт вследствие саморадикализации*» [3].

Исходя из перечисленных определений, сущностными чертами террориста-одиночки как субъекта террористической деятельности являются:

1) *Количественный состав субъектов* – от 1 до 3 человек. Наиболее очевидный признак, прямо вытекающий из смысловой трактовки самого термина, однако имеющий несколько расширенное толкование, позволяющее относить к данному явлению не одного террориста, а малую группу до 3 человек. Отнесение к террористическим актам, совершенным террористами-одиночками, тех из них, которые совершены группой 2–3 человека (например, семейной парой или родственниками) будет корректным при условии соответствия остальным признакам одиночного терроризма (наличие идеологических убеждений, саморадикализация, самостоятельность планирования и исполнения террористического акта).

2) *Наличие идеологических убеждений*, сформированных в том числе вследствие саморадикализации, как отличительный признак террориста-одиночки. При этом саморадикализация представляет собой процесс принятия идей политического, религиозного или другого экстремизма, в рамках которого формирование у лица психологической готовности к совершению теракта и принятие радикальной идеологии происходит в ходе самостоятельного поиска и изучения информации, в том числе экстремистской и террористической направленности, под влиянием иных обстоятельств и их субъективной оценки, но не в ходе вербовочных мероприятий или обработки лица в составе террористической организации. Хотя в основе действий террориста-одиночки может лежать идеологическая подоплека, родственная идеологии устойчивой структуры – признанной террористической организации или группы ненависти (Hate Group).

Современные исследования указывают на то обстоятельство, что у террориста-одиночки может быть своя собственная идеологическая концепция, которая состоит из нескольких, зачастую абсолютно разных идеологий [4]. При оценке такого признака, как саморадикализация, целесообразно делать акцент на признаке самостоятельности в принятии лицом решения о совершении теракта (т. е. самостоятельном достижении психологической готовности к его совершению), поскольку в современном мире человек практически никогда не находится в информационном вакууме и процесс поддержания коммуникативных связей с приверженцами схожей идеологии и лицами, разделяющими его взгляды, включая членов террористических организаций, является естественным процессом коммуникации с единомышленниками.

В любом случае, наличие идеологии, как системы идей и взглядов политического, религиозного, национально-этнического, экономического и иного содер-

жания, обосновывающих необходимость и допустимость террористической деятельности лица, является отличительным признаком одиночного терроризма от других видов насильственных преступлений (из соображений мести, корысти, в результате психического расстройства).

1) *Отсутствие формальных связей*¹ с членами террористических организаций. Данный признак подлежит оценке в совокупности со следующим – самостоятельность лица при принятии решения и совершении террористического акта. Установление наличия данного признака является в некоторых случаях проблематичным, например, в отношении лиц, ранее входивших в состав террористической организации либо поддерживающих регулярные контакты с ее членами, при условии, что такое членство или контакты не оказали непосредственного влияния на принятие решения о проведении конкретного террористического акта – т. е. были совершены не по указанию и не под руководством террористической организации.

2) Самостоятельное совершение террористического акта. Данный признак непосредственно связан с предыдущими. Под ним понимается отсутствие какой-либо информационной, финансовой, материальной и иной прямой внешней помощи либо руководящих указаний террористу-одиночке при принятии решения, планировании, подготовке и совершении им террористического акта. Исполнитель самостоятельно, без чьих-либо указаний, принимает решение о подготовке и совершении террористического акта, включая выбор объекта нападения, времени и способа совершения террористического акта, самостоятельно приискивает необходимые средства, получает нужную ему информацию, в том числе о тактике действий правоохранительных органов и т. д.

Выделение одиночного терроризма в самостоятельный вид имеет значение для практики деятельности правоохранительных органов в связи с тем, что данное явление имеет повышенную опасность ввиду изолированности преступника, отсутствия либо незначительной выраженности «информационного следа», свидетельствующего о сформированном намерении совершить террористический акт, его планировании, подготовке и, как следствие, ограниченности возможностей заблаговременного выявления готовящегося террористического акта правоохранительными органами и специальными службами. Более того, как отмечают специалисты, даже если спецслужбы располагают информацией о потенциальной террористической опасности, сам момент перехода террориста-одиночки от планов к действиям отследить чрезвычайно трудно[5].

Следует отметить, что наиболее важными для квалификации деяния в качестве одиночного терроризма признаками являются количественный состав и самостоятельное совершение террористического акта. Такие признаки как саморадикализация и отсутствие формальных связей с террористической организацией имеют неоднозначное толкование, сложны в фактическом установлении их наличия и подлежат оценке в совокупности с остальными.

¹ Под *формальными связями* в данном случае понимаются связи субординации и координации, регулируемые в соответствии с принятыми в террористической организации правилами, направленные на достижение ее задач и целей.

Полная изоляция и «выключенность» из общественных и информационных связей террориста-одиночки невозможны. В большинстве случаев совершению террористического акта могут предшествовать определенные действия лица, будь то поиск соответствующего контента в сети, изменения в поведении незадолго до совершения теракта либо действия, оставляющие иной «информационный» след. Выделение терроризма одиночек в отдельную категорию необходимо для более детального изучения особенностей данных лиц, поисковых признаков, специфики приемов и способов совершения терактов, причин и условий, способствующих их радикализации, и, в конечном счете, совершенствования тактики действий правоохранительных органов по заблаговременному выявлению и пресечению совершаемых ими терактов.

Сложность выявления намерений террориста, как отмечалось выше, связана со слабой выраженностью или отсутствием «информационного» следа в сравнении с терактами, подготовленными и совершаемыми под руководством террористической организации.

Таким образом, в наиболее общем виде *терроризм одиночек* представляет собой одну разновидностей терроризма – индивидуальный терроризм, при котором террористический акт непосредственно планируют, готовят и совершают от 1 до 3 человек, руководствуясь определенными идеологическими убеждениями, за принятием решения о совершении теракта и действиями которых не стоит какая-либо террористическая или иная организация.

Одиночный терроризм как явление порождается также условиями, объективно складывающимися в социальной среде, во взаимоотношениях людей. Поэтому условия, способствующие нарастанию данной угрозы, опосредованы отдельными особенностями современного общества. Следует согласиться с исследователями, называющими в числе таковых[6]:

- формирование общества потребления и связанную с этим смену ценностных ориентиров общества, возрождение гедонизма и оттеснение традиционных ценностных систем, включая религиозные, а в итоге – цивилизационный конфликт и радикализацию ислама;

- ускоренную цифровизацию и развитие информационных технологий – электронных СМИ, компьютерных технологий, Интернета, и как следствие – доминирование информационного поля в качестве единственного общественно-го феномена, с которым человек находится в постоянном контакте, формирование зависимостей от различных компонентов виртуального информационного пространства.

Ряд факторов и условий, порождающих терроризм одиночек, специфичен для определенных регионов. Собственно миграционные процессы в Европе и цивилизационный конфликт выступают в качестве ключевых причин нарастания угрозы одиночного терроризма. Следует отметить, что проблема нынешнего терроризма в Европе (преимущественно терроризма одиночек) является более острой и социально опасной, чем в прошлом. Она становится судьбоносной для европейцев, о чем свидетельствуют трагические события осени 2020 года.

В государствах – участниках СНГ, в отличие от стран Европы, пока ситуация не столь критичная. Как отмечают эксперты, «просмотр материалов запрещенно-

го в России ИГИЛ и онлайн-радикализация в большинстве случаев не влияют на поведение в реальной жизни. Страх погибнуть или быть арестованным пересиливает обещанные блага»[7].

Подытоживая, следует отметить, что радикализация террористов-одиночек – явление исторически не новое, однако приобретающее свои особенности в современных условиях. Одной из отличительных черт терроризма одиночек сегодня является то, что в большинстве случаев при совершении терактов террористы-одиночки имели определенные связи с террористическими организациями, пусть даже виртуальные, выраженные лишь в изучении соответствующего контента, а их саморадикализация в большинстве случаев весьма условна, так как является результатом продуманной информационно-пропагандистской обработки. Крупные международные террористические организации, на основе проведения массовой информационной кампании, нацеленной на радикализацию целевой аудитории либо провокацию террористической активности одиночек, придали данному феномену широкое распространение.

Вместе с тем, восприимчивость к радикальным идеям зачастую объясняется психологическим складом личности, психическим нездоровьем, стремлением получить признание своей группы идентификации, которая, по мнению потенциального террориста, подвергается гонениям и ведет праведную жизнь, но может диктоваться и социальным контекстом: социальной изоляцией и утратой возможностей для удовлетворения потребностей личности.

Кроме того, особенности постиндустриального общества, ускоренной информатизации, порождающие внутренние личностные противоречия, межцивилизационные конфликты в системе ценностей, наряду с последствиями активных миграционных процессов в Европе и Центрально-Азиатском регионе создают благоприятные условия для реализации международными террористическими организациями на практике концепции сетевого терроризма и бессистемного вовлечения отдельных индивидов в индивидуальную террористическую деятельность.

Разработка методов предупреждения терактов, совершаемых террористами-одиночками, требует взаимодополняющих усилий специалистов в различных областях, которые могли бы охватить весь диапазон мероприятий – профилактику, раннее выявление потенциальных террористов, предотвращение нападения до его начала, нейтрализацию формирующейся угрозы и ее источника.

Террористы-одиночки активны в социальных сетях, и, отслеживая их высказывания, можно выявлять экстремистские убеждения потенциальных преступников. Очевидна эффективность развития возможностей Интернета для раннего выявления и предупреждения террористической активности одиночек, включая создание системы передачи тревожной информации от отдельных пользователей к органам власти.

В целях выявления религиозно ориентированных террористов необходимо активно работать с религиозными общинами и налаживать отношения доверия между ними и правоохранительными органами. Вместе с тем приоритет среди всех мер по противодействию одиночному терроризму должен отдаваться оперативной работе с окружением террориста.

Помимо аналитиков и оперативного состава правоохранительных органов и спецслужб к профилактике и выявлению террористов-одиночек должны активнее привлекаться педагоги, психологи, психолингвисты и психотерапевты. Кроме того, широкой общественности следует предоставить информацию, помогающую распознать экстремистское поведение. Надо убеждать людей в необходимости сообщать об этом правоохранительным органам.

Немаловажную роль играет обмен опытом между правоохранительными органами и спецслужбами государств – участников СНГ, Европолom по выявлению и пресечению деятельности террористов-одиночек, а также своевременному обмену оперативной информацией, в том числе о фактах проявления интереса к экстремистскому контенту в сети Интернет, поддержании контактов с радикально настроенными лицами, объявлении потенциальными террористами о своих намерениях и т. д.

Библиографический список

1. Global terrorism index 2015: Measuring and understanding the impact of terrorism / Institute for economics and peace. – N.Y.; Sydney; Mexico, 2015. – 108 p. – Mode of access: <http://economicsandpeace.org/wp-content/uploads/2015/11/Global-Terrorism-Index-2015.pdf>.
2. Тузмухамедов, Б. Индивидуальный терроризм: поиск дефиниций и подходов к противодействию [электронный ресурс] // Россия в глобальной политике. – 2018. – № 6. – Режим доступа: <https://globalaffairs.ru/articles/terror-odinochek> (дата обращения 24.12.2020).
3. Террорист-одиночка не так уж и одинок... [электронный ресурс] // Посреди России: информационно-аналитический журнал. URL : <https://posredi.ru/terrorist-odinochka-ne-tak-uzh-i-odinok.html>.
4. Павлик, М. Ю. Терроризм одиночек: основные тенденции и особенности противодействия / М. Ю. Павлик, К. В. Боричев // Вестник Санкт-Петербургского университета МВД России. – 2020. – № 1 (85). – Режим доступа: <https://cyberleninka.ru/article/n/terrorizm-odinochek-osnovnye-tendentsii-i-osobennosti-protivodeystviya>.
5. Кореньков, А. Террор будущего. Кто такие террористы-одиночки [электронный ресурс] // ИА «Лигабизнесинформ». URL: https://news.liga.net/world/articles/terror_budushchego_kto_takie_terroristy_odinochki.
6. Терроризм в исторической ретроспективе и современных условиях : монография / под ред. В. Ю. Бельского, А. И. Сацуты. – М., 2019. – 479 с.
7. Военное обозрение. 1 августа 2011 г. <https://topwar.ru/5890-glavnoy-ugrozoy-mira-mogut-stat-terroristy-odinochki.html>.

*Манойло А. В.¹,
профессор МГУ имени М.В. Ломоносова
(факультет политологии), доктор политических наук*

ИНФОРМАЦИОННЫЕ ВОЙНЫ И ПСИХОЛОГИЧЕСКИЕ ОПЕРАЦИИ: ИГРЫ, В КОТОРЫЕ ИГРАЮТ СПЕЦИАЛЬНЫЕ СЛУЖБЫ И ПРОФЕССОРА ПОЛИТОЛОГИИ

Информационные войны в современном мире стали одним из привычных факторов окружающей нас действительности. Каждый из нас ежедневно оказывается в фокусе действия той или иной информационной атаки, несущей заряд убийственной агрессии, направленной как на общество в целом, так и на сознание каждого человека в отдельности. Вместе с тем, большинство наиболее опасных операций информационной войны американского происхождения имеют в своей основе одну и ту же стандартную организационную схему, представляющую собой последовательность информационных вбросов, разделенных периодами экспозиции (информационной «тишины») и согласованных по времени, целям, задачам и объектам воздействия.

Современные технологии информационных войн, основанные на манипулятивном управлении политическим сознанием и поведением граждан, исключительно опасны: их главная задача – разделить и поляризовать общество, разорвать его на множество клочков и фрагментов, заставить эти фрагменты искренне ненавидеть друг друга, чтобы затем столкнуть их между собой, инициировав борьбу на уничтожение, или объединить их агрессию в единый поток и направить его против действующей власти. При этом цель информационной войны – сломить волю противника к сопротивлению и подчинить его сознание своей воле. Высокая эффективность информационных атак и растерянность, являющаяся типичной реакцией большинства стран на акции информационной войны, делает информационные войны одним из основных элементов современных гибридных войн, таких как война в Сирии или конфликт на Украине.

Технологии информационных войн активно и весьма охотно применяют не только страны Запада (прежде всего, США, где термин «информационная война» официально закреплен в полевом уставе Армии США «Психологические операции»), но и международными террористическими организациями и группировками, такими как запрещенные в Российской Федерации «Исламское государство» (ИГ), Аль-Каида, «Братья-мусульмане». ИГ по всему миру ищет, вербует или нанимает на работу высококлассных специалистов в области кибервойны и информационного противоборства, которые в информационно-идеологическом поле конкурируют с силами специальных операций ведущих стран Запада.

Информационная война – это вооруженный конфликт, в котором столкновение сторон происходит в форме информационных операций с применением информационного оружия. Структурно современная информационная война состоит из последовательности информационных операций, объединенных замыслом и согласованных по целям, задачам, формам и методам воздействия.

¹ © Манойло А. В., 2020.

В Соединенных Штатах Америки термин «информационная операция» официально закреплён в полевом уставе Армии США «Психологические операции» FM 33-1. Согласно этому источнику, информационная операция – это проводимая в мирное или военное время плановая пропагандистская и психологическая деятельность, рассчитанная на иностранные дружественные, враждебные или нейтральные аудитории с тем, чтобы влиять на их отношение и поведение в благоприятном направлении для достижения политических и военных целей.

При этом американские военные выделяют три уровня ведения информационных войн: стратегический, оперативный, тактический. Уровень информационных операций – это именно оперативный уровень ведения информационной войны. Тактический уровень ведения информационной войны – это уровень отдельных информационных атак, совокупность которых составляет одну информационную операцию. Стратегический уровень соответствует самой информационной войне, оперативный – информационным операциям, тактический – информационным атакам (отдельным вбросам). В российской практике под информационными операциями понимают оперативные комбинации на каналах ОТКС (открытых телекоммуникационных сетей), сочетающие в себе методы ведения информационной, оперативной и оперативно-разыскной деятельности. Часто эти операции принимают форму оперативных игр (рис. 1).

Операция информационной войны начинается с информационного вброса, направленного на объект (мишень) атаки или на его ближайшее окружение. Если одного вброса недостаточно для того, чтобы сломить противника или подчинить его волю своей, используют серию информационных вбросов, помещаемых в публичное информационное пространство по очереди, последовательно, через заранее намеченные промежутки времени, обеспечивающие эффект экспозиции.

Информационный вброс – это пул специально подготовленной информации, стимулирующей объект информационного воздействия на совершение немедленных ответных действий (в качестве реакции на внешний стимул).

ОПЕРАТИВНЫЕ ИГРЫ



III. Прага, 28 апреля 2020 года
чешский журнал «Respekt»:
«14 марта 2020 г. в Прагу прибыл российский дипломат («человек с дипломатическим паспортом»), доставивший в российское посольство ризин – чрезвычайно опасный сильнодействующий яд»
Источник инф.: анонимные сотрудники чешских спецслужб

Синдром Скрипаля: «Солсберецкая матрица» (шаблонная схема обвинений РФ):
1) яд – есть (в Солсбери был «новичок», здесь – ризин);
2) ликвидатор – есть (в Солсбери были Петров и Боширов, в Праге – А.В. Кончаков, зам. руководителя Россотрудничества); 3) повод для мести – есть: 3 апреля 2020 г. чешские власти снесли памятник маршалу Коневу; 4) наконец, есть целый ряд публичных заявлений российских официальных лиц о том, что «это дело с рук не сойдет» и это «преступление... не останется без ответа» (Мария Захарова и др.), свидетельствующих о наличии у российской стороны определенных намерений и мотивов.

IV. 31 мая 2020, CNN
Сьюзан Райс, б. советник Обамы по нац. безопасности, заявила в эфире CNN, что беспорядки, вызванные гибелью Дж. Флойда, могли быть организованы извне по «русской методичке».
Райс подчеркнула, что, «основываясь на своем опыте, [могу сказать, что] это также прямо из российской методички»; «их цель - не просто опозорить Соединенные Штаты, а разделить нас, сделать так, чтобы мы вступили в борьбу друг с другом».

Разрыв программы:
ЕСТЬ ТАКОЙ УЧЕБНИК! 2015 год.
Color Revolutions: Techniques in Breaking Down Modern Political Regimes
by Oleg Karpovich; Andrei Manoilov
ИМЕННО ЕГО РАЙС И ВИДЕЛА В БИБЛ. КОНГРЕССА
The monograph is devoted to the analysis of the problems associated with the dismantling of the political regimes in modern states (both authoritarian and democratic type) and with the role of technology in the process of color revolutions.
2015 - в Библиотеке Конгресса США (есть отметка)

7 июня 2020
Эфир телеканала Звезда

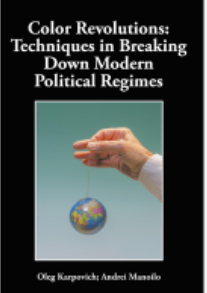


Рис. 1. Примеры оперативных игр

Неправильно считать, что информационный вброс должен содержать только компрометирующую информацию. Содержанием информационного вброса может быть любая информация стимулирующего характера, способная вывести объект атаки из состояния равновесия и побудить его к немедленному совершению спонтанных, неосознанных, часто необдуманных действий. Если грубая лезть воздействует на психоэмоциональное состояние объекта атаки сильнее, чем компромат или шантаж, заставляя его под наплывом эмоций временно утрачивать над собой контроль, то вброс будет насыщен такого рода информацией.

Главным источником сведений о стратегии, тактике, формах и методах ведения информационной войны являются информационные операции, проводимые специальными службами США – такие, как англо-американская операция в Солсбери (более известная как «дело об отравлении Скрипалей», 2018 г.), «Аргентинское кокаиновое дело» (2018), выборы главы Интерпола (2018 г.), завершившиеся поражением нашего кандидата, и «Панамское досье» (2016 г.). Именно они показывают, как именно следует планировать, организовывать и проводить информационные операции – так, чтобы они гарантированно поразили цель, не оставив ей ни шанса на спасение. «Дело Скрипалей» на сегодняшний день продолжает оставаться самой успешной, технологически совершенной и почти безупречно, филигранно проведенной информационной операцией, показавшей, как именно такого рода операции следует осуществлять на практике (рис. 2).



Рис. 2. Дело Скрипалей (2018 – 2020 гг.)

Из новейшей практики информационных операций, затронувших 2020 год, стоит также упомянуть «Пражское дело» (связанное якобы с попыткой провести через границу «человеком с российским дипломатическим паспортом» чрезвычайно опасный яд рицин), заявление Сьюзан Райс об использовании русскими специальной «методички» (по организации госпереворотов) для дестабилизации политической ситуации в США (по словам Райс, она ее сама видела и читала)

и отравление Навального, являющееся точной копией «дела Скрипалей». Все это – операции специальных служб США и их союзников, имеющие серьёзную информационную и психологическую составляющую.

Среди них особо выделяются информационные операции гибридного типа, осуществляемые в спайке с боевыми технологиями других классов и типов:

- «антинаркотеррористическая операция» США против Венесуэлы, начатая 26 марта 2020 года, дополняет сценарий информационной операции (в ходе которой за головы Мадуро и 14 его ближайших соратников была объявлена награда в 10-15 млн. долл.) силовыми методами: угрозой морской блокады, угрозой похищения и ареста и, наконец, угрозой военного вторжения по сценарию вторжения в Панаму в 1989 г. (операция «Гедеон» в этом плане является репетицией);

- операция ЦРУ по захвату (при содействии КГБ Белоруссии) 33 российских граждан, следовавших транзитом в одну из стран Ближнего Востока (в которых США подозревали сотрудников т.н. ЧВК Вагнера), и попытка переправить их на Украину (чтобы следователи контрразведки ФБР могли их беспрепятственно допросить), ставит на первое место активные мероприятия спецслужб, создавая для развертывания на базе этой оперативной комбинации массовой информационной кампании стратегическую перспективу и глубину (включая условия для реализации излюбленных схем и приемов американских специалистов по информационным операциям – «загонной охоты», травли и шантажа).

Отличительной особенностью всех без исключения информационных операций, проводимых спецслужбами США, является лежащая в основе их сценариев одна и та же англосаксонская организационно-технологическая схема. Благодаря этому все без исключения информационные операции США после 2016 г. используют один и тот же, многократно повторяющийся, сценарий, отличающийся в разных «постановках» только деталями антуража, декорациями и «актерами массовых сцен». Данная схема впервые появилась у американцев в конце 2015 г. как ответ на присоединение Крыма – и нашла свое первое применение в «Панамском досье» в 2016 г. До этого момента (точнее, до вхождения Крыма в состав России) у США не было никакой универсальной схемы: все операции разрабатывались как уникальные и неповторимые, под конкретную оперативную ситуацию или игру, и работа организаторов и сценаристов информационных операций была чисто ремесленной. В 2014 г. ситуация резко изменилась: производство Вашингтоном информационных операций ставится на промышленную основу – в дело вступает конвейер, требующий стандартизации выпускаемых «изделий»; только так можно обеспечить массированное применение новейших методов информационного воздействия против русских, «нагло оттяпавших» у США и НАТО Крым. В результате в течение 2014–2015 гг. вся практика оперативных комбинаций и игр в информационной сфере собирается, систематизируется и на ее основе вырабатывается первая в истории США (и всего остального мира тоже) стандартная схема операции информационной войны. Первое испытание в реальных боевых условиях эта схема получает в 2016 г. в скандале с панамскими офшорами – «Панамском досье», ставшим благодаря реализованным в данной схеме новым технологическим приемам успешной информационной операцией, определившей стандарты их проведения на годы вперед.

Все последующие операции ЦРУ уже строятся только на основе «Панамского досье». Так, оперативная игра вокруг «дела Скрипалей» целиком и полностью построена на базе этой схемы; в рамках этой игры спецслужбы США и Великобритании чрезвычайно успешно реализовали два этапа (весной и осенью 2018 г.), по 4 вброса в каждом: «игру с поэтапным повышением ставок» (март-апрель 2018 г.) и «загонную охоту» (сентябрь-ноябрь 2018 г.). И это не единственный пример такого «подражания панамскому делу»: теперь операции информационной войны – это не уникальный креатив, а точно просчитанная, кодифицированная и формализованная технология, практически не дающая осечек.

Противостоять этой технологии крайне сложно – особенно, если противник сам еще не достиг технологического уровня и по-прежнему пытается отразить сыплющиеся на него со всех сторон информационные атаки «практикой умелых импровизаций» или «грозным молчанием»: в стратегическом плане такая тактика всегда ведет к провалу. Тем не менее, в российской практике появился определенный опыт успешного противостояния информационным операциям Запада:

- это операция по разоблачению агента влияния ЦРУ в ближайшем окружении президента Венесуэлы Николаса Мадуро (человека, вступившего за спиной Мадуро в конфиденциальные отношения с разведкой США) – в августе 2019 г., завершившаяся отставкой Джона Болтона, лично руководившего операцией;

- это операция по внедрению в окружение Роберта О'Брайена дезинформации о том, что в оперативном директорате ЦРУ или в аппарате директора национальной разведки действует «крот» (агент русской разведки), передавший летом 2019 г. сведения о контактах Диосдадо Кабельо (друга и соратника Мадуро, шефа Cartel de los Soles) с ЦРУ (с Маурисио Клеве-Короне, директором отдела по делам Западного полушария СНБ США); в результате устроенной О'Брайеном чистки в октябре 2019 г. своих должностей лишились 80 высококвалифицированных сотрудников американской разведки (рис. 3);

БЕЛЫЙ ДОМ И ЦРУ: ПОИСК КРОТА, ИЛИ КАК РАБОТАЕТ ОПЕРАТОР ОТРИЦАНИЯ «НЕ»
ANDREI MANOILU: NO ES CIERTO QUE LOS RUSOS TENAMOS INFORMANTES INTERNOS EN LA CIA, AL MENOS NO POR AHORA

ЧИСТКА РЯДОВ: БОЛЕЕ 80 СОТРУДНИКОВ РАЗВЕДКИ УВОЛЕННЫ

Andrei Manoilo (Andrey Manoylo): No es cierto que los rusos tengamos informantes internos en la CIA, al menos no por ahora

РОБЕРТ О'БРАЙЕН (ОКТАБРЬ 2019): ПОСЛЕ ОТСТАВКИ [БОЛТОНА] МЫ ... ЗАЧИСТИЛИ ОПЕРАТИВНЫЙ ДИРЕКТОРАТ ЦРУ, АППАРАТ СОВЕТА НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ И АППАРАТ ДИРЕКТОРА НАЦИОНАЛЬНОЙ РАЗВЕДКИ. БОЛЕЕ 80 СПЕЦИАЛИСТОВ УВОЛЕННЫ

Quintero: Andrei Viktorovich, la pregunta más importante de interés de los lectores: ¿de quién recibió la información secreta sobre los contactos de la residencia de la CIA en Bogotá con Diosdado Cabello? ¿Tiene relaciones con un agente secreto que trabaja con la dirección de la CIA, el Consejo de Seguridad Nacional de los Estados Unidos y la dirección de inteligencia nacional? No necesitamos nombres, solamente nos gustaría saber más sobre sus fuentes de información.

Manoilo: No. No me codeo aún con personas asociadas a la dirección de la CIA, el Consejo de Seguridad Nacional y la inteligencia nacional de los Estados Unidos. Menos aún son ciertos los rumores que señalan que yo personalmente he reclutado agentes secretos en los Estados Unidos. Yo soy

Рис. 3. Операция по дезинформации советника по национальной безопасности президента США Роберта О-Брайена (октябрь 2019 г.)

– технологии бумеранга и некоторые другие эпизоды.

Так, в июне 2019 г. Диосдадо Кабельо (бывший вице-президент Венесуэлы, действующий председатель Национальной конституционной ассамблеи и, одновременно, руководитель крупнейшего венесуэльско-колумбийского наркокартеля «Cartel de los Soles»), втайне от президента Венесуэлы Николаса Мадуро вступил в контакт с разведкой Соединенных Штатов. Однако уже в конце августа 2019 г. эта связь была вскрыта и предана публичной огласке благодаря грамотно проведенной в отношении Кабельо оперативной комбинации, основанной на информационном вбросе провокационного содержания. В результате в сентябре 2019 г. переворот в Венесуэле был поставлен Вашингтоном «на паузу», и вернулись к нему только в конце марта 2020 г. В практике информационных операций это уникальный случай, когда информационный вброс, вскрывший тайную операцию ЦРУ, заставил реагировать президента США Дональда Трампа, включившегося в операцию прикрытия своей агентуры влияния в Венесуэле. Для специалистов в области информационных и гибридных войн операция по разоблачению Кабельо – образец того, как надо планировать и проводить современные операции информационной войны – «операции прямого действия» (рис. 4).



Рис. 4. Главный принцип проведения операций прямого действия.

Однако для обеспечения коренного перелома в информационном противостоянии России с США этого явно недостаточно: в России система информационного противоборства, способная на равных соперничать с аналогичной системой США, до сих пор не создана. А идти против системы, действующей в США, с жалкими фокусами (и не менее убогим троллингом от таких же убогих спикеров) – затея, заранее обреченная на провал.

Средства массовой информации и коммуникации (СМИ) играют в информационных войнах особую роль. СМИ являются, с одной стороны, каналом доведения информационного воздействия до конкретной целевой аудитории (политических элит, лидеров мнений, широких слоев общественности, политически

активной молодежи), с другой – выступают непосредственным участником конфликтного взаимодействия. В современных конфликтах СМИ активно используются как средство дезинформации и пропаганды, как инструмент манипулирования общественным мнением, массовым сознанием и поведением граждан, как инструмент прямого давления на оппонентов. Именно через так называемые «независимые» СМИ спецслужбы осуществляют вбросы («контролируемую утечку») информации, компрометирующей их соперников, дестабилизирующей политическую обстановку в различных странах, инициирующей массовые протесты в стиле «цветных» революций.

Многие СМИ имеют обыкновение выдавать непроверенную информацию за достоверную, если в ней содержатся элементы сенсационности, тем самым способствуя ее легализации. Экстремисты часто используют СМИ для усиленного разжигания националистических, экстремистских настроений даже в тех регионах, где эти противоречия уже давно не проявлялись; именно прозападные, демократические СМИ формируют романтический образ «цветных» революций в тех странах, где осуществляются «цветные» государственные перевороты, они же затем легитимируют хунты, пришедшие к власти. Западные СМИ активно участвуют в формировании образов «стран-изгоев» (в эту категорию попадают все страны, проводящие независимую от США внешнюю политику), провоцируя новые международные конфликты и столкновения.

Действие американской схемы операции информационной войны представляет собой многократно повторяющийся (циклический) процесс, в ходе которого объект подвергается прямой информационной атаке (в форме вброса информации, провоцирующей объект атаки на немедленное действие). Его ответная реакция (со всеми характерными для данного человека индивидуальными особенностями) считывается по каналам обратной связи, анализируется и поступает в механизм коррекции. На основании выявленных индивидуальных особенностей реагирования объекта атаки на внешние информационные раздражители определяются его «болевые точки», темы и поводы, выводящие человека из состояния равновесия и способные мгновенно его возбудить и довести до крайне неустойчивого «пограничного» состояния, в котором он теряет способность контролировать себя и свои действия. С учетом выявленных «болевых точек» содержание исходного информационного вброса корректируется таким образом, чтобы сфокусировать информационное воздействие именно на этих проблемах, воспринимаемых объектом атаки наиболее болезненным образом. Затем этот вброс вновь вводится в публичное информационное пространство по референтным (для объекта атаки) каналам связи и снова бьет по психике объекта атаки, ломая ее волю к сопротивлению. Только теперь уже более болезненно. Так продолжается до тех пор, пока объект атаки своими ответными реакциями полностью себя не скомпрометирует, либо до тех пор, пока его воля не окажется полностью сломлена или подчинена источнику внешнего управляющего воздействия – вплоть до полного «удушения» воли противника.

Для придания достоверности вбрасываемой информации в современных операциях информационной войны используются так называемые «операции по легализации вбрасываемой информации». По своей природе и функциям это опе-

рации прикрытия (так они называются на языке разведки), придающие вбрасываемой информации вид достоверности, объясняющие ее происхождение (где она хранилась, как попала в руки ее теперешних владельцев) и отвечающие на вопрос, из какого источника она пришла – компетентного или сомнительного.

В современных операциях информационной войны вбросы компрометирующей информации никогда не попадают в информационное пространство без сопровождения – только в рамках проводимой одновременно с вбросом операции прикрытия (операции легализации вбрасываемой информации).

В современных операциях информационной войны используется три основных вида операций легализации вбрасываемой информации:

- «контролируемая утечка»;
- публичные заявления, сделанные от имени пожелавших остаться неназванными официальных лиц;
- публичные заявления уполномоченных официальных лиц (президентов, премьеров, глав национальной разведки и др.).

Среди названных выше операций легализации вбрасываемой информации операции «контролируемой утечки» являются наиболее распространенным видом операций прикрытия. Сам же термин «контролируемая утечка» в информационные войны пришел из разведки.

«Контролируемая утечка» (на языке разведки) – это специальная разведывательная операция, цель которой – дезинформация противника путем передачи ему под видом достоверной информации заведомо ложных или специально сфабрикованных под конкретную задачу сведений «секретного характера» путем создания иллюзии случайной утраты этих сведений секретносителями из-за проявленных ими халатности или неосторожности.

Операции «контролируемой утечки» информации делятся на четыре вида:

- операция утечки, реализованной путем провоцирования журналистов на кражу секретных материалов, с которых в этот момент снимается защита «от взлома» и они на время становятся доступными для потенциальных похитителей;
- технологии класса «WikiLeaks», предусматривающие маскировку заведомо ложных (сфабрикованных) сведений в большом потоке подлинных, но малоценных документов;
- операции типа «перебежчик» (типичный пример такой операции – побег Э. Сноудена и история с его преследованием);
- операции легализации вбросов через механизм публичных дебатов (технологии класса «Псаки – Метью Ли»).

При этом на практике наиболее часто встречается именно первый тип операций, основанный на провоцировании кражи секретных сведений.

При всей своей опасности, информационные войны все же не являются «смертельным оружием»: в этой войне побеждает тот, кто умеет предсказать действия своих противников на несколько шагов вперед и затем нанести удар, который они не ожидают.

Именно так была перехвачена оперативная инициатива в Венесуэле в августе 2019-го: в операции по разоблачению агента ЦРУ в окружении Мадуро с нашей

стороны был сделан всего один информационный вброс, который буквально взорвал ситуацию в Венесуэле, заставив резидентуру ЦРУ в Боготе удариться в панику, перекинувшуюся затем и на штаб-квартиру ЦРУ Ленгли. В ходе нее оперативники ЦРУ сами же завалили собственную операцию, своими руками, без уговоров и принуждения, слив свою агентуру, кадровый состав, каналы агентурной связи и даже те места, где происходили сеансы связи между агентом ЦРУ из окружения Мадуро и его американским куратором.

Но этот пример, к сожалению, едва ли не единственный в огромной череде неудач и провалов, многие из которых напрямую связаны с отсутствием системной работы, квалифицированных кадров и подменой настоящей системной работы по данному направлению импровизированными попытками взять американцев на понт.

Попович А. С.¹,
старший менеджер компании «Веб Шилд»

ТЕХНОЛОГИЯ ПРЕСТУПЛЕНИЯ. КРИПТОВАЛЮТА – ПРЕДМЕТ, ИСКУССТВО ИЛИ СПОСОБ?

Преступники всегда ищут старым аферам новое применение. Особенно это актуально в случае криптовалют.

Криптовалюта – это виртуальная валюта, основанная на математических алгоритмах и защищенная криптографией. Условно все криптовалюты делятся на Биткоин, альткойны и токены. Альткойны – это все криптовалюты альтернативные биткоину, например, Эфириум, Рипл и т. д. Токены – это одновременно единица стоимости и расчета в новых проектах. Они создаются для привлечения инвестиций в новый криптовалютный проект, а когда проект запускается, токены получают стоимость, а значит, становятся криптовалютой и могут торговаться на бирже.

Биткоин, как первый и самый известный представитель криптовалют, работает на основе технологии распределенного реестра, более известного как Блокчейн. Эта технология предназначена для документирования транзакций. Его заявленная цель – исключить посредников в процессе оплаты: банки или платежные системы для обработки транзакций больше не нужны.

Благодаря прозрачности инфраструктуры Биткоина любой пользователь может отследить перевод и убедиться в том, что он был отправлен. Платательщик не может отозвать или заморозить платеж, обманув получателя. Криптовалюта эмитируется в ограниченном количестве, а значит такое явление как инфляция исключено. Блокчейн обеспечивает анонимность операций с Биткоином.

Несмотря на кажущуюся прозрачность криптоинфраструктуры, криптовалюты все чаще используется в схемах обмана. По данным исследовательского фонда Bette Business Bureau криптовалюта в 2019 г. стала самым распространенным объектом аферы, обогнав интернет-покупки, выдачу ссуд, фейковые чеки и расписки.

Криптовалюта играет важную роль в отмывании денежных средств, приобретенных незаконным путем. Согласно исследованиям платежной системы Swift, ежегодно киберпреступники зарабатывают около \$1,5 трлн. Эти средства подлежат трем циклам стирки. Первый цикл – внедрение в финансовую систему. Второй – маскировка: деньги перемещаются по финансовой системе, чтобы запутать следы. Третий – выход из тени: денег либо попадают в легальную экономику, либо инвестируются в преступную деятельность. Для второго этапа стирки преступники зачастую используют криптовалюту благодаря ее свойствам:

1) волатильность;

2) быстрота, невозвратность и анонимность транзакций;

3) отсутствие государственных механизмов регулирования и привлечения к ответственности.

Среди актуальных схем мошенничества с криптовалютой следует выделить:

¹ © Попович А. С., 2020.

- фишинг;
- фальшивые криптовалюты;
- мошеннические ICO;
- финансовые пирамиды;
- Биткоин-миксеры;
- программы-вымогатели;
- криптовалюта, как средство платежа за нелегальные товары или услуги;
- прочее.

Более детально схемы мошенничества с применением криптовалют рассматриваются ниже.

Виртуальная валюта

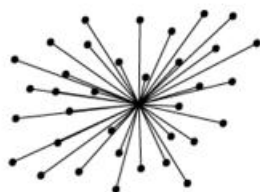
Виртуальная валюта - это цифровое **представление стоимости**, которое выступает в качестве **средства обмена**, либо расчетной **денежной единицы**, либо **средства хранения стоимости** и при этом не подпадающее под понятие законного платежного средства, т.е. не является официально действующим средством платежа при расчетах с кредиторами.



Источник: FATF (2014) - Virtual Currencies: Key Definitions and Potential AML/CFT Risks. [Online](#).



Распределенный Реестр



централизованный
реестр



распределенный
реестр



Блокчейн

- Цепь блоков - постоянно растущий **список записей**.
- Новый блок каждые 10 минут - время вычисления **хэша**.
- Хеширование - подтверждение легитимности изменений в цепи.
- **Изменить или удалить** ранее введенные данные на более ранних блоках **невозможно**.
- Центральный администратор отсутствует.



Думайте о блокчейн как о бухгалтерской книге.

Майнинг = обслуживание

Майнеры

- выбирают несколько переданных в сеть транзакций,
- заключают список транзакций в **блок**,
- проверяют их - создают хэш:
 - c4ca4238a0b923820dcc509a6f75849b,
- добавляют данные в блокчейн (**консенсус**),
- получают вознаграждение.



Криптовалюта

Криптовалюта - это распределенная **пиринговая** виртуальная валюта с открытым исходным кодом, основанная на **математическом коде**. Ее создание, функционирование и защита обеспечивается за счет **криптографических методов**.

- Единицей такой валюты является «**coin**» (монета).
- Условно все криптовалюты делятся на биткоин, альткоины и токены.
- Не все криптовалюты децентрализованные (Пример: Рипл).



Источник: Houben, Robby; Snyers, Alexander (2018). Cryptocurrencies and blockchain - Legal context and implications for financial crime, money laundering and tax evasion. Policy Department for Economic, Scientific and Quality of Life Policies. European Parliament. [Online](#).



Proof of Work vs Proof of Stake



proof of work is a requirement to define an expensive computer calculation, also called mining



Proof of stake, the creator of a new block is chosen in a deterministic way, depending on its wealth, also defined as stake.



A reward is given to the first miner who solves each blocks problem.



The PoS system there is no block reward, so, the miners take the transaction fees.



Network miners compete to be the first to find a solution for the mathematical problem



Proof of Stake currencies can be several thousand times more cost effective.



Источник: Rasic, Amir. Proof of Work vs Proof of Stake: Basic Mining Guide. Blockgeeks. [Online](#).

Преимущества криптовалюты

- высокая степень защищенности транзакций - копирование, взлом и подделка невозможны;
- быстрота перевода транзакции;
- прозрачность данных совершенных транзакций;
- невозвратность всех транзакций;
- отсутствие географических границ;
- анонимность транзакций;
- децентрализация;
- ограниченность;
- отсутствие посредников и комиссий.



Недостатки криптовалюты

- отсутствие гарантий по сбережениям владельцев кошельков;
- анонимность каналов транзакций в блокчейне, как следствие, отмывание преступных доходов и финансирование терроризма;
- волатильность валюты;
- риск запрета государственными органами;
- отсутствие возможности отозвать платеж;
- невозвратность монет при утере ключей.



Способы кражи криптовалют

- мошеннические стартапы
- социальные сети
- мессенджеры
- фальшивые кошельки
- фишинг
- программы-вымогатели
- SIM-своппинг

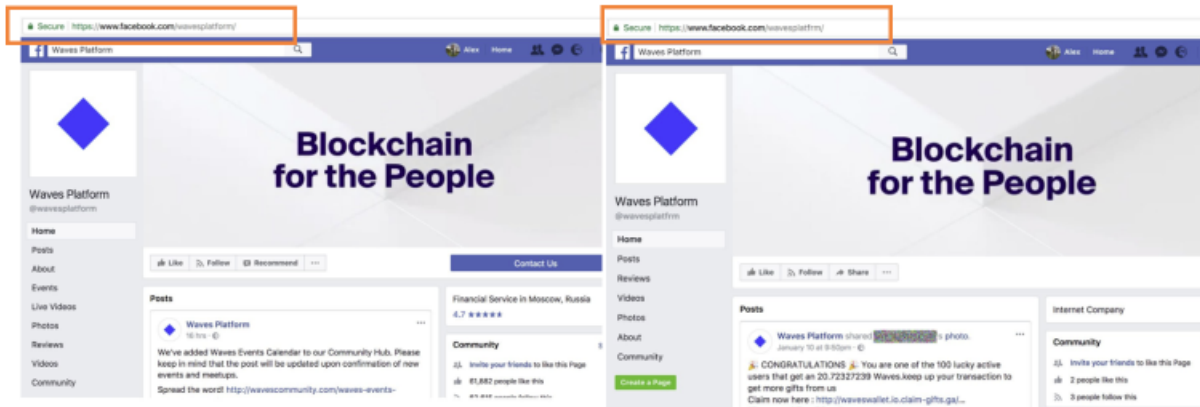


Мошеннические стартапы

- 9 декабря 2018 года в возрасте 30 лет скончался основатель биткоин-биржи QuadrigaCX Джеральд Коттен.
- В день своей смерти Коттен оказался единственным держателем приватных ключей от **холодных кошельков**.
- По данным EY, незадолго до смерти Коттен перевел миллионы долларов в криптовалюту с аккаунтов своих клиентов на конкурирующие биржи. При этом эти средства использовались для покупки недвижимости и предметов роскоши для Коттена.
- 75 тысяч пользователей лишились доступа к своим **цифровым активам** на \$137 млн.

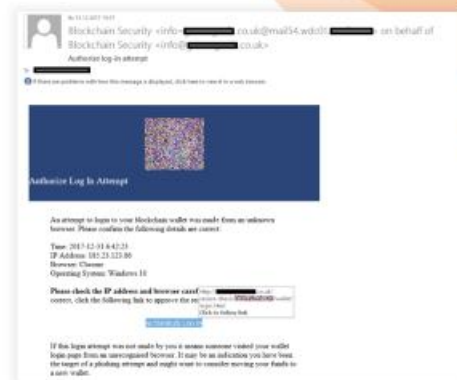


Социальные сети



Фишинг

- Наиболее распространенная схема фишинга - это **спам-рассылка** электронных писем от якобы доверенного адресата.
- Характерной чертой таких фишинговых писем является наличие ссылки, по которой жертва попадает на ресурс, где **учетные данные** ее кошелька будут **украдены**.



Программы-вымогатели

- Программа-вымогатель - это **вредоносное программное** обеспечение (вирус), которое устанавливается на компьютер и зашифровывает данные на нем.
- Вирус попадает на компьютер из сети Интернет или через **фишинговые письма**.
- Путем шантажа мошенники получают от жертвы «**вознаграждение**» в криптовалюте.
- Наиболее распространенный вирус-вымогатель - GandCrab - получил от жертв более \$2 млрд.



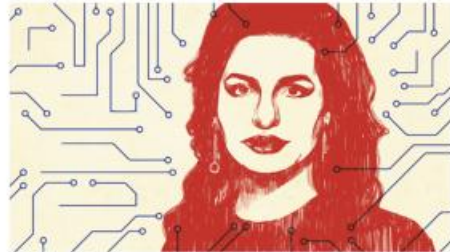
Способы кражи и отмывания средств

- финансовые пирамиды
- фальшивые криптовалюты
- мошеннические ICO
- миксеры
- денежные мулы



OneCoin - финансовая пирамида

- Основательница OneCoin Ружа Игнатова утверждала, что изобрела криптовалюту, способную конкурировать с биткоином.
- Инвесторам обещали **прибыль** размером до **900%** от первоначального капитала.
- Дополнительное вознаграждение за привлечение других вкладчиков.
- Компания **не имела блокчейн**.
- В период с 2014-го по 2017-й год OneCoin привлек **€4 млрд**.



Миксеры

- Несмотря на свою анонимность большую часть криптовалют достаточно легко отследить, особенно, если она в последствие «выводится» в фиатные деньги.
- Для запутывания следа транзакции были разработаны **миксеры**.
- Биткоин-миксер (Bitcoin mixer) — сервис анонимизации, который усложняет или делает **невозможным отслеживание транзакций** в блокчейн путем деления транзакций на мелкие суммы и многократного перемещения между различными адресами.
- Сервисы анонимизации транзакций разделяют по принципу работы на **централизованные** и **пиринговые**.





Гидра

Банк думает, что держатель карты **покупает ноутбук**. В действительности же он **покупает наркотики**.

Регулирование



Russian Federation		
Authorized Overview		
Regulatory Authority UNREGULATED Regulatory Authority: "The Central Bank of the Russian Federation (Bank for Foreign Payments)" Merchant List (R) Merchant List (R)	Regulatory Authority UNREGULATED Regulatory Authority: "The Central Bank of the Russian Federation (Bank for Foreign Payments)" Merchant List (R) Merchant List (R)	Regulatory Authority UNREGULATED Regulatory Authority: "The Central Bank of the Russian Federation (Bank for Foreign Payments)" Merchant List (R) Merchant List (R)

DOWNLOAD ANALYSIS OF LEGAL COMPLIANCE



THE BANKS FOR PREPARING A CONFIRMATION OF LEGAL COMPLIANCE, MERCHANTS RISK ASSESSMENT AND

LEGAL COMPLIANCE VERIFICATION

EXECUTIVE SUMMARY - LEGAL COMPLIANCE VERIFICATION

In order to facilitate understanding for the future BSA participants and to fully understand requirements, this verification addresses 3 separate aspects of business related to compliance: (1) risk assessment, (2) compliance exchange, (3) shipping with cryptocurrency payments and unregulated in Russia for

Legal status on the date of preparation of legal opinion

Activity	Legal Status	Comments	Recommendations
advertising	unregulated	not regulated activity, new provisions expected in the near future	monitoring of changes in law
cryptocurrency exchange	unregulated	not regulated activity, new provisions expected in the near future	monitoring of changes in law
shipping with cryptocurrency payments	unregulated	not regulated activity, new provisions expected in the near future	monitoring of changes in law

Therefore, it has to be noticed, that based on applicable law provisions confirmed by

relevant legal opinions, which related to cryptocurrencies cover by the scope of legal opinion are considered to be:

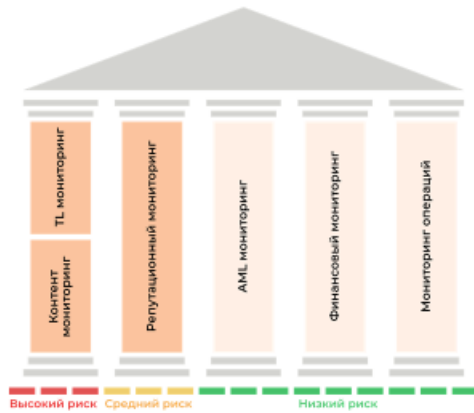
Legal in Russia

However, despite the lack of regulation of many aspects by the relevant legal provisions, it is necessary and highly recommended to monitor changes in the legal environment on an ongoing basis. It is expected in Russia that in the near future legal regulations regarding the cryptocurrency market in a comprehensive manner, including ICO, crypto exchange as well as shipping with cryptocurrency payments will be issued.

The general law applicable to the running of business activities in that country that apply to cryptocurrency activities. Although the law on financial market shall also apply, however, important additional for cryptocurrency market are issued by government bodies, it applies to The Central Bank of the Russian Federation.

Having regard to the fact that all legal analysis should be always up-to-date as well as that Blockchain should be notified of any changes to the information provided to Mastercard, this Confirmation of Legal Compliance should be periodically updated in order to ensure constant compliance with the applicable law provisions.

Стратегия надлежащей проверки



WEB SHIELD®

Мониторинг регулирования является лишь одним из элементов комплексной стратегии надлежащей проверки.

Качественный процесс онбординга и мониторинга должен не только учитывать законодательную базу, но и распространяться на другие сферы.

Reputation Risk			
Indicator	Status	Classification	Rev By
Entity Research	Done	No warnings identified	-
Address(es) Research	Open	Indications for potential reputation issues detected Background research for the address not reviewed/concluded	MD
Contact(s) Research	Rev	Indications for potential reputation issues detected Background research for contact details not reviewed/concluded	MD
Individual(s) Research	Done	Director/Beneficial Owner information missing	-
Website(s) Research	Done	No warnings identified	-
Billing Descriptor(s) Research	Open	Indications for potential reputation issues detected Background research for the billing descriptor(s) not reviewed/concluded	MD
Parent Entity(s) Research	Done	No parent entity name provided	-
Social Media Research	Done	No social network profiles identified	-
Date of Incorporation	Open	Missing incorporation date	-
Website Age	Open	Average website age between 1 - 3 years	-
Better Business Bureau	Open	No BBB rating identified	-
OpenCorporates	Done	No hit on OpenCorporates identified	-
License Verification	Open	License verification not necessary	-
Web Shield Warning List	Open	No entry on Warning List detected	-
MATCH	Open	MATCH query not conducted	-
VMSS	Open	VMSS query not conducted	-
User Defined Blacklist	Done	No blacklist entry detected	-

Content Risk			
Indicator	Status	Classification	Rev By
Business Classification	Med risk	MCC 5499	MD
Content Violation Scan	Rev	Potential content violations detected Potential content violations not reviewed/concluded	MD
Historical Content Violations	Open	Historical content violations identified	-
Deceptive Marketing	Open	Potential deceptive marketing indications detected Potential deceptive marketing indications not reviewed/concluded	MD
Website Compliance Detection	Done	All necessary requirements met (90% + 90%)	-
Merchant Location	Open	Signup/checkout not conducted	-
Subscription/Membership Detection	Open	Indications for subscription billing models not reviewed	-
Price Point Comparison	Open	Not conducted	-
Advertised Payment Options	Open	Potential payment options advertised	-
Closed Member Area	Done	No closed member area detected	-
Phishing Check	Open	No warning issued	-
Sale/browsing	Open	No warning issued	-

Money Laundering Risk			
Indicator	Status	Classification	Rev By
Sanction & PEP Screening Director	Done	No screening conducted	-
Sanction & PEP Screening UBO	Done	No screening conducted	-
Sanction & PEP Screening Entity	Done	No hit(s) detected	-
FATF Country Risk Address	Open	No hit(s) identified	-
FATF Country Risk Contacts	Open	No hit(s) identified	-
FATF Country Risk GeoIP	Open	No hit(s) identified	-
Virtual Address Research	Rev	Virtual address indications confirmed	MD
Portfolio Cross-Check	Open	Shared entity details detected (> 5 hits) Shared details not reviewed	MD
Director Structure	Open	Director/beneficial owner information not provided	-

Transaction Laundering Risk			
Indicator	Status	Classification	Rev By
Site/Reveal Scan	Done	Level 2 Info: 39 - Moderate relationship probability Level 3 Info: 8 - Low relationship probability	MD
Load Balancing Detection	Rev	High load balancing probability detected	MD
Traffic Analysis	Open	Not activated	-
IP Scan	Done	Multiple domains identified on IP address (> 5)	-
Whois Scan	Open	Entity mismatch detected	-
Website Usage	Open	Inactive URL(s) detected (no visitors)	-
Outgoing & Backlinks	Open	Low risk content sites detected	-
Mobile App Detection	Open	No indications for mobile apps detected	-
Affiliate Network Detection	Done	No affiliate network identified	-
Historic TL Violations	Open	No historical transaction laundering violations recorded	-

Минаев В. А.¹,
 профессор Московского государственного
 технического университета имени Н.Э. Баумана,
 доктор технических наук, профессор

Федорович В. Ю.²,
 заместитель начальника по научной работе
 Московского университета МВД России
 имени В.Я. Кикотя, кандидат юридических наук,
 доцент, полковник полиции

МОДЕЛИРОВАНИЕ ИНФОРМАЦИОННОГО ПРОТИВОБОРСТВА В СОЦИАЛЬНЫХ МЕДИА: ОТ ТЕОРИИ К ПРАКТИКЕ

Основная цель социальных сетей (СС) – обеспечение и поддержание связи между людьми, даже когда они находятся друг от друга далеко. Наряду с данным положительным и прогрессивным направлением имеется и отрицательная сторона эксплуатации СС – это распространение деструктивной манипулятивной информации.

По данным исследования Brand Analytics «Социальные сети в России: цифры и тренды» [1], в конце 2019 г. в стране насчитывалось 49 млн. активных авторов соцмедиа. Более трети россиян, используя одну или несколько соцсетей, писали хотя бы один пост в месяц, а все вместе – 1,3 млрд. публичных сообщений (постов, репостов и комментариев). Наиболее популярными по размещению контента площадками стали: ВКонтакте, Instagram, Одноклассники, Facebook, Twitter, YouTube. По итогам 2020 г. к ним ожидаемо добавятся Telegram и TikTok.

Действующие платформы продолжают прирастать аудиторией, происходит активное появление новых участников. Причем данные сервисы далеко не всегда нацелены на позитивное объединение людей, часто истинные цели создания и развития той или иной платформы тщательно скрываются.

Совокупность применяемых и перспективных информационных технологий, все шире внедряемых в повседневную жизнь общества, является фактором, оказывающим значимое влияние как на позитивные, так и на негативные общественные характеристики, связанные с терроризмом и экстремизмом.

Использование средств информационного воздействия нашло большой практический интерес у террористических организаций. Оно позволяет им без серьезных материальных затрат влиять на определенную аудиторию, осуществлять практически акции, влекущие за собой громкий общественный резонанс.

Информационно-психологическое (информационное) воздействие (ИПВ или ИВ) явно или скрыто проводится целенаправленно для изменения поведения объекта воздействия в сфере психологических структур сознания и подсознания, трансформации эмоциональных состояний, стимулирования определенных типов реагирования. Каналами для ИВ являются непосредственное общение, ис-

¹ © Минаев В. А., 2020.

² © Федорович В. Ю., 2020.

пользование СС, средств массовой информации (СМИ), которые реализуются в различных форматах (печатные, радио- и телевидение, изобразительные).

Кратко проанализируем состояние общественного (массового) сознания как пространства для осуществления ИВ на поведение социальных групп и как определяющего создание и продвижение информационно-коммуникативных технологий реализации позитивных и негативных ИВ. Исследования в этой области являются междисциплинарными и ведутся философами, психологами, педагогами, культурологами, социологами, политологами, экономистами, юристами, специалистами в области математического моделирования.

Массовое сознание формируется через понимание людьми социальных условий их бытия и усвоения различных сведений через СМИ, социальные и политические коммуникации, пронизывая при этом все сферы жизни.

Исходя из сказанного, определим *массовое сознание* как особую форму группового и общественного сознания с присущим ему внутренним противоречием. Противоречие может быть стабилизирующим или креативным фактором в жизни общества, а может усиливать парадоксы общества и доводить их до кризиса. Консервативным элементом массового сознания является феномен «сопротивления среды» социальным преобразованиям, а также «радикализм массовых настроений», характеризующийся склонностью к неповиновению и революционными изменениями существующего порядка.

Среди видов негативного ИВ выделяются:

- фальсификация (подтасовка) и дезинформация;
- «зомбирование» или целевое программирование на выполнение тех или иных, в том числе – негативных, действий;
- причинение вреда жизни и здоровью;
- астротерфинг – намеренное централизованное манипулирование общественным мнением в сети Интернет с целью дезинформации, искажения статистических сведений и злоупотребления общественным мнением;
- троллинг – размещение провокационных сообщений в целях склонения пользователей к дискуссии определенного направления или создания конфликтной ситуации.

Выделяются пять основных перспективных направлений в моделировании распространения негативных ИВ на массовое сознание и противодействия им:

- традиционные статистические модели (корреляционные, регрессионные, факторные, дискриминантные и т. п.) [2];
- модели, развиваемые в рамках теории игр [3];
- модели, основанные на использовании нейросетей [4];
- модели клеточных автоматов [5];
- динамические модели диффузии инноваций [6].

Каждый тип моделей имеет свои преимущества и недостатки при решении конкретных задач, возникающих при исследовании ИВ.

Аппаратно-программной платформой для реализации системно-динамических моделей ИВ и ИПД выступала современная система имитационного моделирования AnyLogic, позволяющая:

- «проигрывать» любое количество противоборствующих идей;
- визуально наблюдать динамику всех исследуемых переменных, отражающих основные характеристики процессов ИВ на социальные группы;
- изменять значения параметров во время процесса имитации, тем самым выявляя степень их влияния на отслеживаемые переменные;
- проводить различные виды имитационных экспериментов.

С помощью разработанных моделей в социуме отслеживалась динамика таких основных переменных, которые описывали количество лиц:

- подверженных ИВ;
- находящихся в латентной стадии ИВ;
- принявших идею ИВ;
- отказавшихся от идеи ИВ.

Основной особенностью комплексной системно-динамической модели информационного противоборства, логически и структурно развивающей модель ИВ, является учет замещения идеи ИВ на идею противоборствующей стороны.

Проанализируем результаты некоторых экспериментов, проведенных в работе [7] по изучению влияния характеристик модели на динамику процессов ИВ и противоборства в СС. Именно эти результаты использованы для изучения особенностей распространения информационных воздействий в социальных сетях различных регионов.

На рис. 1 показана скорость принятия информационного воздействия в зависимости от вероятности коммуникации на тему, вложенную в контент ИВ (параметр p). С её ростом скорость принятия ИВ возрастает с ярко выраженным пиком, смещающимся к началу исследуемого интервала времени.

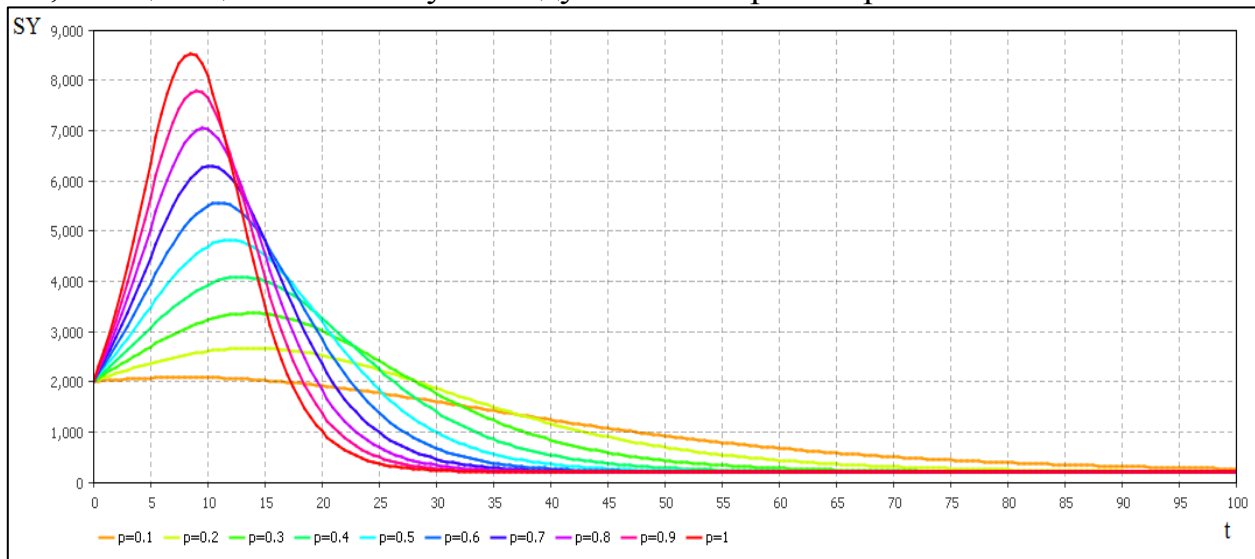


Рис. 1. Скорость принятия идеи информационного воздействия в зависимости от вероятности коммуникации на тему его содержания (параметр p)

Приведем динамику количества лиц, принявших и распространяющих идею ИВ (Y), в зависимости от длительности латентного периода (f) (рис. 2).

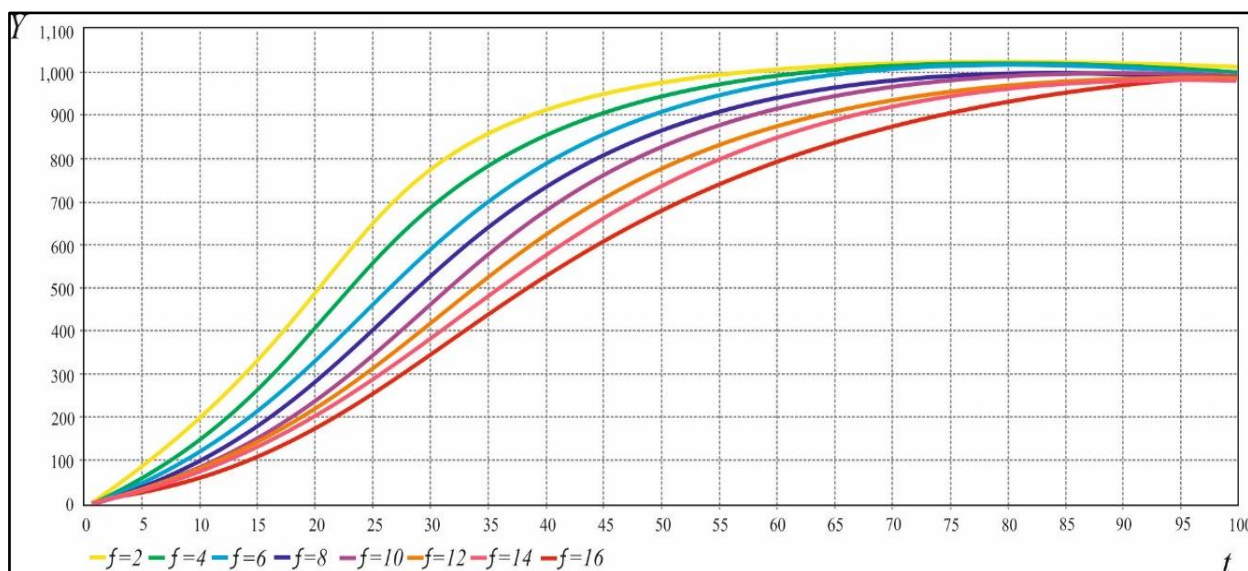


Рис. 2. Динамика количества лиц, принявших и распространяющих идею ИВ, в зависимости от длительности латентного периода (параметр f)

Из рис. 2 следует – чем более длителен латентный период (когда индивид принял идею ИВ, но не является ее распространителем), тем более растянут во времени переход к состоянию «зараженный и распространяющий ИВ».

В целях апробации моделей ИВ также исследованы статистические данные по сообществу ВКонтакте, созданному в марте 2017 г. командой известного оппозиционера для ведения агитационной кампании с призывом к политическим митингам экстремистского характера. Из оценки статистических данных следует вывод, что за исследуемый период имели место два информационных вброса. Они произошли 16 и 24 марта в российских городах и характеризовались резким всплеском количества вступивших в сообщества.

В имитационной среде моделирования *AnyLogic* оценены значения параметров системно-динамической модели: $t \in [0; 7]$, $a = 0,568$; $b = 0,179$; $t \in (7; 14)$, $a = 0,464$; $b = 0,016$. Результаты моделирования приведены на рис. 3.

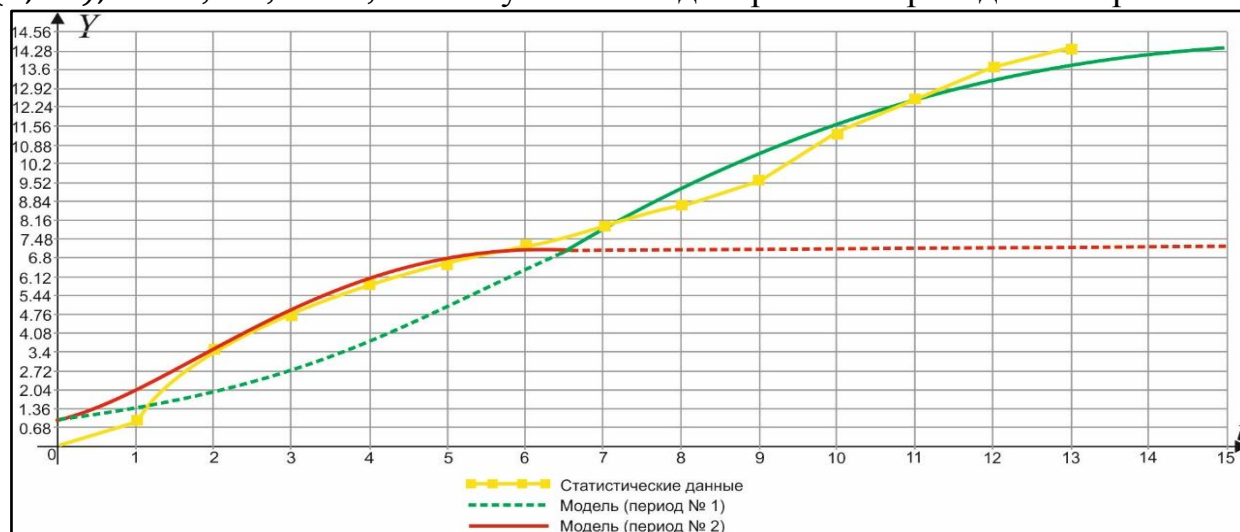


Рис. 3. Распространение ИВ с экстремистскими призывами в СС Санкт-Петербурга (квадратами обозначены реальные статистические данные, сплошной линией – результаты моделирования)

Приведем результаты имитационного эксперимента [8], где исследуется зависимость скорости принятия какого-либо воздействия (экстремистское не является здесь исключением) пользователями сети от количества социальных контактов лица, уже увлеченного ею (рис. 4).

Из анализа рис. 4 следует, что, например, при двух контактах в день ($n=2$) скорость принятия экстремистской идеи достигнет своего максимума через 48 дней, а уже при восьми ($n=8$) – через 12 дней.

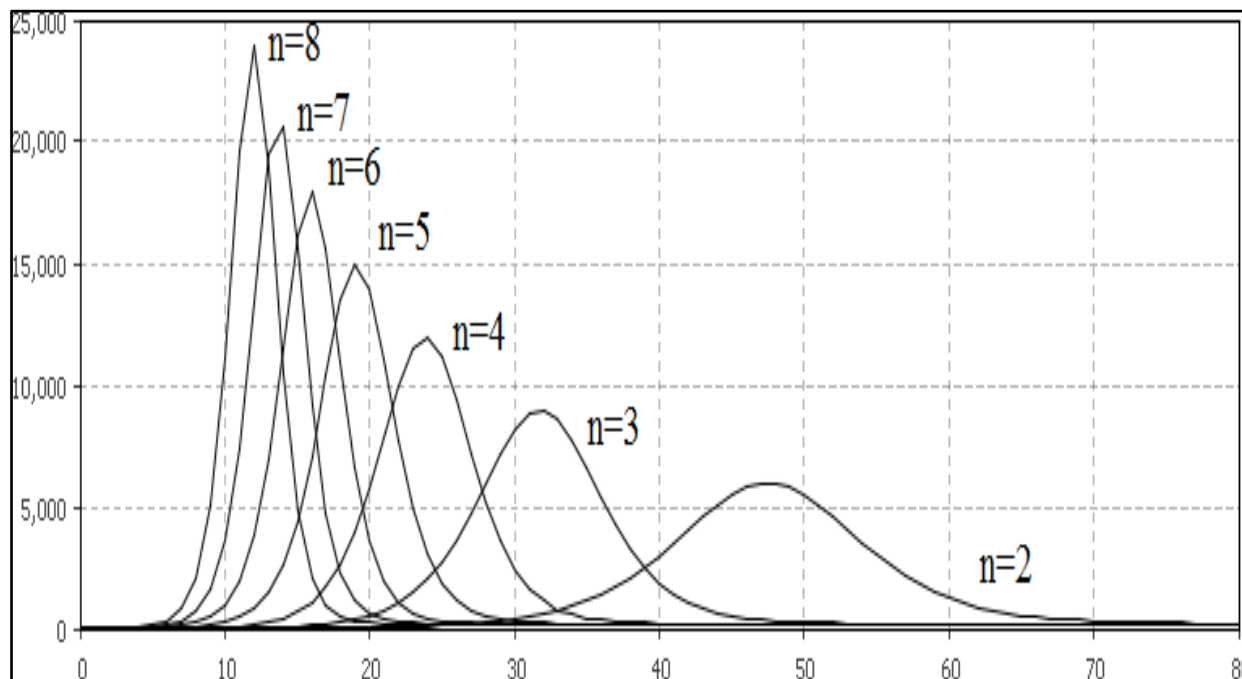


Рис. 4. Зависимость скорости принятия информационного воздействия от частоты социальных контактов

Целенаправленное использование СС на порядки увеличивает указанные показатели, доводя их до нескольких часов. Подобную зависимость экстремистские структуры активно используют в своей вербовочной деятельности.

В качестве перспективных направлений разработки и применения современных математических моделей выступают:

- подготовка планов по предупреждению и реагированию на массовые противозаконные акции, когда важным элементом является получение разведывательных сведений в социальных сетях об их организации, подготовке и проведении. Это могут быть данные о времени, предполагаемых силах и средствах участников акций, мотивах, уровне и широте размаха, ожидаемых последствиях, перспективах продолжения. Могут применяться как системно-динамические модели развития массовых явлений, так и агентные подходы информационного «заражения», базирующиеся на моделях клеточных автоматов;

- другой областью, где необходим сбор разведывательной, а также доказательственной информации, является проведение мониторинга социальных сетей в целях организации борьбы с незаконным оборотом наркотиков, как правило, связанным с экстремальными проявлениями в обществе [9], а также другие методы компьютерной разведки, основные из которых описаны в работе [10]. Здесь также применимы и системно-динамические, и модели клеточных автоматов;

– выявления негативного контента в социальных сетях, а также информации о лидерах и структуре террористических и экстремистских группировок.

Соответствующие модели, отражающие два последних направления, дают возможность эффективно проводить:

- деанонимизацию пользователей или акторов в социальных сетях;
- оценку дестабилизирующих воздействий на террористическую организацию на основе приложений теории безмасштабных сетей;
- изучение сложных динамических структур с помощью «следающей системы» на основе нейронной сети;
- выявление значимости внешних деструктивных воздействий на СС на основе иммунных сетей.

Рассмотренные подходы к моделированию явления дают потенциально новые возможности для аналитической деятельности организаций, активно занимающихся молодежной агрессией. Развитие моделей в данном направлении связано с созданием автоматизированного метода выявления по текстам сообщений демографических атрибутов пользователей сетей. Программная система должна поддерживать основные мировые языки: английский, испанский, итальянский, китайский, корейский, немецкий, португальский, русский, французский.

Мониторинг сложных информационных сообщений связан с оценкой и анализом информационных сообщений в СС, которые содержат разнообразные по объему и значимости сведения деструктивной направленности.

Подобная задача является весьма сложной по многим аспектам. Отметим только правовой и программно-технологический аспекты, сказывающиеся на возможностях использования при моделировании.

Разведывательный характер проводимых действий обязывает соблюдать требования законности и регламентируемой технологичности.

Охарактеризуем *программно-технологический аспект* мониторинга деструктивного информационного контента СС. Приближение моделей анализа контента к реальным процессам в СС должно учитывать значительное количество нюансов, подходов, особенностей проработки, ограничений, несоответствий желаемым параметрам и иного.

Приведем краткий обзор методов и моделей программной обработки контента на естественных языках.

Общий поисковый алгоритм выглядит так:

- выявление «подозрительных» публикаций;
- анализ их содержания;
- определение эмоциональных особенностей и тональности текста;
- фильтрация информации в целях последующего поиска (например, выявление авторства);
- принятие мер по блокировке или уничтожению деструктивных сообщений.

Наиболее заметными возможностями в решении обозначенной задачи обладают компьютерные методы *обработки естественного языка* (NLP – *Nature Language Processing*), объединяющие в себе искусственный интеллект и математическую лингвистику.

Дадим характеристику подходам компьютерной лингвистики в выполнении модулей автоматического реферирования, минимизации неоднозначностей и ошибок определения лексического смысла. В числе таких подходов значатся самостоятельные виды анализа текстов: морфологический, синтаксический, семантический. Поясним их понятия и варианты программной реализации.

Морфологический анализ – это анализ слов естественных языков, их значимой части и морфологических признаков. Такой анализ выступает предварительным этапом обработки текстов и решает задачи:

- *токенизации* (выделение единиц текста) – распознавания слов, знаков препинания, чисел, формул, таблиц и т. д.;
- *лемматизации* – определения канонической формы слова;
- определения грамматических характеристик (часть речи, падеж и т. д.).

Основными методами морфологического анализа считаются: применение словарей; использование системы правил; статистические методы (на базе машинного обучения).

Синтаксический анализ (*парсинг*) представляет собой автоматическое распознавание структуры любых текстовых данных, предложений. Он расширяет возможности предварительного морфологического анализа. Основными подходами здесь являются грамматика зависимостей и грамматика непосредственных составляющих. В качестве вариантов реализаций можно назвать следующие программные средства:

- синтаксический модуль AOT;
- Stanford NLP;
- NLTK – пакет библиотек и программ для символьной и статистической обработки естественного языка, написанных на языке программирования Python. Парсер является составной частью пакета.

Семантический анализ является самой сложной задачей NLP. На него возлагается формальное представление смысла текста в целях его последующей обработки. Завершающими в алгоритме автоматической обработки текста являются процедуры анализа тональности текста, определения авторства и жанра.

Анализ тональности текста обеспечивает субъективную оценку информации, возможное определение жанра и авторства текста. Объектом тональности выступает определенный набор слов, отражающий оценку информации.

Здесь лидируют методы машинного обучения. Интересным в этом плане является анализатор тональности Eureka Engine, объединяющий словари и методы машинного обучения. Другим примером является анализатор тональности SentiStrength.

Определение авторского стиля также использует анализ тональности. Стилистическими признаками авторства в тексте являются: длина слов и предложений; редкие и специфические слова; пунктуация; статистическая оценка частотности словоформ; буквенные n -граммы.

Примерами программ – текстовых анализаторов с наличием определения авторства текста выступают:

- DKPro Statistics компании Ubiquitous Knowledge Processing Lab;

- Figure Eight той же компании;
- PubMed от NCBI (медицинское направление);
- Pilot Study от Zenodo;
- Authorship Attribution от NeoNeuro – отечественная разработка.

Таким образом, существует достаточное число программ, основывающихся на различных моделях, для решения задач выявления деструктивного информационного контента. Однако далеко не все задачи здесь решены. Существует необходимость в разработке специализированных методов NLP для решения задач мониторинга контента, связанного с терроризмом и экстремизмом.

В работе [11] предложен алгоритм *мониторинга СС*, использующий функционал полнотекстового поиска. Среди методов мониторинга выделяется две основных разновидности, ориентированные на решение задач органов правопорядка, государственной власти и местного самоуправления: обнаружение и предотвращение информационных атак, выявление информационных сообществ, занимающихся деструктивным информационным обменом (террористического, экстремистского и иного подобного вида). Авторы разработки обращаются к открытым версиям программных продуктов: М-13, Медиалогия-ПРИЗМА, Медиалогия-Инцидент, Крибрум.

В области мониторинга деструктивного контента перспективным направлением представляются *методы тематического моделирования* [12], которые традиционно применяются в машинном обучении и NLP. Они обеспечивают выявление основных тематик из массива документов, скрытых семантических структур, анализ новостных потоков и представление информации в СС.

В работе [13] проведены изыскания в области *алгоритмов поиска и классификации деструктивного контента* в СС, которая необходима при создании инструментов автоматического поиска деструктивного контента, где эксперты отсутствуют вообще или их участие крайне ограничено. Классификатор деструктивного контента включает такие явления и события как разжигание этнической и религиозной ненависти; пропаганда экстремизма, наркотиков, сепаратизма, суицида; отрицание традиционных ценностей; оправдание и популяризация террористических организаций; подрыв суверенитета государства и политической стабильности.

В работах [14, 15] предлагаются практически реализованные алгоритмы, позволяющие составлять частотный словарь регионального пользователя сети Интернет, преобразовывать корпуса текстов в упорядоченные списки, определять частотность ключевых слов; анализировать контент на наличие деструктивной направленности.

В работе [16] рассматриваются вопросы, связанные с определением *ареала распространения деструктивного контента* в СС по элементам идентификации пользователей в них. В числе таких элементов: личная информация; семейное положение; политические и религиозные взгляды; количество и состав друзей; фото, видео.

Вопросам *методического и алгоритмического обеспечения оценки деструктивного контента* также посвящена работа [17], в которой проводится анализ видеоконтента и делается попытка определения степени его деструктивности.

Нельзя не отметить интересные работы, связанные с *картографическим подходом к описанию киберпространства* [18], где фигурируют такие информационные объекты, как базы данных информационных уязвимостей, характеристики пользователей СС в форме профилей, различные события в сфере безопасности информации, реализации атак, способы и методы защиты.

При картографическом подходе выделяются исследования в сфере *уязвимостей программного обеспечения* [19]. Работы в этом направлении позволяют оценивать потенциальные угрозы по внедрению деструктивного контента в пользовательские социальные платформы. Требуемый при этом функционал решения задач противодействия базируется на применении комплекса программ: сбор, хранение исходных данных (Neo4j); визуализация, анализ создаваемых карт (Gephi); интерактивный анализ данных карты и нанесение дополнительных меток (PowerBI); реализация 3D-картографирования (WebGL).

В статье [20, 21] подведены итоги использования известных методов анализа знаковой организации текста, оценки его тональности по уровню эмоциональной экспрессивности слов. Авторы сформировали критерии степени деструктивности не только текстового, но и фото-, аудио-, видеоконтента.

Важную составляющую изображения с точки зрения выявления деструктивного контента представляет цвет [22, 23]. Например, черный цвет (разрушительность, подавление, депрессия, пустота); красный – (физическое насилие, нетерпимость, похоть); синий – (идеализм, фанатизм, подчиненность).

У аудиоконтента свои особенности воздействия. Например, воздействие низкочастотного звукового диапазона (близкого по спектру к 20 Гц) приводит к очень сильным проявлениям беспокойства, паники, страха, к нанесению себе физических увечий вплоть до летальных исходов [24]. Выявление подобных негативных воздействий звукового диапазона дает возможность вырабатывать противодействия деструктивному аудиоконтенту.

Наиболее сложной представляется оценка видеоконтента. Она, прежде всего, должна совмещать в себе все подходы для текстового, аудиоконтента и изображений. Кроме того, следует учитывать скорость смены кадров, различные визуальные эффекты.

Принципиальным критерием в любых типах контента выступает наличие тех или иных запрещенных материалов. Их перечень должен сверяться с федеральным списком экстремистских материалов [25].

Итак, реальная задача мониторинга деструктивного информационного контента в СС относится к категории особо сложных для решения. Она характеризуется множеством как известных, так и скрытых параметров, требует применения самых современных алгоритмов, расширения аппаратных платформ и методических принципов для осуществления моделирования. Как подчеркивалось выше, она представляет собой самостоятельный предмет исследований, в то же время тесно увязана с кругом вопросов, обсуждаемых в статье.

Как перспективные из-за своей актуальности для организации эффективного противодействия выделяются следующие направления:

- 1) моделирование распространения в социальных сетях деструктивных воздействий агрессивного характера применительно к молодежной среде;

2) мониторинг сложных информационных сообщений, различающихся по формату контента (текст, фото, видео, аудиозаписи), которые могут содержать разнообразные по объему и значимости сведения террористической, экстремистской и иной криминальной направленности.

Указанные направления пока методически не сформированы и требуют дополнительных исследований. Рассматриваемые в статье подходы, определяющие развитие данных направлений, несут потенциально новые возможности для совершенствования аналитической деятельности различных структур, активно занимающихся проблемами молодежной агрессии и анализа деструктивного контента в социальных сетях.

Библиографический список

1. Социальные сети в России: цифры и тренды [электронный ресурс] // Блог Brand Analytics. – URL: <https://br-analytics.ru/blog/social-media-russia-2019> (дата обращения 12.12.2020).
2. Гмурман, В. Е. Теория вероятностей и математическая статистика : учебное пособие : 10 издание. М. : Высшая школа, 2004. – 479 с.
3. Мазалов, В. В. Математическая теория игр и приложения. СПб. : Лань, 2010. – 446 с.
4. Еремин, Д. М. Искусственные нейронные сети в интеллектуальных системах управления / Д. М. Еремин, И. Б. Гарцев. – М. : МИРЭА, 2004. – 75 с.
5. Аристов, А. О. Теория квазиклеточных сетей : научная монография. – М.: МИСиС, 2014. – 188 с.
6. Минаев, В. А. Как управлять массовым сознанием: современные модели : монография / [В. А. Минаев и др.]. – М.: РосНОУ, 2013. – 200 с.
7. Минаев, В. А. Исследование модели динамики деструктивных информационно-психологических воздействий на массовое сознание // Безопасность информационных технологий. – 2016. – № 4. – С. 52–58.
8. Пидусов, Е. А. Использование специальных знаний и информационных ресурсов при расследовании незаконного оборота наркотических средств и психотропных веществ в сети Интернет : учебно-методическое пособие / [Е. А. Пидусов и др.]. Воронеж: Воронежский институт МВД России, 2018. – 67 с.
9. Компьютерная разведка : учебное пособие / сост. Е. С. Поликарпов. – Краснодар: Краснодарский университет МВД России, 2018. – 198 с.
10. Титов, Н. Г. Методы мониторинга социальных сетей, их развитие и применение в контексте обеспечения их информационной безопасности / [Н. Г. Титов и др.]. // Информация и безопасность. – 2019. – Том 22. – № 3(4). – С. 305–324.
11. Телегин, Е. Н. Методы тематического моделирования, их развитие и применение для контента, циркулирующего в региональных онлайн-сообществах / [Е. Н. Телегин и др.]. // Информация и безопасность. – 2019. – Том 22. – № 3(4). – С. 325–344.
12. Гончаров, А. А. Развитие методов и построение алгоритмов поиска и классификации деструктивного контента, циркулирующего в социальной сети / [А. А. Гончаров и др.]. // Информация и безопасность. – 2019. – Том 22. – № 3(4). – С. 345–360.

13. Гончаров, А. А. Развитие методов и построение алгоритмов поиска и классификации деструктивного контента, циркулирующего в социальной сети / [А. А. Гончаров и др.]. // Информация и безопасность. – 2019. – Т. 22. – № 3(4). – С. 345–360.
14. Злоказов, К. В. Контент-анализ текстов деструктивной направленности / К. В. Злоказов // Политическая лингвистика. – 2015. – № 1. – С. 244–250.
15. Ишков, Д. А. Определение ареала распространения деструктивного контента в социальной сети [Д. А. Ишков и др.]. // Информация и безопасность. – 2019. – Т. 22. – № 3(4). – С. 361–372.
16. Гончаров, А. А. Методическое и алгоритмическое обеспечение оценки деструктивного контента, циркулирующего в социальной сети / [А. А. Гончаров и др.]. // Информация и безопасность. – 2019. – Т. 22. – № 3(4). – С. 373–386.
17. Остапенко, А. Г. Картографический подход к описанию киберпространства в контексте обеспечения безопасности информации и информационной безопасности / А. Г. Остапенко, А. Л. Сердечный // Информация и безопасность. – 2019. – Т. 22. – № 3(4). – С. 387–398.
18. Сердечный, А. Л. Карты источников, содержащих сведения об уязвимости программного обеспечения / [А. Л. Сердечный и др.]. // Информация и безопасность. – 2019. – Т. 22. – № 3(4). – С. 411–422.
19. Москалева, Е. А. Использование и развитие методик оценки тональности контентов социальных сетей в целях обеспечения информационной безопасности пользователей / [Е. А. Москалева и др.]. // Информация и безопасность. – 2019. – Т. 22. – № 3(4). – С. 433–444.
20. Котельников, В. В. Распознавание эмоциональной составляющей в текстах: проблемы и подходы / [В. В. Котельников и др. ; под ред. С. М. Окулова]. – Киров: ВятГГУ, 2012. – 103 с.
21. Воздействие цвета на человека и его психику // Виртуальный фотожурнал «Хулиганствующий элемент» [электронный ресурс]. – URL: <http://photoelement.ru/analysis/color2/color2.html> (дата обращения 12.12.2020).
22. Яньшин, П. В. Введение в психосемантику цвета / П. В. Яньшин. – Самара: СамГПУ, Пиквик-Club, 2000. – 200 с.
23. Воздействие частот на сознание // Mindmachine.ru: приборы для саморазвития [электронный ресурс]. URL: http://www.mindmachine.ru/articles/frequency_consciousness.htm (дата обращения 11.09.2020).
24. Федеральный список экстремистских материалов // Министерство юстиции Российской Федерации [официальный сайт]. – URL: <https://minjust.gov.ru/ru/extremist-materials>. (дата обращения 11.09.2020).

Рыженко А. А.¹,

*доцент кафедры информационных технологий
учебно-научного комплекса автоматизированных
систем и технологий, руководитель направления
подготовки «Информационные технологии
в техносферной безопасности» Академии
Государственной противопожарной службы МЧС России,
кандидат технологических наук, доцент*

МОДЕЛЬ ВЛОЖЕННОЙ ПИРАМИДЫ СИСТЕМЫ УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ ИНФОРМАЦИОННОГО ПРОСТРАНСТВА ГОСКОРПОРАЦИИ

Развитие цифрового пространства за последние шесть лет поражает масштабностью, «безграничными границами», а также насыщением цифровых агентов псевдослучайным интеллектом. Данные научно-практические направления (здесь нет ошибки, так как то, что сейчас внедряется на практике достаточно подробно изложено в научных работах 20-летней давности) сопровождаются повышением доверия со стороны социальной среды к новым «более совершенным» информационным ресурсам, что имеет свои негативные стороны. Например, многие крупные игроки мирового рынка не стесняясь используют обратную сторону цифрового пространства, под позитивом прячут множество негативных моментов. В частности, одним из ведущих игроков является банковская система. То, что сейчас происходит с мировой валютой в цифровой среде – уже давно ни для кого не секрет. Тихое противостояние между признанными лидерами в лице государств, и скрытыми – в лице госкорпораций ведется не первое десятилетие. Но насколько готовы ведущие государства к противостоянию, можно судить двояко: афишируемая сторона постоянно не успевает, согласно скрытой – весь сценарий идет согласно инструкции. В данной статье раскрывается один из примеров такого противостояния в сфере информационного терроризма.

В 2020 г. Российская Федерация приняла существенные поправки к Конституции. Большая часть электората проголосовала «ЗА». Что может скрываться за основными восемью глобальными изменениями – не тема данной статьи. Но факт остается фактом, в среде МЧС России был проведен независимой опрос, результаты поражают. Процент доверия достигает максимальных значений. Но, что было сделано если проголосовали «НЕТ»? Рассмотрим только одну сторону, объясняющую, насколько толково государство подстраховалось от заведомо неверных решений, а также от возможного информационного экстремизма. Самый эффективный способ принудительного ограничения – внесение изменений в основную нормативную базу. Весной 2020 г. в основной ФЗ внесено глобальное изменение, меняющее представление к собственности цифровой информации. Такие понятия как «собственник», «хозяин» или «владелец» исчезли. Осталось только расплывчатое понятие: «обладатель информации» [1, ст. 2]. Т. е., любая информация, попадающая в пространство сети Интернет больше никому не при-

¹ © Рыженко А. А., 2020.

надлежит, все имеют одинаковые права обладателя. Для усиления этого фактора, в другой ФЗ внесено определение «*мобильное приложение*», где недвусмысленно привязывают данное устройство к сети Интернет [2, ст. 2]. Единственный ГОСТ, определяющий термины «*собственник*» и «*владелец*» считается морально устаревшим и не принимается к цифровому пространству [3, прил. А]. Другой ФЗ, где были упомянуты термины «*собственник*», «*владелец*» и «*пользователь*» [4, ст. 2] был аккуратно в 2020 году изменен на [5].

При данных обстоятельствах можно представить, что государство проигрывает информационную войну. Все чаще появляются такие ресурсы, как «*Информационный экстремизм*» [6] или «*Информационный терроризм*» [7] где черный пиар все больше набирает обороты. Но не зря чуть выше зашел разговор о Конституции. Поток информации растет с каждым годом. Если социум в 2008 г. старался еще разобраться, найти истину (согласно данным Росстата), то 10 лет спустя данный показатель опустился ниже критического [8]. Государство приняло решение ограничить права социума и передать права более компетентным органам власти, осознающим всю степень ответственности. При нарастающем влиянии госкорпораций на повседневную и профессиональную деятельность социальной среды данные обстоятельства вполне оправданы.

Возникает другой вопрос: а насколько ведомственные структуры готовы к данным обстоятельствам? Далее будет изложен материал только по одной ветке готовности МЧС России, касающийся цифровой среды.

Можно достаточно смело заявить, что на момент официального заявления Министром МЧС России (декабрь 2019 г.), безопасное цифровое пространство сформировано и укомплектовано. В результате, после качественной проработки, сформировано распоряжение, согласно которому выполняется план дальнейшего развития [9]. Рассмотрим крупноблочно хронологию формирования:

1. Первый модуль – географическая основа МЧС России ЕСИМО – межведомственная информационная система для доступа к ресурсам морских информационных систем и комплексного информационного обеспечения морской деятельности (введена в действие в 2013 г.) [10].

2. Система безопасности переходит на принципиально новый уровень, обеспечивая защиту такого рода информации. Подключается аппаратно-программный комплекс «Безопасный город» (введен в действие в 2014 г.) [11].

3. Подписано соглашение об осуществлении информационного обмена при решении задач предупреждения и ликвидации чрезвычайных ситуаций от 21.08.2015 г. № НТЭК-32-665/15 [12]. На карту нанесены дороги, направления, населенные пункты и прочие объекты, подключенные к общей системе энергоресурсов.

4. В этом же году МЧС России заключен договор на использование систем космического мониторинга на случай ЧС для контроля обстановки. Назначение ПРМ «Астероид» – прогнозирование сценариев катастроф при воздушных, наземных и подводных взрывах, связанных с астероидной и кометной опасностью, прогнозирования обстановки и ППР по защите населения и территорий. Передана система защиты информации при анализе потоковых данных.

5. Следующий год переориентировал глобализацию обобщенной информации на персонифицированную. МЧС России получил полный доступ к ресурсам РОСРЕЕСТР [13]. Использование данного типа ресурсов позволило нанести на карты жилищный фонд. На данном этапе отрицательный момент получил человеческий фактор. Доступ к информации спровоцировал утечки. Естественное следствие – усиление системы безопасности в сторону персонификации. МЧС России получил доступ в этом же году к системе «ДОСЬЕ», объединяющее сотовых операторов.

6. Подключение информации о социальной среде. С одной стороны, МЧС России с 2017 г. предоставляет возможность получить государственные услуги в электронном виде. С другой – получена информация о личных данных социальной среды (локально на случай ЧС) [14].

7. Полнота информации спровоцировала новую волну в аналитической безопасности, подключена система ГосСОПКА [15]. В результате в информационном пространстве систематизировано и успешно функционирует множество взаимосвязанных программных систем и модулей (рис. 1).

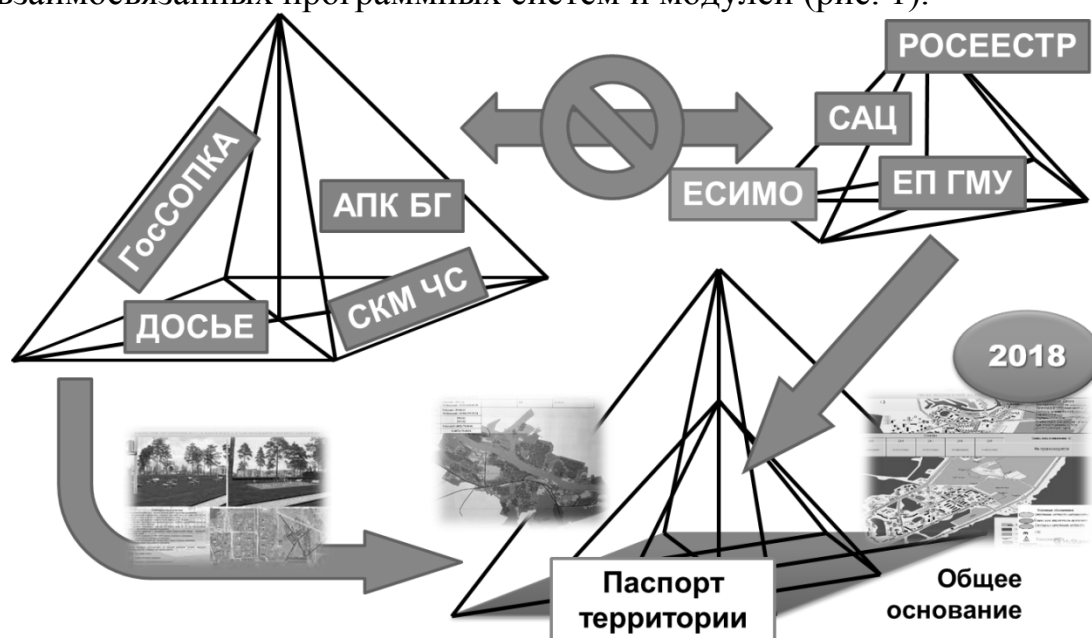


Рис. 1 – Синтез цифровой информации
(расшифровка сокращений не приводится)

Утвержден План мероприятий «дорожная карта» по развитию конкуренции в отраслях экономики Российской Федерации и переходу отдельных сфер естественных монополий из состояния естественной монополии в состояние конкурентного рынка [16]. В рамках программы реализовано единое информационное пространство МЧС России. Ядром системы служит АИУС РСЧС (в 2020 г. трансформировалось в СЭД). Встроен механизм альтернативности принятия управленческих решений, способствующий гибкости системы, а также видоизменению структурных элементов вплоть до полного изменения.

Как было упомянуто ранее, приведен неполный перечень используемых компонентов и нормативных документов. Тем не менее, общее понимание о готовности цифрового пространства МЧС России представлено в необходимом объеме.

Библиографический список

1. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СПС «Консультант-Плюс» – URL: http://www.consultant.ru/document/cons_doc_LAW_61798.
2. Федеральный закон от 2 августа 2019 г. № 259-ФЗ (ред. от 20.07.2020) «О привлечении инвестиций с использованием инвестиционных платформ и о внесении изменений в отдельные законодательные акты Российской Федерации» // СПС «КонсультантПлюс» – URL: http://www.consultant.ru/document/cons_doc_LAW_330652.
3. ГОСТ Р 50922-96 «Защита информации. Основные термины и определения». – Режим доступа: <http://www.e-nigma.ru/stat/gost4>.
4. Федеральный закон от 4 июля 1996 г. № 85-ФЗ «Об участии в международном информационном обмене» (с изменениями и дополнениями) // СПС «Гарант-сервис» – URL: <http://base.garant.ru/135401>.
5. Федеральный закон от 1 апреля 2020 г. № 85-ФЗ «О внесении изменений в ст. 20 Федерального закона “Об особенностях реорганизации федерального государственного унитарного предприятия ‘Почта России’, основах деятельности акционерного общества ‘Почта России’ и о внесении изменений в отдельные законодательные акты Российской Федерации”» // СПС «КонсультантПлюс». – URL: http://www.consultant.ru/document/cons_doc_LAW_349071.
6. Информационный экстремизм: сущность и проявления [электронный ресурс] // СМИ «Обозник». – URL: <http://www.oboznik.ru/?p=61182>.
7. Информационный терроризм // PSYERA [сайт]. – URL: <https://psyera.ru/informacionnyy-terrorizm-1859.htm>.
8. Федеральная служба государственной статистики [официальный сайт]. – URL: <https://rosstat.gov.ru>.
9. Распоряжение МЧС России от 21 октября 2020 г. № 793 «Об утверждении единой технической политики МЧС России в области информационных технологий и информационной безопасности».
10. Постановление Правительства Российской Федерации от 29 декабря 2005 г. № 836 «Об утверждении Положения о ЕСИМО» // Портал единой государственной системы информации об обстановке в Мировом океане». – URL: http://esimo.ru/esimo_static/documents/polojenie.pdf.
11. Распоряжение МЧС России от 3 декабря 2014 г. № 2446-р «Об утверждении Концепции построения и развития аппаратно-программного комплекса «Безопасный город». // Портал МЧС России [официальный сайт]: Главное управление МЧС России по Красноярскому краю. URL: <https://24.mchs.gov.ru/deyatelnost/napravleniya-deyatelnosti/grazhdanskaya-zashchita/1-organizaciya-ekstrennogo-reagirovaniya/1-5-apk-bezopasnyy-gorod>.
12. Соглашение между ФГБУ «САЦ Минэнерго России» и АО «НТЭК» об осуществлении информационного обмена при решении задач предупреждения и ликвидации чрезвычайных ситуаций от 21.08.2015 г. № НТЭК-32-665/15.
13. Приказ МЧС России от 14.06.2016 г. № 323 «Об утверждении административного регламента МЧС России исполнения государственной функции

по осуществлению федерального государственного надзора в области защиты населения и территорий от чрезвычайных ситуаций природного и техногенного характера» // СПС «Гарант-сервис». URL: <http://base.garant.ru/71442320>.

14. Распоряжение МЧС России от 25.07.2017 г. № 366 «О внесении изменений в приложение к распоряжению МЧС России от 19.05.2017 г. № 233».

15. Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

16. Распоряжение Правительства Российской Федерации от 16 августа 2018 г. № 1697-р «Об утверждении плана мероприятий («дорожной карты») по развитию конкуренции в отраслях экономики Российской Федерации и переходу отдельных сфер естественных монополий из состояния естественной монополии в состояние конкурентного рынка на 2018 – 2020 годы».

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;
Андрющенко А. Ю.²,
 врио начальника УВД по Северо-восточному
 административному округу ГУ МВД России
 по г. Москве, полковник полиции

ИНФОРМАЦИОННЫЕ СФЕРЫ КАК ПОЛЯ СРАЖЕНИЙ

Новые грани информационной безопасности связаны с развитием технологий, цифровизацией, искусственным интеллектом, наконец, с распространением систем контроля уже в условиях пандемии. Это требует отступления от представлений об информации как объекте защиты. Более актуально рассматривать информацию как средство контроля, а, главное, как инструмент управления социальными процессами.

Спектр угроз в области информационной безопасности неуклонно смещается в сторону воздействия на сознание людей, сообществ, народов. Мы все чаще видим, как протестные настроения и выступления в разных странах мира переходят в погромы, открытые грабежи, гражданские конфликты, столкновения.

Таким образом, сегодня приоритеты должны отдаваться обеспечению безопасности информационных сфер. Традиционно под такими сферами понимались сферы отношений, связанные непосредственно с производством, обработкой, получением, использованием сведений и данных.

Если подходить к информации как к инструменту воздействия и управления, то к информационным сферам необходимо отнести и семейные отношения, системы образования, культуру, науку, религию. И это только в первом приближении. Сделав шаг вглубь проблемы безопасности информационных сфер, мы сталкиваемся с построением истории, выработкой идеологии, формированием мировоззрения...

В целом, информационные сферы современного общества представляются многомерной и многоуровневой фронтально организованной системой связей и отношений, формирующей массовое сознание и сознание отдельных людей.

Именно в этих сферах сейчас бушуют информационные войны: гибридные, смысловые, психоисторические, идеологические, психодемографические... В этих сферах формируются идеи экстремизма и терроризма.

Концептуальные моменты обеспечения безопасности информационных сфер можно выделить, обратившись к истории вопроса.

В начале Первой мировой войны В. И. Ленин сформулировал лозунг «О превращении войны империалистической в войну гражданскую». Были намечены и конкретные меры: «полный разрыв с политикой национального ми-

¹ © Овчинский А. С., 2020.

² © Андрющенко А. Ю., 2020.

ра», «поддержка массовых протестных выступлений», «война с правительством вплоть до поражения своей страны».

Эти призывы к пролетариату всех воюющих стран преподносились как высшее достижение революционной мысли. По-видимому, так и было. К чему это привело в исторической реальности – отдельная тема.

Мы же обратим внимание на то, что идея превращения столкновений с внешним противником во внутреннее противостояние оказалась весьма продуктивной именно для информационных войн, для организации экстремистских выступлений и подготовки террористических актов.

Казалось бы, в этом нет новизны. В наставлениях древнекитайского военного деятеля Сунь Цзы (IV век до н.э.) можно встретить рекомендации и по стратегии, и по тактике информационных войн, которые не теряют актуальности: «разжигайте ссоры и столкновения среди граждан враждебной вам страны», «обесценивайте традиции ваших врагов», «подрывайте их веру в своих богов», «подстрекайте молодежь против стариков».

Однако, в прокатившихся волнах цветных революций – революция роз, революция тюльпанов, арабская весна, революция достоинства – информационные войны, как правило, воспринимались как внутренние полустихийные социальные конфликты, которые хотя и готовились, и управлялись извне, но решали с переменным успехом вполне определенные геополитические задачи.

Сейчас же становится все более очевидным, что в условиях нарастающего мирового кризиса, экономического, политического, военного противостояния, информационная война предстает практически неизбежным фактором социальной реальности, психологических отношений как на международной арене, так и внутри государств.

При этом экстремистские акции в той или иной сфере методично раскручивают маховики информационной войны, а террористическая активность угрожает переходом в горячую фазу.

И если одна из основных стратегических задач уже в смысловых войнах состоит в том, чтобы преобразовать энергию внешних противоречий в разрушительную энергию внутренних конфликтов в стане противника, то глобальная стратегическая задача обеспечения безопасности информационных сфер – это не допустить гражданскую информационную войну.

Понятие информационной гражданской войны как организованного и управляемого столкновения групп консультативно-технического обеспечения неких сил, действующих внутри страны с целью захвата и удержания власти, встречается в работах И. В. Лягушкина.

Суть явления представляется более тревожной. Гражданская информационная война последовательно охватывает и раскалывает на враждебные лагеря практически все информационные сферы жизни общества: от семейных отношений, образования, культуры, искусства, до экономики, внутренней и внешней политики.

Она отражается в семейных отношениях, когда родители старшего поколения не могут остановить своих подросших детей, выходящих на протестные акции, спланированные и спонсируемые зарубежными центрами.

Гражданскую информационную войну в последние десятилетия в нашей стране можно увидеть в сфере образования. Происходит борьба традиционной для нас «Школы знаний», требующей всеобщего полноценного фундаментального образования и привнесенной извне «Школы компетенций», готовящей будущие поколения к рынку труда, к тому, как зарабатывать и потреблять.

Гражданская война в идеологии то вспыхивает, то затухает. Саму идеологию нужно рассматривать не только как систему взглядов, определяющую отношение к окружающей реальности, а, в первую очередь, как систему идей и установок, которые обосновывают право на ту или иную деятельность, на образ жизни, на образ мыслей.

В борьбе основных мировых идеологий уже в гражданской информационной войне формируются или человек-потребитель, а в перспективе и человек-беспольный, или человек-защитник, патриот своей Родины, или человек-творец – созидатель будущего. Оглядевшись, мы можем оценить, кого в нас и вокруг нас больше: потребителей, защитников или творцов.

Информационная война охватывает и сферы демографии. Это и сексуальные революции, и борьба за права секс-меньшинств, и пропаганда однополых браков. Набирает силу зародившееся в США еще в 70-е годы XX века движение «Чайлдфри» (Childfree) – «свобода от детей», когда дети в современном обществе представляются лишними, ненужными, мешающими добиваться успеха, потреблять, получать от жизни максимум удовольствий. Идеейные корни психодемографической войны были заложены в мальтузианстве, социодарвинизме, теориях превосходства одних народов и рас над другими.

Одним из основных предметов ожесточенных дискуссий сейчас является история. И здесь также реализуется стратегия превратить империалистическую, уже психоисторическую войну в гражданскую в стане противника. Задача психоисторической войны – скрыть истинные причины мировых потрясений, отвести внимание от виновников мировых потрясений, от субъектов глобального управления.

Россия не раз становилась эпицентром этой войны как главный барьер к мировому государству. Основная мишень сегодня – это победа в Великой Отечественной войне. И у нас находится все больше деятелей, которые согласны с западными стратегами в том, что Коммунистическая Россия наравне с Фашистской Германией несет ответственность за начало Второй Мировой войны. В годовщину Нюрнбергского процесса формируется мнение, что надо было бы наряду с гитлеровским, привлечь к ответственности и сталинский режим...

К сожалению, противостояние в вопросах истории для нашего общества становится привычным.

Можно выделить фактологический вектор построения истории – это формирование ресурсов дошедших до нас сведений и свидетельств. Исторические события требуют интерпретации. Это уже концептуальный вектор создания истории. Но интерпретация определяется идеологическим фоном, преследует определенные цели, а главное, отражает позиции авторов.

Позиции часто оказываются по разные стороны не только фронтов психоисторической войны, но и по разные стороны баррикад в гражданской историче-

ской войне, давая повод первоначальным проявлениям экстремизма. «Невинная» фальсификация или даже тенденциозный подбор исторических фактов, не говоря о концептуальном извращении смысла исторических событий, формируют гражданскую позицию, склоняют человека к определенному выбору, действию и поступку.

Так, на выборах своего президента большинство жителей Молдавии отдали голоса Майе Санде, политическая позиция которой имеет антироссийский характер. По мнению западных политологов, молдавский народ «дозревает» до выбора европейского пути развития. В школьных учебниках в Молдове 1941 г. описан как ознаменованный вводом в страну румынских войск для освобождения Бессарабии от Советской власти.

Перед празднованием 75-летия Победы накал психоисторической войны достигал такого уровня, что сам Президент Российской Федерации Владимир Владимирович Путин объяснял мировому сообществу причины начала Второй Мировой войны на основе подлинных архивных документов.

При необходимости отвести угрозы от своей страны следует выводить информационную войну на межгосударственный уровень. Пример тому показывают политики США, объявляя то Россию, то Китай, а иногда и Иран, и Северную Корею «источником мирового зла».

Хотя сегодня кажется, что Америка сама становится жертвой своих теоретических и практических наработок по дестабилизации гражданского мира. Приемы разжигания гражданских информационных войн в других государствах сейчас используются в борьбе внутренних политических сил США.

Мы видели, как в разных штатах полицейские становились на колени перед дебоширами, погромщиками, как с большими почестями хоронили преступника (или, по другим версиям, жертву полицейского произвола), как безжалостно сносили и разрушали величественные монументы, памятники ранее почитаемым историческим деятелем страны.

Что касается научного обеспечения информационных войн, то можно выделить созданный в США в 80-е годы институт Санта-Фе (SFI), который стал широко известен весьма комфортными условиями работы привлекаемых известных ученых из разных стран. Их подкупала и фундаментальная проблематика исследований по нелинейным взаимодействиям, сложным системам, синергетике, фрактальности... В результате была создана довольно фундаментальная научная база в виде теории управляемого хаоса, которая развивалась, наполнялась и продолжает наполняться практикой самых разнообразных информационных войн и «цветных» революций.

Основные рекомендации по хаотизации и реформатированию социальных систем были понятными и действенными. Их эффективность испытали на себе многие страны постперестроечного мира.

Основной удар в 90-е годы приняла на себя наша страна. И последствия «прогрессивных» реформ сказываются до сих пор.

Суть рекомендаций заключалась в «развитии рыночных отношений», «внедрении либеральных ценностей», «проведении демократических выборов», «встраивании в мировую экономику», «опоре на кредиты мировых банков»,

«проведении реформ образования», «создании межсистемных (свободных) средств массовой информации», и наконец, «деидеологизации», то есть лишении общества какой-либо объединяющей идеи.

Сегодня же, например, тревожные вести приходят из Белоруссии. Противостояние продолжается. Под действием интенсивного информационного воздействия из Польши, Литвы, Чехии люди, голосовавшие за А. Г. Лукашенко и называвшие его «Батькой», начинают сомневаться в своем выборе. Позиция России вызывает у них все большее недоверие. На наших глазах разворачивается очередная гражданская информационная война, которая на Украине не раз переходила в горячие фазы.

Угроза гражданской войны существует и в США. Таким образом, рожденная американскими стратегиями теория управляемого хаоса с экстремизмом, терроризмом, гражданским противостоянием и кровавыми столкновениями может воплотиться на практике с соответствующими разрушительными последствиями в стране, которая ее «изобрела».

Возникает вопрос, как нам противостоять социальной деструкции, противодействовать экстремизму и терроризму в информационных сферах?

Мы выслушиваем, осмысливаем, обсуждаем мнения и подходы экспертов, ученых, специалистов, наших коллег. Разные позиции и подходы, безусловно, заслуживают внимания.

Со своей стороны скажу лишь о необходимости постановки и проведения фундаментальных научных исследований и необходимости подготовки соответствующих специалистов. Для этого следует, в первую очередь, углублять представление об информации как инструменте воздействия и управления.

В нашем подходе информация – это не сведения и данные, это не то, что слышит и видит человек, это не сообщения и даже не содержание сообщений, полученных в результате приспособления наших чувств (как говорил еще Норберт Винер). Информация – это непосредственно то, что возникает в сознании человека как реакция на воздействие, и главное, в результате интерпретации поступающих сообщений и сигналов.

Основные вопросы в этой области – как происходит интерпретация? Кто формирует и задает ключи этой интерпретации – наставники, учителя, кумиры, СМИ или социальные сети?

Нужно углублять представления о работе сознания, о том, как происходит его хаотизация или структурирование, как управлять энтропией массового сознания в цифровом мире. И это одно из направлений исследований, раскрывающих функциональное проявление информации (она возникает как функция интерпретации). Данная функция заключается в накоплении потенциалов энергии желаний, стремлений, той социально-психологической энергии, которая требуется для принятий решений, для действий и поступков.

Другое направление исследований – это выявление инструментальных проявлений информации в актуализации энергоинформационных потенциалов и их разрядке.

Принципиальная сложность моделирования, предсказания, контроля заключается в том, что при сигнальных воздействиях небольшого импульса извне бы-

вадет достаточно, чтобы вызвать разрядку огромных потенциалов энергии, запасенной в той или иной системе. Если речь идет об энергии социальных связей и психологических отношений, источником и генератором которой является информация, то здесь важно, где и как формируются ключи актуализации накапливаемых потенциалов и кто в нужное время и в нужном месте дает сигнал к их разрядке, сигнал, приводящий в движение огромные массы людей.

Формирование ключей интерпретации и задание ключей актуализации – это заключительные стадии информационно-психологической операции.

Начинается все с формирования ресурсной базы с экстремизма, то есть с выдавливанием через задающие цели (фильеры) определенных идей, наполняемых, как правило, деструктивными потенциалами.

В моей памяти остался эпизод из школьных лет, когда появился новый молодой учитель истории, и объяснил, что золотой век древней Руси был именно тогда, когда она была раздроблена на отдельные княжества. Именно тогда наиболее интенсивно развивались торговля и ремесла, возводились города, строились храмы, возникло много центров и, главное, они конкурировали. А с образованием централизованного государства развитие замедлилось и приходилось догонять Европу.

Эти и подобные им идеи 60-х годов проросли в 90-е годы распадом Советского Союза. Они остаются в арсенале тех, кто работает на расчленение России.

Следующий этап, наиболее скрытая стадия информационно-психологической операции, заключается в интрузии, т. е. внедрении в массовое сознание тех идей, идеологем, концептов, которые будучи активированы, должны привести систему социальных отношений к требуемому состоянию. Для этого из сформированных ресурсов идей создается информационный фон, поскольку фоновая информация может обходить защитные функции сознания.

Для решений этой задачи привлекается сила искусства. Выполняя коммуникативную, воспитательную, гедонистическую и множество других функций, именно произведения искусства решают сверхзадачу – внелогического, чувственно-эмоционального восприятия и познания того, что было, есть и будет.

Здесь можно бесконечно обсуждать, какие фильмы, сериалы, постановки, передачи вносят свой вклад в информационное противостояние. Нет сомнений, что именно искусство представляет собой ту сферу нашей жизни, где происходят главные сражения информационных войн.

Повышение эффективности управления социальными процессами, противодействия экстремизму и терроризму, информационное противоборство настоятельно требуют адекватной научной базы и высококвалифицированных специалистов по обеспечению безопасности информационных сфер.

Против нас выступают и «полевые армии», и «диверсионные группы», способные проводить и масштабные, и точечные подрывные информационно-психологические акции в наиболее чувствительных сферах жизни общества.

Пора и нам начать готовить специалистов не столько по защите информации, сколько по обеспечению безопасности информационных сфер.

Лягушкин И. В.¹,

доцент кафедры философии

Московского университета МВД России имени В.Я. Кикотя,

кандидат философских наук полковник полиции

САКРАЛЬНО-ГЕОГРАФИЧЕСКАЯ КАРТА РОССИИ КАК ПОЛЕ ИНФОРМАЦИОННОГО ПРОТИВОБОРСТВА

События 2014–2020 гг. на Украине и 2020 г. в США характеризуются беспрецедентным ростом числа случаев разрушения и свержения памятников, а также вандализма по отношению к ним.

Отечественные и зарубежные исследователи отмечают как всплеск интереса к монументальной пропаганде, так и сведения о кризисе пропаганды как таковой. Вполне возможным представляется даже выдвинуть версию отработки рядом политических акторов новых технологий управления социальными средами. В этом, вероятно, и заключается переход от привычных пропагандистских мероприятий к новому этапу и новому виду информационной войны как составной части политического процесса.

В массовом обществе, основанном на тиражировании образцов поведения, появились институциональные возможности для работы не только с организованными социальными группами, но и с массовыми общностями, в частности, с целевыми аудиториями, роями и даже с толпой. В результате прекрасно зарекомендовавшая себя с шестнадцатого столетия пропаганда к началу девяностых годов XX века окончательно исчерпала свой мобилизационный потенциал.

Причина этого кроется, прежде всего, в ключевых используемых стратегиях. В общем смысле **пропаганда – это технология создания социальных систем с общей памятью**. Основа успешной пропаганды – возникающая у представителя целевой аудитории фасцинация, которая обесценивает существовавшие ранее представления о значимых объектах. Пропаганда также задает универсальный вариант социального позиционирования индивида, выстраивает внешний идеологический контекст, в который индивид вписывается. Это требует непрерывной работы и постоянного целенаправленного информационного сопровождения, значимых информационных поводов. Пропаганда перестала работать с прежней эффективностью. Она осталась как фон и как элемент информационной инфраструктуры.

Информационная война же построена на стратегии резонанса, который запускает самовоспроизводящееся информационное оружие. Образно выражаясь, оно само себя чистит, смазывает, перезаряжает, продает, навязывает, рекламирует и даже выпускает для себя боеприпасы. Каждый индивид, подвергшийся воздействию информационного оружия, переносит его боевую часть и обеспечивает воздействие его поражающих факторов на других индивидов.

Кризис инструментальной пропаганды ярко проявился в росте числа исследований в области смысловых и психологических войн, зримым свидетельством чего стало создание в вооруженных силах ряда стран соединений, частей и под-

¹ © Лягушкин И. В., 2020.

разделений психологических операций (PsyOp). Их во многом успешная деятельность привела к формированию начал принципиально иной стратегии информационного противоборства – стратегии непрямого управления социальными средами, прежде всего – информационными. Стратегия основывается на использовании феномена коллективного бессознательного и его воплощения в мифах, легендах, предрассудках и элементах исторической памяти народа.

Эффективное и успешное противодействие подобного рода стратегии предполагает использование феномена, позволяющего работать с общественным сознанием помимо коллективного бессознательного. Таким явлением, безусловно, является сакральная география. В связи с этим необходимо творческое переосмысление сложившихся представлений о сакральной географии.

Следует признать, что сакральная география в настоящее время может быть рассмотрена как форма общественного сознания, которая отражает представления членов социальных групп о всемирно-историческом значении и политической роли природных и рукотворных объектов, являющихся воплощением величия, красоты и подвига, жизни и смерти героев, а также связи с вечностью.

Сакрально-географические объекты обладают спатальными (пространственными) и темпоральными (временными) характеристиками и значениями.

Наиболее часто в числе сакральных природных объектов России опрашиваемые называли озеро Байкал, а в числе рукотворных – г. Москву. В числе сакрально-географических объектов чаще всего опрашиваемые упоминают московский Кремль и комплекс Красной площади в Москве.

Начиная с 2011 г., США и их союзники по НАТО ведут информационную войну с использованием управления информационными средами в рамках концепции стратегических коммуникаций. Их цель – «убеждение или принуждение целевой аудитории к принятию решений или совершению действий, направленных на создание, сохранение или развитие благоприятных условий для продвижения интересов США[1]». Фактически речь идет об управлении информационными средами других стран.

Под стратегическими коммуникациями американские специалисты понимают тотальную пропаганду (ключевое слово тут – «тотальная») и ещё три ключевых направления – связи с общественностью, народная дипломатия и, собственно, специальные информационные операции.

Последние понятие также претерпело изменения с течением времени. Сейчас под информационной операцией теоретики и практики гибридных войн понимают «интегрированное использование в ходе военных операций всех связанных с информацией возможностей совместно с другими действиями для разрушения, искажения, захвата и влияния на процесс принятия решений противниками или потенциальными противниками при защите своих интересов[2]».

В настоящее время на работу с Россией из числа структур США и НАТО сориентирован Центр превосходства в области стратегических коммуникаций в Риге[3]. Официально его главной задачей является улучшение имиджа блока НАТО. Но специалисты центра работают и над тем, чтобы переубедить граждан других стран, сделать так, чтобы они потеряли свою волю, не хотели защищаться и ненавидели свое государство.

В координации с вышеуказанным Центром работает аналитическая структура East StratCom Task Force[4] в Брюсселе. Аналитики центра уделяют серьезное внимание России. Институциональных структур, подобных центрам стратегических коммуникаций, в России в настоящее время нет.

В этих условиях рано или поздно остро встанет вопрос: что мы можем противопоставить стратегическим коммуникациям? Использовать и далее пропаганду и контрпропаганду – значит обречь себя на поражение в информационной войне. У наших оппонентов несравнимо больше ресурсов, а средства нападения всегда совершенствуются быстрее средств обороны. Необходим асимметричный ответ.

Усилия специалистов упомянутых выше структур фактически направлены на ведение информационной партизанской войны и разжигании информационной гражданской войны в России и ряде других стран. В чем их отличие?

Информационная партизанская война – организованное и управляемое группами консультативно-технологического обеспечения деятельности групп давления, столкновение массовых общностей, проводящих специальные информационные мероприятия в рамках выработанных стратегий проведения специальных информационных операций внутри одной страны с целью развязывания информационной гражданской войны в данной стране.

Информационная гражданская война – организованное и управляемое столкновение групп консультативно-технологического обеспечения деятельности групп давления, действующих внутри одной страны с целью захвата, использования и удержания политической власти в данной стране.

Информационная партизанская война была начата на Украине. В 2015 г. был создан Центр информации и документации НАТО в Киеве и разработана Дорожная карта партнерства в сфере стратегических коммуникаций между НАТО и Украиной. Итогом стала провозглашенная Министром внутренних дел Украины Арсеном Аваковым концепция «информационного спецназа».

На данный момент на Украине активно идет информационная гражданская война, а также развязаны действия по ведению информационной партизанской войны в российском информационном пространстве с целью в перспективе развязать информационную гражданскую войну в России.

Парадоксально, но главные субъекты современной информационной войны – группы аналитического обеспечения деятельности субъектов политического процесса, группы давления. Сами политики считают информационное оружие неконвенциональным, поэтому главные разработки и практическое применение его в основном идут у сервисных, прежде всего аналитических структур. Фактически последние имеют интересы, отличные от интересов обслуживаемых ими групп давления, предпринимателей, организаций и политиков.

Пропаганда очень плохо работает на образованную и подготовленную аудиторию, на скептическую или безразличную аудиторию. Поэтому со времен доктора Йозефа Геббельса пропагандисты интуитивно искали способы взломать эмоциональную защиту. То же самое делают специалисты в области стратегических коммуникаций. Они прежде всего пытаются нарушить целостность референтных групп представителей целевых аудиторий, используя техники управления информационными средами.

Можно вбросить информационный повод: в одном из регионов будет открыт полигон для приема московского мусора. Москва – явный сакрально-географический объект. Следовательно, брошенный в информационное пространство повод обеспечит гарантированный резонанс. Другой пример: периодически в информационное пространство России вбрасывается повод о грядущем закрытии мавзолея В.И. Ленина на Красной площади в Москве. Так специалисты в области информационных войн проводят контрразведку боем, проверяя единство носителей различных идеологий среди представителей народов России.

В этих условиях целенаправленная воспитательная работа с элементами сакральной географии страны позволит удерживать неизблемость границ референтных групп индивидов, нивелируя воздействие поражающих факторов информационного оружия. Минимальную защиту обеспечивают базовые знания о принципах информационных войн. В целом, лучший рецепт – сохранять критичность, оставаться в рамках научного мировоззрения. Помогут простейшие навыки демифологизации, анализа и толкования текстов.

Библиографический список

1. Новосельцев Б. Стратегические коммуникации. Украина в фокусе. // Фонд стратегической культуры [электронное издание]. – URL: <http://www.fondsk.ru/news/2015/09/13/strategicheskie-kommunikacii.-ukraina-v-fokuse-35372.html> (дата обращения 28.12.2020).
2. Information operations // Federation of American Scientists [официальный сайт]. – URL: <https://fas.org/irp/doddir/army/fm34-1/ch7.htm>.
3. NATO Stratcom Centre of Excellence [официальный сайт]. – URL: <https://stratcomcoe.org>.
4. Официальный сайт Евросоюза (An official website of the European Union) – URL: <https://eeas.europa.eu>.

Шевко Н. Р.¹,

*доцент кафедры правовой информатики,
информационного права и естественнонаучных
дисциплин Казанского филиала*

*Российского государственного университета правосудия,
кандидат экономических наук, доцент*

ИНТЕРНЕТ-ТЕХНОЛОГИИ ПРОТИВ ТЕРРОРИЗМА

В разное время средства массовой информации играли и продолжают играть большую роль в жизни общества. Ознакомление с газетами и журналами в той или иной степени раньше как на территории бывшего СССР, так и практически во всем мире позволяли себе многие. Каждый выбирал себе издание по интересам. Особенностью современного мира является внедрение в жизнь практически каждого человека вне зависимости от его национальности, территориального нахождения, профессиональных и творческих интересов нового инструмента средств массовой информации – Интернета во всем многообразии его представления. Сведения во всемирной сети распространяются молниеносно. И ничто им не является помехой – ни местоположение, ни цензура, ни время суток. Причем в молодежной среде новостям из всемирной паутины доверяют гораздо больше, чем каким-либо иным источникам. Поэтому, на наш взгляд, необходимо более серьезно относиться к информации в виртуальном пространстве и использовать это пространство для реализации патриотического воспитания молодежи, как основы закладки фундамента становления культурного и морально-устойчивого гражданина России.

В 2010 г. Интернетом в России пользовались 43,3 млн. человек, в 2015 г. – 78 млн. человек, в 2017 г. – 87 млн. человек, к середине 2018 г. – более 90 млн. человек [4], в 2020 г. – 118 млн. человек (81% россиян). Но фактически эти данные немного занижены. Дело в том, что официально дети не могут на себя зарегистрировать аккаунты. Они пользуются учетными данными старших (братьев, сестер, родственников, друзей или родителей). А просматривают информацию в Интернете (в основном развлекательного характера) даже дети до года, которые никак не могут попасть в эту статистику.

Среднестатистический пользователь-россиянин проводит в Интернете каждый день более 7 часов, т. е. более 40% бодрствования. А сейчас, во время частичной самоизоляции и работе/учебе в дистанционном формате некоторых организаций эти цифры значительно увеличиваются.

По данным исследования [3] «центр тяжести интернета постепенно перемещается на восток. Азиатские приложения и веб-сайты занимают все большую долю по активности пользователей со всего мира.

В частности, в последних рейтингах популярных веб-сайтов стало больше азиатских платформ электронной коммерции. Сервис по сбору статистики с сайтов Alexa ставит китайскую платформу Tmall на третье место в мировом рейтинге веб-сайтов, что на 10 позиций выше, чем главный западный конкурент плат-

¹ © Шевко Н. Р., 2020.

формы Amazon. В топ-20 самых популярных сайтов рейтинга Alexa входят 5 китайских платформ электронной коммерции, 4 из которых принадлежат Alibaba».

Пользователи стали реже доверять различным источникам в Интернете, чаще используют ежемесячные блокировщики рекламы. В среднем 4 из 5 пользователей Интернета в возрасте от 16 до 64 лет регулярно пользуются игровыми интернет-приложениями. Если соотнести эту цифру с мировой численностью интернет-пользователей, то глобальное игровое сообщество составляет более 3,5 млрд. геймеров. Число онлайн-потребителей видеоконтента тоже растет. Их количество достигает 90 % всех интернет-пользователей.

И, как правило, играете ли вы в игры, смотрите ли видео, либо просто читаете новости в ленте, обязательно высвечиваются ролики, причем не всегда позитивного содержания.

Мессенджер Telegram заблокировал 25358 аккаунтов, связанных с запрещенной в России террористической организацией ИГИЛ только в январе 2020 г. Теперь они появляются с завидной регулярностью. За один день их фиксируется порядка одной тысячи.

Массовую блокировку аккаунтов террористической направленности начали в 2016 г. Так, в социальной сети Twitter с середины 2015 г. [1] были заблокированы более 125 тыс. аккаунтов, в которых содержались террористические угрозы или пропаганда терроризма. Причем они особенно активизировались в последние месяцы. Первые пару лет за месяц количество заблокированных страниц редко когда превышало полтора десятка.

Для распространения террористической идеологии используются социальные сети, в Интернете действуют сотни сайтов, которые распространяют идеологию террористов. Дальнейшее развитие межведомственного и международного информационного сотрудничества дало положительные результаты по обнаружению и прекращению действия финансовых источников материального обеспечения терроризма. К сожалению, международные террористические организации пытаются активизировать свою деятельность по рекрутированию новых членов, формированию пособнической базы и дальнейшей популяризации своей идеологии насилия, устрашения населения, межнациональной розни. В 2019 г. по решению органов государственной власти пресечено распространение террористического и экстремистского контента на 50 тыс. страницах в Интернете, заблокирован доступ к 16 тыс. зарубежных ресурсов [2].

В 2020 г. [5] не допущено совершения террористических актов, а на стадии приготовления предотвращено 61 преступление террористической направленности, в том числе 41 теракт. Нейтрализовано 49 бандитов, в том числе 8 главарей, задержаны 36 главарей банд, 162 боевика и 591 пособник, изъято около 600 единиц огнестрельного оружия. С начала года в стране разоблачили 55 законспирированных ячеек международных террористов, не допущен въезд 149 иностранных граждан, причастных к экстремистской и террористической деятельности. Также при взаимодействии с Роскомнадзором и правоохранительными органами удалось ограничить доступ к 66,5 тыс. материалов [5] террористического содержания и пресечь деятельность 110 иностранных граждан, осуществлявших их распространение в Сети. Росфинмониторингом заблокированы финансовые ак-

тивы более 1,2 тыс. лиц, подозреваемых в причастности к террористической деятельности на общую сумму свыше 57 млн. рублей.

Благодаря четким и слаженным действиям правоохранителей, число терактов в России за последние пять лет сократилось в девять раз. Наибольшую значимость принимает организация системного подхода к пресечению и предупреждению популяризации взглядов террористического характера и недопущения создания пособнической базы террористов.

Нельзя недооценивать повсеместное внедрение интернет-технологий в нашу жизнь и увлеченность молодежи гаджетами и медиа-приложениями. Эта мощная медиа-империя может и должна работать на предотвращение негативного влияния пропаганды и рекрутинговой кампании в ряды террористических и экстремистских организаций, на популяризацию патриотического воспитания, укрепление морального устоя подрастающего поколения, нацеленность на созидание и творчество. Наиболее эффективными методами противодействия рекрутированию являются:

- ликвидация компьютерной безграмотности населения (через проведение тематических занятий в образовательных организациях, создания компьютерных курсов при отделах социальной защиты и т. д.);
- повышение информационной безопасности пользователей (в том числе посредством социальной рекламы);
- проведение социальных акций (видеоролики, мероприятия) по патриотическому воспитанию молодежи;
- создание информационных буклетов (в том числе видеорекламы).

Библиографический список

1. Twitter заблокировал более 125 тысяч аккаунтов за пропаганду терроризма [электронный ресурс] // Элвисти (электронные вести). – URL: <http://elvisti.com> (дата обращения: 09.12.2020).
2. В России в 2019 году предотвратили 34 теракта [электронный ресурс] // ТАСС. – URL: <https://tass.ru/proisshestviya/7886151> (дата обращения: 05.12.2020).
3. Вся статистика Интернета на 2020 год – цифры и тренды в мире и в России [электронный ресурс] // Web-Canape – digital-агентство № 1 в Смоленске [официальный сайт]. – URL: <https://www.web-canape.ru/business/internet-2020-globalnaya-statistika-i-trendy>. (дата обращения: 01.12.2020).
4. Интернет в России 2018: главные цифры. [Электронный ресурс] // Безопасный интернет – проект Городского методического центра. – URL: <http://security.mosmetod.ru/> (дата обращения: 01.12.2020).
5. Официальный сайт полномочного представителя Президента Российской Федерации [Электронный ресурс]. – URL: <http://szfo.gov.ru> (дата обращения: 07.12.2020).

Гончар В. В.¹,

заместитель начальника кафедры информационной безопасности учебно-информационного комплекса информационных технологий Московского

университета МВД России имени В.Я. Кикотя, кандидат юридических наук, полковник полиции

Акиньшин И. С.²,

заместитель начальника Московского университета

МВД России имени В.Я. Кикотя по профессиональному обучению, дополнительному и профессиональному образованию, кандидат экономических наук, полковник полиции

ОСОБЕННОСТИ РАССЛЕДОВАНИЯ КИБЕРПРЕСТУПЛЕНИЙ ТЕРРОРИСТИЧЕСКОЙ И ЭКСТРЕМИСТСКОЙ НАПРАВЛЕННОСТИ

В современном мире стремительно растет количество технологий, внедряемых в самые разные сферы жизни государства и общества. Этот процесс параллельно с позитивными последствиями дает почву для совершения различных преступлений, в том числе целенаправленных атак с целью террора или шантажа. Киберпреступники могут взломать системы управления сложным технологическим оборудованием завода, больницы, школы, финансово-кредитного учреждения, создать проблемы в управлении целого региона. «Телефонные террористы» отвлекают значительные ресурсы на проверку массово поступающих ложных сообщений о минировании различных объектов.

Следует отметить, что сегодня сложно разделить обычного киберпреступника, специализирующегося на хищениях с использованием социальной инженерии в личных целях, и кибертеррориста, занимающегося той же деятельностью в целях финансирования будущих террористических актов. С уверенностью можно утверждать лишь то, что одни и другие сегодня хорошо организованы, оснащены и информированы об особенностях законодательства.

Отличительной особенностью рассматриваемой категории преступлений является их межрегиональный характер, что требует значительных временных затрат при подготовке и проведении необходимых проверочных действий на стадии возбуждения уголовного дела. Они совершаются, как правило, технически оснащенными преступными группами, характеризуются постоянно совершенствующимися и усложненными способами подготовки, совершения преступления и сокрытия следов.

Приведем наиболее типичные способы совершения IT преступлений.

1. Хищение денежных средств с расчетных счетов граждан путем направления в банки распоряжений о перечислении денежных средств на счета, подконтрольные преступникам.

¹ © Гончар В. В., 2020.

² © Акиньшин И. С., 2020.

Распоряжение о переводе создается от имени клиента с применением аутентификаторов и электронных средств платежа, полученных различными способами, наиболее актуальным из которых является использование методов социальной инженерии (психологических знаний, умений, приемов) при совершении преступлений. В результате данных действий пострадавшие самостоятельно предоставляют злоумышленникам реквизиты своих банковских карт, конфиденциальную информацию, а также паспортные данные, позволяющие провести подложную идентификацию и совершить хищение денежных средств. При развитии атаки по указанному сценарию в зависимости от конкретной ситуации преступники могут инициировать от имени клиента на сервисе переводов платеж с карты на карту или входят в приложение дистанционного банковского обслуживания под учетной записью клиента и оттуда осуществляют платежи. Данный способ представляет наибольшее распространение и социальную опасность, имеет тенденцию к значительному росту.

2. Совершение преступлений в качестве услуги или *cybercrime-as-a-service*, включающей в себя предоставление в аренду БОТНЕТов (компьютеры, «зараженные» вредоносными компьютерными программами, используемые для обеспечения удаленного доступа и управления ими), активно применяемые при организации и проведении DoS- и DDoS-атак, массовой sms- или email-рассылки вредоносных программ и фишинговых писем.

3. Кражи с расчетного счета, а равно в отношении электронных денежных средств (кражи из электронных кошельков, с банковских счетов физических и юридических лиц) и хищения из банковских устройств самообслуживания с использованием вредоносного программного обеспечения (BlackBox-атаки).

4. Атаки на облачные хранилища данных пользователей, в целях получения доступа к их конфиденциальной информации. Продолжают совершаться взломы электронных почтовых ящиков, учетных записей социальных сетей, в результате чего появляется возможность «кражи цифровой личности» и осуществления под ее видом различных противоправных действий. Кроме того, все чаще фиксируются преступления, связанные со взломом различных компьютерных систем в сфере торговли и услуг с целью получения персональных данных, коммерческой и банковской информации (целевые атаки). В этих же целях работают специализированные колл-центры, под разными предложениями обзванивающие потенциальных жертв, собирающие информацию об их интересах для выработки наиболее реализуемых сценариев хищения у конкретного лица.

Требуют внимания так называемые «дистанционные мошенничества», в том числе совершенные на сайтах бесплатных объявлений (Авито, Юла, Drom и др.). В подавляющем большинстве случаев злоумышленники, используя методы социальной инженерии, становятся владельцами идентификационных данных банковской карты потерпевшего или получают доступ к его личному кабинету мобильных банковских приложений. Указанные действия осуществляются под предлогом перевода средств в счет оплаты товара либо осуществления предоплаты за товар, а также каких-либо услуг по фиктивной доставке товара. Данные преступления получили распространение ввиду простоты совершения и отсутствия необходимости использования сложных технических средств.

Анализ информации, поступившей из территориальных органов предварительного следствия МВД России, выявил следующие типичные проблемы в расследовании IT преступлений.

1. Отсутствие действенного инструментария быстрого получения от кредитных организаций, интернет-провайдеров, операторов связи, социальных сетей и интернет-сервисов информации, имеющей доказательственное значение по уголовным делам (сведений о лице, биллинге, движении денежных средств по лицевым счетам абонентских номеров и др.).

В настоящее время длительность ее получения составляет от 1 до 3 месяцев. В этой связи принимаются меры по совершенствованию механизма взаимодействия следственных органов с оперативными подразделениями, заинтересованными ведомствами и представителями бизнес-сообщества, предусматривающие возможность оперативной блокировки сайтов интернет-пирамид (хайп-проектов), фишинговых сайтов и мошеннических колл-центров, а также номеров мобильных телефонов, с использованием которых осуществляются хищения средств.

Следует положительно оценить опыт взаимодействия СУ МВД России по Белгородской области с ПАО «Сбербанк» в области формирования образцов запросов, по которым банком гарантированно будет представлена информация.

Проблема заключалась в том, что значительное количество уголовных дел приостанавливается производством ввиду неустановления лица, подлежащего привлечению в качестве обвиняемого. Это, в свою очередь, происходит из-за непредоставления сотрудниками банка следователю по запросу полной информации о движении похищенных денежных средств. Обращаем внимание, что сотрудник банка вправе отвечать только на те вопросы, которые ставит следователь в соответствующем запросе. В то же время он зачастую, не обладая полным перечнем фиксируемой банком информации, не знает, что возможно запросить.

В решении данного вопроса принял активное участие Московский университет МВД России имени В.Я. Кикотя, выступивший коммуникационной и научной площадкой, на базе которой сотрудники следственного подразделения и работники департамента кибербезопасности ПАО «Сбербанк» обменялись информацией и совместно разработали образцы необходимых запросов.

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.

Следует отметить, что проблема идентификации преступников, использующих программы-анонимайзеры, в настоящее время одна из наиболее актуальных. Ее разрешение видится в комплексе законодательных, технических, организационных и научных мер.

Определенные успехи в расследовании преступлений, связанных с деанонимизацией правонарушителей, достигнуты в ГУ МВД России по г. Москве, где активно исследуется информация, содержащаяся в cookie-файлах, важной особенностью которых является их неизменность. Мошенник может менять свой IP-адрес через VPN, проходить регистрацию с разных абонентских номеров, но ад-

министраторы сайта все равно «поймут», что все это время к нему подключается один и тот же пользователь, т. е. используется браузер одного и того же персонального компьютера. Например, преступник регулярно размещает на сайте бесплатные объявления мошеннического характера, при этом перед входом на сайт подключается к VPN, чтобы его реальный IP-адрес оставался неизвестным. В этой связи следователям рекомендовано при формировании запроса администраторам сайта о предоставлении информации о лице, разместившем объявление, в обязательном порядке в нем истребовать информацию об анализе cookie-файлов данного лица с целью установления всех объявлений, которые размещались с браузера его персонального компьютера, а также информацию обо всех IP-адресах, использованных для посещения сайта.

Таким образом, изначально имея информацию лишь по одному объявлению мошенника, возможно получить сведения по всем объявлениям, размещенным указанным лицом. Целесообразно провести анализ всех объявлений мошенника с целью определения реальных, размещенных с данного персонального компьютера, с указанием личных IP-адресов и личного абонентского номера. Эти объявления мог разместить сам преступник до того, как начал заниматься мошенничеством, или же один из членов семьи, воспользовавшись его компьютером, тем самым раскрыв реальные персональные данные мошенника.

Неопределенность при квалификации хищений по п. «г» ч. 3 ст. 158 УК РФ и п. «в» ч. 3 ст. 159.6 УК РФ. Несмотря на разъяснения, приведенные в постановлении Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате», в данных нормах не учитывается конкретный способ хищения денежных средств с банковских счетов, что вызывает различия в трактовке со стороны следствия, органов прокуратуры и суда. При введении упомянутых норм законодателем не решен вопрос о сумме причиненного ущерба, что порождает спор следствия и органов прокуратуры о применении ч. 2 ст. 14 УК РФ, в части малозначительности деяния при хищении на сумму менее 2500 руб. Возникает необходимость в дополнительном разъяснении порядка определения места совершения подобных преступлений и момента их окончания.

Кроме того, в текущем году ожидается принятие постановления Пленума Верховного Суда Российской Федерации о внесении изменений в постановления пленумов Верховного Суда Российской Федерации от 27 декабря 2002 г. № 29 «О судебной практике по делам о краже, грабеже и разбое» и от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате», в котором планируется разъяснение имеющихся спорных моментов. Недостаточная компьютерная грамотность населения. Руководителям следственных подразделений поручено обеспечить принятие действенных мер, направленных на совершенствование методов информирования населения, в том числе с привлечением федеральных и региональных СМИ, социальных медиа о способах совершения IT-преступлений, методах защиты, а также алгоритме действий пострадавшего. Они предупреждены о недопустимости формального подхода к направлению представлений в порядке ст. 158 УПК РФ.

В целях профилактики преступлений, связанных с использованием IT-технологий, в МВД по Чеченской Республике разработаны памятки «Осторожно, телефонные мошенничества!», «Внимание, мошенники!» и «Владельцам банковских пластиковых карт!», которые изготовлены полиграфическим способом и направлены во все территориальные подразделения республики и в наиболее посещаемые населением учреждения региона для размещения на информационных стендах, в местах, удобных для ознакомления граждан. Подготовлены и распечатаны в типографии листовки, несущие ту же информацию, которые переданы сотрудникам (ОУП, ПДН и ОУР) для использования в практической деятельности при организации профилактической работы с населением.

Возмещение имущественного вреда, причиненного преступлениями, совершенными в сфере IT-технологий.

В настоящее время действующим законодательством не урегулированы процедура и порядок взыскания денежных средств, арестованных на расчетных счетах, на которые потерпевшие перечислили денежные средства, когда подозреваемый (обвиняемый) не открывал указанный счет в банковском учреждении, либо его местонахождение не установлено. Арест денежных средств является эффективной мерой только по уголовным делам о раскрытых преступлениях.

Касаемо остальных случаев, в частности, ПАО «Сбербанк» дает разъяснение, что наложение ареста на безналичные денежные средства не влечет за собой переход права собственности иным лицам, носит временный характер и распоряжение ими возможно только по решению суда. Такие денежные средства не могут быть признаны вещественными доказательствами, поскольку они в соответствии с позицией Конституционного Суда Российской Федерации представляют только обязательное требование к банку.

Разрешение данной проблемы требует законодательного урегулирования.

Не в полной мере сформированы специализированные базы данных, например, существует единая база данных «Дистанционное мошенничество», где аккумулируется информация о зарегистрированных IT-преступлениях и устройствах, с помощью которых осуществляются хищения денежных средств.

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

Для эффективного расследования IT-преступлений всегда необходимы специальные познания в направлениях, не связанных с обычной деятельностью специалистов (экспертов). К таким познаниям относятся: устройство и организация систем мобильной связи и дистанционного банковского обслуживания, программирование на малораспространенных языках и т. д. Из-за быстрого развития технологий соответствующие образцы компьютерной техники, применяемой в экспертно-криминалистической деятельности, и знания специалистов (экспер-

тов) достаточно быстро устаревают. В этой связи необходимо постоянное обновление экспертного оборудования, программного обеспечения и знаний соответствующих специалистов.

Отдельного внимания заслуживают вопросы организации взаимодействия следователей с представителями организаций и правоохранительных органов иностранных государств.

Анализ практики свидетельствует о необходимости перед направлением запроса о правовой помощи принимать меры к обеспечению сохранения зарубежным поставщиком информационных услуг интересующих следствие данных, поскольку сроки их хранения существенно различаются в различных странах и у различных провайдеров. В противном случае, инициаторы запросов о правовой помощи спустя продолжительное время получают ответы об отсутствии запрашиваемых данных, что ведет к расходованию ресурсов следствия и ресурсов иностранных партнеров на заведомо невыполнимые действия.

Следственные подразделения должны учитывать, что соответствующий запрос о сохранении данных может направляться по одному или одновременно нескольким каналам:

- непосредственно иностранному провайдеру, в частности, оказывающему услуги на территории Российской Федерации, если в официально опубликованных разъяснениях своей политики он декларирует возможность своих прямых сношений с иностранными правоохранительными и судебными органами, в том числе поддерживает русскоязычный портал для соответствующих обращений в электронной форме;

- по каналам правоохранительного (полицейского) сотрудничества: коммуникационной сети Интерпола, другим подобным сетям; непосредственно в адрес иностранного правоохранительного органа на основании международных договоров Российской Федерации, межведомственных соглашений или на основе принципа взаимности;

- офицерам связи полиции и иных правоохранительных органов, аккредитованным при посольстве или консульском учреждении соответствующего иностранного государства в России.

В дальнейшем, при направлении запросов о предоставлении упомянутых видов электронных доказательств в отношении состоявшихся сообщений, в данных запросах об оказании правовой помощи или правоохранительного содействия следует делать ссылку на осуществленное сохранение, по возможности с приведением сообщенных провайдером идентификационного номера, кода или иных реквизитов сохраненного материала.

Кроме того, необходимо отметить, что успешность расследования во многом зависит от организации взаимодействий следователя с сотрудниками оперативных подразделений. Сложившаяся практика показала, что наибольший успех при раскрытии и расследовании преступлений указанного вида достигается именно при активном оперативно-разыском сопровождении, суть которого заключается в комплексном использовании методов оперативно-разыскной деятельности, направленных на изобличение лица, совершившего преступление, и документирование его преступной деятельности.

Борзунов К. К.¹,

*доцент кафедры информационной безопасности
учебно-научного комплекса информационных технологий
Московского университета МВД России имени В.Я. Кикотя,
кандидат технических наук, старший научный сотрудник;*

Лопатин П. Д.²,

*старший оперуполномоченный отдела уголовного розыска
УВД по Северо-восточному административному округу
ГУ МВД России по г. Москве, майор полиции*

КИБЕРРАЗВЕДКА В ВЫЯВЛЕНИИ ТЕРРОРИСТИЧЕСКИХ И ЭКСТРЕМИСТСКИХ УГРОЗ

Технологическое развитие коммуникаций в виде компьютерных сетей отдельных университетов и научных центров, в последующем отдельных стран и континентов, в итоге их межконтинентальное объединение породило глобальную сеть. На базе этой сети первоначальная практика передачи данных между отдельными компьютерами университетов и научных центров дала мощнейший импульс развитию обмена информацией на уровне государственных структур, на уровне производственных комплексов, коммерческих и финансовых структур и иных организаций и учреждений. Практика активного обмена данными, в свою очередь, привела к возникновению систем управления в самых разнообразных сферах деятельности – государственной, экономической, финансовой, социальной и прочих.

Параллельно этому возникала практика информационных контактов отдельных пользователей в сети и далее все более обширное удовлетворение информационных потребностей населения стран и континентов. Возникли и получили глобальное распространение различные «социальные сети».

Следует отметить, что уже на ранних этапах интерес к развитию и применению компьютерных сетей со стороны ученых, преподавателей, учителей перерос в явление планетарного масштаба, когда все поголовно увлеклись освоением появившегося неизвестного, невиданного ранее сетевого пространства, которое манило и притягивало миллионы людей. Не оставались в стороне и представители криминального мира, которые с таким же порывом и энтузиазмом, как и все остальные, осваивали сети, но в своих корыстных интересах.

Глобальная виртуальная сеть, возникшая на планете, представляет собой множество разнообразных по конфигурации, размеру и типу подсетей, объединенных между собой случайным образом многочисленным сетевым оборудованием. Лишь в последние одно-два десятилетия можно говорить о каком-либо плановом развитии сетей на территории отдельных стран. На определенном этапе развития сети появились международные стандарты, позволяющие использовать методологию взаимодействия открытых систем (ВОС), которая стала основой регламента обращения друг к другу пользователей сети, установления связи

¹ © Борзунов К. К., 2020.

² © Лопатин П. Д., 2020.

между компьютерами в сети, передачи данных с применением общих коммуникаций. На базе ВОС были созданы протоколы взаимодействия компьютеров и передачи данных, которые позволяют «единообразно» учитывать разнородность сетевого и компьютерного оборудования, программного системного и прикладного обеспечения средств вычислительной техники и сетевых устройств.

Около десяти-двадцати лет программное обеспечение не имело аналогов «компьютерных вирусов». Фактически появление их произошло в 1970-е гг., были описаны прообразы вирусных и антивирусных программ – Virus и Vaccine.

Около двадцати-тридцати лет компьютерные сети не были подвержены угрозам, аналоги которых теперь существуют – «сетевые и вирусные атаки». Фактически первые угрозы в сети появились в 1980-е гг. Одна из самых первых угроз в сети встретила 13 мая 1988 г., когда ряд высших учебных заведений и компаний нескольких стран мира подвергся атаке вируса Jerusalem, уничтожавшего файлы при их запуске. В этот же день сообщения о заражении компьютеров поступали из стран Европы, Америки и Ближнего Востока.

Формирование сети длительное время шло без каких-либо средств защиты с точки зрения современных представлений о безопасности информации (информационных ресурсов) и передачи данных в коммуникационных системах.

Появившиеся угрозы в 1990-е гг. в практике эксплуатации сети Интернет дали импульс поиску инженерно-технических решений обеспечения безопасности информации (информационных ресурсов), установления связей между абонентами, передачи данных в сети.

Это привело к разработке и применению методов и средств *защиты конфиденциальных данных*. Однако в то же самое время криминальные структуры развивали и стали активно применять методы и средства *реализации нелегальных товаров и услуг*. А также получила импульс развития «псевдодемократия» – «свобода слова» и *обход цензуры*.

Этим в полной мере воспользовались экстремисты и террористы, деятельность которых как вид современной организованной преступности характеризуется чрезвычайно опасными для населения, общества и государства интрузивно-деструктивно-мимикрийными свойствами.

Стремительное развитие сетевого, виртуального пространства порождало неизвестные и невиданные ранее проблемы, риски, угрозы. Приходило осознание того, что не может быть абсолютно открытого и доступного виртуального пространства, необходимо разграничить доступ к информационным ресурсам, обеспечить защиту информации ограниченного доступа, внедрить в практику технологии защищенного и скрытого обмена данными и установления каналов связи в сети. Это осознание происходило на самых разных уровнях – как на государственном, общественном, личном, производственном, коммерческом, финансовом, так и на криминальном.

Современное развитие глобальной виртуальной сети таково, что на базе сетевого оборудования и средств вычислительной техники планетарного масштаба одновременно и параллельно реализуются как традиционное и уже хорошо известные, так и новейшие и малоизвестные технологии установления каналов связи между точками (узлами) в сети, организации защищенного и скрытого обмена

данными, управления, в том числе программного, сетевым оборудованием и точками (узлами) сети, программного взаимодействия, воздействия и противодействия информационных процессов средств вычислительной техники, подключенных так или иначе к сети.

Все это порождает многоуровневость, многоплановость и сегментность (фрагментируемость) глобальной сети с точки зрения ее состояния и использования в самых разных целях.

Возникшее глобальное виртуальное пространство в виде сети раскрывает в новом свете как самые лучшие достижения человечества, так и все его пороки.

Отметим еще раз, что современные террористы, экстремисты, торговцы наркотиками и оружием и прочие преступники так же, как и обычные пользователи глобальной сети, в свое время осваивали появляющееся Интернет-пространство, искали и находили возможности использования этого пространства в своих криминальных интересах.

Угрозы террористического и экстремистского характера в глобальной виртуальной сети, в частности на территории Российской Федерации, подразделяются на несколько крупных направлений – таких, как распространение экстремистской и террористической идеологии; вовлечение (вербовка) новых членов в организованные группы боевиков; планирование и организация экстремистских акций и актов терроризма, согласование и синхронизация действий организованных групп террористов и экстремистов; кибератаки на субъекты критической информационной инфраструктуры.

Потенциальные угрозы террористического и экстремистского характера также могут быть связаны с попытками информационно-психологического воздействия на отдельные группы населения, представителей власти и сотрудников правоохранительных органов, а также и при определенных условиях с прямым шантажом и ультиматумом в отношении руководителей отдельной страны (государства).

Нужно выделить необходимость противодействия финансированию терроризма и экстремизма с использованием глобальной сети как платформы, которая позволяет осуществлять перевод и распределение денежных средств «сверху до низу» по всей структуре экстремизма и терроризма на территории России. Область противодействия при этом несколько шире за счет организации в этой же сети структур снабжения материально-техническими ресурсами организованных групп экстремистов и террористов (вплоть до аренды жилого и нежилого помещений, аренды легкового и грузового автотранспорта и т. д.).

Необходимость противодействия правоохранительных органов преступности в целом в условиях стремительной и всеохватывающей компьютеризации и информатизации вызвало к жизни новые и перспективные виды разведок – аналитическую разведку и компьютерную разведку.

Под аналитической разведкой изначально понимали выведывание информации (иногда даже подчеркивали: новой информации) в ходе обработки, осмысления, в ходе применения различных методов анализа данных и сведений, накапливаемых в процессе деятельности органов внутренних дел по профилактике, расследованию и пресечению правонарушений и преступлений.

Под компьютерной разведкой изначально понимали поиск источников информации и последующее добывание данных и сведений из различных компьютерных систем и сетей в интересах профилактики, расследования и пресечения правонарушений и преступлений. Компьютерная разведка развивается уже более трех десятилетий и сегодня представляет собой лишь одно из направлений «киберразведки», стоящей на вооружении спецслужб технологически развитых стран и определяемой как целенаправленный поиск информации в социальных сетях во всей киберсфере, в том числе в «самых темных закоулках» сетей[1].

Однако появление киберразведки связано, прежде всего, с усложнением задач противодействия преступности в глобальном виртуальном пространстве, характеризующимся, многоуровневостью, многоплановостью и сегментированностью (фрагментируемостью). В настоящее время решаются задачи выявления физического (географического и адресного) расположения объектов глобальной сети – целенаправленно установленных или используемых сетевых устройств, каналов связи, средств вычислительной техники («рабочих мест» лиц, занимающихся противоправной деятельностью). Сложность в решении этих задач добавляет разнообразие гаджетов и информеров – тех устройств, которые оказываются мобильными, перемещающимися вместе с тем лицом, которое их использует.

Таким образом, особое место киберразведки в противодействии терроризму и экстремизму – это физическое определение разнообразных устройств в глобальной сети и их местоположения (географического и адресного) и выявления лиц, использующих эти устройства и имеющих отношение к экстремистской и террористической деятельности; дальнейшее обнаружение мест нахождения выявленных лиц, постановка их на оперативный контроль. Сочетание компьютерной разведки, аналитической разведки и рассматриваемого направления киберразведки способствует выявлению угроз и позволит правоохранительным органам эффективно противодействовать терроризму и экстремизму.

Другая причина возникновения киберразведки связана с необходимостью изучения устройства (построения) глобальной сети, функционирования, взаимодействия, воздействия и противодействия информационных процессов средств вычислительной техники, подключенных к сети. Таким образом, в киберразведке выделяется еще одно направление – картография, т. е. формирование карт глобальных сетей. Без решения данной проблемы не может быть решена основная задача правоохранительных органов противодействия преступности, в частности наиболее опасным ее проявлениям – терроризму и экстремизму в глобальном виртуальном пространстве.

Следует отметить, что отечественным специалистам приходится решать чрезвычайно сложную задачу, поскольку по вполне понятным причинам военноморская разведка США не делилась с кем бы то ни было технологиями скрытного (латентного) установления связей между абонентами сети и технологиями передачи зашифрованных сообщений. Более того, IT-специалисты, примкнувшие к криминальным структурам, за последние лет двадцать развивали подобного рода технологии, целенаправленно отступая от общепринятых стандартов мировой практики.

Таким образом, в рамках ведения киберразведки IT-специалисты правоохранительных органов вынуждены изучать неизвестные специальные сетевые технологии, фактически используемые на просторах глобального, виртуального пространства, создаваемые преступными сообществами в своих интересах, а также целенаправленно создаваемые скрытые в сети структуры типа «DarkNet», «DeepNet» и прочих, множество которых появляется ныне.

Одно из направлений киберразведки – в полном смысле разведка сегмента, к которому относят большую часть одноранговых сетей, – это так называемый «темный веб» (*dark web*), название которого обязано широким использованием разнообразных специфических ресурсов преступными организациями, незаконными антисоциальными группами и группировками, экстремистами и террористами. Основными платформами этого сегмента являются сети типа *Tor* или *I2P*, платежная сеть *BitCoin* и некоторые другие, на которых проявляется чрезвычайно высокая криминальная активность, в частности, самая опасная – экстремистская и террористическая.

Практическая деятельность изучения технологической структуры всемирной сети и организованных на ее базе сетей по большей мере энтузиастов, в меньшей мере IT-специалистов правоохранительных органов уже обрела свое название – нетсталкинг (от англ. *netstalking* – «выслеживание в сети»).

Эта деятельность, осуществляется в пределах сети методами поиска, проб и ошибок. Она направлена на обнаружение малоизвестных, малодоступных и малопосещаемых объектов с последующим их анализом, систематизацией и сохранением результатов исследований. Чаще всего цель таких исследований энтузиастов – удовлетворение собственного любопытства в разнообразных планах (эстетического, информационного, на предмет возможности использования и т. д.) искателя. Под это определение попадает поиск объектов глубокой сети, в том числе IoT-устройств, поиск и описание ресурсов, поддержка которых ведется на устаревших протоколах или на неизвестных протоколах, которые не соответствуют каким-либо стандартам. В целом деятельность нетсталкеров иррациональна, но все чаще становится осознанной в поисках, формирует определенные навыки сетевого поиска.

Что же касается поисково-исследовательских операций IT-специалистов правоохранительных органов и специальных служб, то их деятельность носит сугубо осмысленный и целенаправленный характер и базируется на закрытых разработках технологий скрытной работы в сети, на богатом накопленном опыте конкуренции этих служб.

Практически во всех высокоразвитых в информационно-технологическом плане странах в 2010-е годы были разработаны и приняты концептуальные и стратегические документы в сфере информационной безопасности, а в некоторых даже появились и стремительно развиваются специализированные структуры, так называемые «кибервойска».

События и процессы, происходящие в мире, свидетельствуют, что многие государства весьма активно берут под контроль свои территориальные части мировой сети и развивают программно-аппаратные средства мониторинга кибератак, защиты коммуникаций и процессов передачи данных, подключенных к се-

ти многочисленных информационных систем, относимых к субъектам государственной критической инфраструктуры.

Именно контроль разнообразных сетевых коммуникаций и информационных процессов в них на государственном уровне предопределяет развитие киберразведки на новом качественном уровне, начиная с инициатив Президента Российской Федерации в 2020 г. провести на международном уровне обсуждение проблем и заключения договоренностей в сфере кибербезопасности.

Учитывая мировые процессы и события последнего времени, киберразведку можно представить как методы и средства выявления уязвимостей и скрытых угроз безопасности в информационной сфере, замыслов и реализации киберпреступлений и кибератак (как внутренних, так и внешних), попыток организации в сети незаконных латентных сайтов и их работы, основанных на информационно-технологических решениях, умышленно несоответствующих каким-либо стандартам – государственным либо международным.

Несомненно, в нынешних условиях пришла пора в рамках оперативно-разыскной деятельности развивать такие составляющие или направления как сетевой сыск или сетевой розыск по аналогии, например, с уголовным розыском преступников и рецидивистов в Российской Федерации и политическим сыском в царской России по отношению к экстремистам и террористам. Так можно обозначить принципиально новую область использования киберразведки.

Библиографический список

1. Денесе Э. Как Израилю удастся бороться с терроризмом с помощью соцсетей // Сетевое издание – интернет-проект «ИноСМИ.ру» – URL: <http://inosmi.ru/military/20160426/236299149.html>.

Цимбал В. Н.¹,

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

ОСОБЕННОСТИ ПРОТИВОДЕЙСТВИЯ ИДЕОЛОГИИ ЭКСТРЕМИЗМА В СРЕДСТВАХ МАССОВОЙ ИНФОРМАЦИИ

В обществе бытует мнение, что средства массовой информации (СМИ, mass media) – «четвертая власть», имеются научные исследования на этот счет [1; 2; 3]. Мы не полностью разделяем данное мнение, однако согласимся с тем, что сила воздействия, влияния, убеждения на сознание аудитории со стороны СМИ достаточно высока.

Согласно действующему законодательству (ст. 2) под СМИ понимается периодическое печатное издание, сетевое издание, телеканал, радиоканал, телепрограмма, радиопрограмма, видеопрограмма, кинохроникальная программа, иная форма периодического распространения массовой информации под постоянным наименованием (названием) [4].

Совокупность всех жанров, посредством которых реализуется все содержание массовой информации, представляется в форме интервью, репортажа, комментария, обзора, заметки и т. п.

Материальное представление СМИ может быть представлено в виде газет, журналов и иных печатных изданий, нематериальное – телевидения, радио и кино. Также информация через СМИ может распространяться через сеть Интернет, для их обозначения используют следующие понятия: «Интернет-СМИ», «онлайн-СМИ», «электронные СМИ», «сетевые СМИ» и т. д.

В целом, функционирование СМИ и его популярность стало возможным благодаря широкому распространению грамотности среди населения, увеличению количества свободного времени, развитию и проникновению в жизнь общества технологий передачи данных (радиоканалы, проводные линии связи), а также наличию у людей доступа к принимающей аппаратуре (телевизорам, радиоприемникам, мобильным телефонам, компьютерам) таких данных.

К основным функциям СМИ относятся: информационная, образовательная, пропагандистская, социализации, критики и контроля, мобилизационная, инновационная, оперативная, формирование общественного мнения и иные.

Масс-медиа на сегодня заняли важную нишу в жизни человека, общества и государства. Оно доводит актуальную и оперативную информацию до потребителей (новости, аналитические программы), осуществляет образовательную функцию (документальные и научно-публицистические программы и отдельные каналы), развлекательную роль (демонстрация художественных фильмов и сериалов; разных программ юмористического и иных жанров) и имеет большое значение в политической жизни общества.

¹ © Цимбал В. Н., 2020.

Государство использует ресурсы СМИ для доведения до граждан страны сведений о деятельности органов власти, представляет свою точку зрения на геополитические и международные вопросы, используется в процедуре выборов. Многие государства осуществляют контроль и надзор за деятельностью СМИ, а в некоторых странах существуют только государственные масс-медиа, роль независимых либо сильно занижена, либо вообще сведена на нет: Северная Корея, Туркменистан, Вьетнам, Судан и другие[8].

При всех положительных чертах СМИ логично было бы отметить и негативную сторону публичности и оперативности в процессе доведения информации до потребителей – это возможность использования данных информационных ресурсов в противоправных целях. Одна из таких отрицательных черт, которые использовались и иногда используются преступниками, – пропаганда своих взглядов через СМИ, которую последние, бывало, не ограничивали, а порой и использовали для привлечения аудитории.

За достаточно короткий срок экстремизм (от лат. *extremus* – крайний) превратился в одну из главных проблем в Российской Федерации. Под термином понимается «...приверженность в политике к крайним взглядам и мерам» [9].

Проявления экстремизма разнообразны – от возбуждения гражданской ненависти, провокации беспорядков до создания незаконных вооруженных формирований и совершения террористических актов.

В соответствии с действующим законодательством Российской Федерации (ст. 3) основными направлениями противодействия экстремистской деятельности являются: осуществление профилактических мер, предупреждающих подробную деятельность, а также ликвидация ее причин; выявление, предупреждение и пресечение экстремистской деятельности как со стороны физических лиц, так и в их отношении, в организациях, объединениях и ином [5].

К сожалению, в российском законодательстве отсутствуют четкие определения либо регламентация информации, запрещенной к публикации, однако из имеющихся нормативных правовых актов можно выделить следующие, которые регламентируют этот вопрос хотя бы частично.

Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», где обозначается запрет на распространение следующей информации: направленной на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды, а также иной информации, за распространение которой предусмотрена уголовная или административная ответственность (персональные данные, нарушение авторских и смежных прав, сведения, составляющие государственную тайну и т. п.) (ч. 6 ст. 10) [6].

В Законе Российской Федерации от 27 декабря 1991 г. № 2124-1 «О средствах массовой информации» также имеется перечень сведений, запрещенных к распространению, но уже конкретно в СМИ, в части рассматриваемой нами тематики работы: материалы, содержащие публичные призывы к осуществлению террористической деятельности или публично оправдывающие терроризм, другие экстремистские материалы и иная информация (ст. 2) [4]. Также имеются другие

нормативные правовые акты, запрещающие к распространению информацию экстремистского характера, однако рассматривать их все нецелесообразно.

На сайте Министерства юстиции Российской Федерации имеется федеральный список экстремистских материалов, по данным на ноябрь 2020 г. в нем более 5 тыс. записей [10].

Причинами роста экстремизма в современном обществе и в Российской Федерации, в частности, отметим следующие: улучшение морального самосознания молодежи, снижение качества образования, низкая политическая и правовая свобода, недостаточное нравственное и духовное воспитание молодежи в учебных заведениях, пропаганда в СМИ культа силы, политическая и правовая неграмотность, наличие субкультур, криминализация общества, психологические особенности личности (подверженность влиянию, внушаемость, мнительность). Все вышеперечисленное в той или иной мере оказывает влияние на появление новых, молодежных и не только, экстремистских объединений, течений, рост ксенофобии, агрессии, грубости, хулиганства, преступности на национальной, политической и религиозной почве.

Укрепление патриотизма и гражданской ответственности в обществе, воспитание уважения к представителям других национальностей, чужой культуре, открытость и толерантность – одно из наиболее действенных средств борьбы с экстремизмом, но только лишь, как указано выше, при условии объединения усилий всех государственных и общественных структур и граждан.

Предполагается, что профилактическая деятельность в части преступлений экстремистской направленности является наиболее эффективной мерой борьбы с подобными преступлениями как в СМИ, так и в сети Интернет. Необходимо выделить практические способы противодействия экстремизму:

- информирование общественности об экстремизме, его формах, проявлении, проблематике, негативном воздействии на государство, общество и граждан в целом;
- осуществление мониторинга СМИ и информационных ресурсов сети Интернет с целью выявления контента, содержащего вышеуказанные материалы (сотрудниками правоохранительных органов проверяется информационное пространство – социальные сети, сайты, блоги. Применяются при этом современные программные и программно-технические решения (к примеру, СОРМ));
- прямое разоблачение, аргументированная критика высказываний, противопоставление истины экстремистским доводам;
- занижение пропускной способности канала связи, перекрытие каналов распространения информации от злоумышленников через СМИ и сеть Интернет, а также при необходимости блокирование доступа к различным информационным ресурсам (в случае выявления преступления);
- дискредитация личности, авторитета и доводов преступных лидеров и/или руководителей противозаконных организаций (специфическая деятельность правоохранительных органов);
- распространение правдивой, достоверной информации о тех, или иных обстоятельствах [7, с. 43];

– развитие толерантности, правовой грамотности, социальной ответственности, патриотизма, нравственности и духовности личности через СМИ.

Без доступа к информации и информационным ресурсам жизнь современного человека уже практически не представляется. Они позволяют ему быть в курсе общественной и политической жизни, учиться, общаться, работать, социализироваться в целом, а СМИ в обозначенных процессах играет немаловажную роль. Масс-медиа может и приносить пользу обществу, и наносить серьезный вред, допуская использование такого источника информации в преступных целях. Поэтому, как представляется, роль СМИ в современном информационном обществе будет только возрастать, в связи с чем, государству придется все больше прилагать усилия для контроля над информацией, обрабатываемой в них (тем самым прививая ответственность перед потребителем), что в свою очередь, не должно отражаться на независимости СМИ, а также на актуальности и объективности проецируемых ими сведений (отсутствия цензуры, необоснованных запретов передаваемых сведений и иного).

Библиографический список

1. Сафарян, А. В. СМИ как «четвертая власть» и институт социализации // Власть. – 2008. – № 5. – С. 62–65.
2. Цветкова Л. А. Перерождение СМИ: Интернет-журналистика на олимпе «четвертой власти» // Материалы IV Международной научной конференции «Реклама и современный мир». – Тверь, 2016. – С. 246–248.
3. Мрочко, Л. В. СМИ в современном обществе: «Четвертая власть» или слуга власти? / Л. В. Мрочко, А. И. Пирогов // Экономические и социально-гуманитарные исследования. – 2020. – № 2 (26). – С. 165–174.
4. Закон Российской Федерации от 27 декабря 1991 г. № 2124-1 «О средствах массовой информации» (ред. от 01.03.2020) // СПС «КонсультантПлюс» – URL: http://www.consultant.ru/document/cons_doc_LAW_1511.
5. Федеральный закон от 25 июля 2002 г. № 114-ФЗ «О противодействии экстремистской деятельности» // СПС «Гарант-Сервис» URL: <http://base.garant.ru/12127578> (режим доступа: ограниченный).
6. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СПС «КонсультантПлюс». – URL: http://www.consultant.ru/document/cons_doc_LAW_61798.
7. Карташов, К. А. Развитие социальных сетей как базис повышения конкуренции в маркетинге или как источник информации об экстремистской деятельности / К. А. Карташов, В. Н. Цимбал // Вопросы экономики и права. – № 70. – 2014. – С. 40–44.
8. Сайт международной правозащитной организации «Репортеры без границ». – URL: <https://rsf.org/en/ranking/2019#>. (дата обращения 05.11.2020).
9. Сайт международной неправительственной организации Freedom House. – URL: <https://freedomhouse.org/report/freedom-press/2017/press-freedoms-dark-horizon> (дата обращения 05.11.2020).
10. Политология: словарь / под ред. В. Н. Коновалова. – Ростов-н/Д: РГУ, 2001. – 285 с.

11. Федеральный список экстремистских материалов // Сайт Министерства юстиции Российской Федерации [электронный ресурс]. – URL: <https://minjust.gov.ru/ru/extremist-materials> (дата обращения: 11.11.2020).

Клочкова Е. Н.¹,

*доцент кафедры специальных информационных технологий
учебно-научного комплекса информационных технологий Московского
университета МВД России имени В.Я. Кикотя, полковник полиции*

КИБЕРТЕРРОРИЗМ КАК ОДНА ИЗ ФОРМ ПРОЯВЛЕНИЯ СОВРЕМЕННОГО ТЕРРОРИЗМА

Согласно Федеральному закону Российской Федерации «О противодействии терроризму» терроризм – это 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.

Терроризм – многообъектное преступление, главной целью которого является общественная безопасность, равно как посягательства на:

- жизнь и здоровье граждан;
- объекты критической инфраструктуры;
- природную среду;
- информационную среду;
- органы государственного управления;
- государственных и общественных деятелей.

Такие действия проводятся в интересах достижения политических, военных, экономических, социальных и других целей террористов.

Одной из форм проявления терроризма является кибертерроризм, который в последние годы набирает все большие обороты. Основное его действие, направлено на нарушение работы различных автоматизированных систем, на информацию, обрабатываемую с использованием средств вычислительной техники, на компьютерные сети.

Современное развитие общества в настоящий момент таково, что для его нормальной жизнедеятельности разрабатывается и внедряется все большее количество информационных систем, связанных с жизнью людей. Любое несанкционированное вмешательство в работы систем может привести к печальным последствиям, начиная от нанесения материального ущерба, заканчивая возможной гибелью людей или даже значительной техногенной катастрофой.

Говоря о кибертерроризме, мы должны понимать, что, как и обычный терроризм, это комплексная акция, выражающаяся в преднамеренной, политически мотивированной атаке. Основными объектами атаки кибертеррористов становятся информация, обрабатываемая с использованием средств вычислительной техники, информационные системы, аппаратура, предназначенная для передачи данных, и иные элементы информационных систем, позволяющие злоумышленнику проникнуть в систему. При этом проникновение в систему может сопровождаться не только хищением циркулирующей информации, но и различными деструктивными воздействиями, которые будут зависеть только от целей, которые преследует кибертеррорист.

¹ © Клочкова Е. Н., 2020.

В настоящее время выделяют три уровня кибертерроризма.

Первый уровень связан с простейшими хакерскими атаками на информационные системы. Злоумышленниками в данном случае чаще всего являются молодые люди, решившие попробовать себя на поприще кибертеррориста. Их обычно можно отнести к категории начинающих программистов. Программные средства, которые используются для реализации атак, в большинстве своем, берутся из сети Интернет. Потери от такого вида атак, как правило, минимальны, а угрозы быстро нейтрализуются специалистами по защите информации.

Второй уровень предполагает, что организацией атак на информационные системы занимается не одиночка, а уже организация, обладающая всеми признаками управляемой структуры, а также имеющая возможности создания собственного программного обеспечения для взлома компьютерных сетей, обучения новичков. Основная их деятельность связана с получением материальной выгоды. Последствия от реализации их угроз могут быть значительными, но в большинстве своем носят только материальный характер.

Последний уровень предусматривает, что кибертеррористы способны к скоординированной атаке, которая может привести к массовым нарушениям систем безопасности страны. Для реализации своих целей они имеют возможность создания очень сложного специализированного программного обеспечения. Организация обычно четко структурирована, ее члены могут анализировать свои действия, вырабатывать совместные планы действий. Последствия от реализации таких атак будут максимальны не только с точки зрения значительных материальных потерь, но и с учетом возможности гибели людей.

На сегодняшний момент мы можем говорить об увеличении количества угроз, связанных с кибертерроризмом. Это вызвано, прежде всего, распространением COVID-19. В период пандемии многие предприятия, как государственные, так и коммерческие были вынуждены перевести своих сотрудников на удаленную работу. При этом для продолжения нормального функционирования они предоставляли сотрудникам удаленный доступ к информационным системам.

Если технически организовать такое взаимодействие не представляет трудностей, т.к. в большинстве случаев сотруднику достаточно иметь компьютер и точку выхода в сеть Интернет, то проблема обеспечения безопасности передаваемых данных резко обострилась. Далеко не все организации были готовы гарантировать защищенность своей информации, прежде всего потому, что у некоторых из них раньше такой проблемы не существовало в связи с отсутствием выхода в общедоступные сети. В таком случае на предприятиях могло просто не оказаться специалистов, способных обеспечить безопасные соединения, а с другой стороны, сотрудники, работающие с информацией и получившие к ней удаленный доступ, не всегда понимают важность ее защиты и владеют навыками по обеспечению ее безопасности на собственных компьютерах. Как следствие, резко возросло количество уязвимостей различных информационных систем, которыми могут воспользоваться злоумышленники.

Кибертерроризм представляет серьезную угрозу для человечества. Наиболее опасны, с точки зрения последствий, атаки на объекты критически важных инфраструктур, это объекты энергетики, телекоммуникации, финансовые, про-

мышленные информационные системы, а также автоматизированные системы, связанные с обеспечением обороноспособности страны. В большинстве своем данные угрозы носят удаленный характер и их трудно обнаружить до того момента, когда они будут реализованы. При этом для проникновения в систему нет необходимости физического присутствия на объекте, и атака может происходить из любой точки мира, а кибертеррористом может оказаться даже талантливый подросток, решивший проверить свои возможности.

Библиографический список

1. Федеральный закон от 6 марта 2006 г. № 35-ФЗ «О противодействии терроризму». // СПС «КонсультантПлюс». – URL: http://www.consultant.ru/document/cons_doc_LAW_58840. (дата обращения 25.11.2020).
2. Информационное противодействие терроризму. URL: <https://docviewer.yandex.ru/view/673819555/?page=11/> (дата обращения: 25.11.2020).
3. Степанов О.А. Противодействие кибертерроризму в цифровую эпоху: монография. М.: Юрайт, 2020. – 103 с.

Гущина А. А.¹,
 старший преподаватель кафедры
 радиотехники и электроники
 Воронежского института МВД России,
 кандидат технических наук, майор полиции;

Пакляченко М. Ю.²,
 старший преподаватель кафедры специальных
 информационных технологий учебно-научного
 комплекса информационных технологий
 Московского университета МВД России
 имени В.Я. Кикотя, кандидат технических наук,
 капитан полиции

К ВОПРОСУ ТЕРРОРИЗАЦИИ МЕДИА-КОНТЕНТА

На данный момент видится весьма актуальной задача охарактеризовать процессы, происходящие с терроризмом в цифровую эпоху. При этом главный акцент следует сделать на технологии воплощения террора в сети, а также на эффектах, которые связаны с их использованием.

Коммуникация, выстраивание идентичности, распространение идей, рекрутство – указанные практики во многом упрощаются благодаря использованию новейших средств информационно-коммуникационных технологий, когда само медийное пространство превращается в поле боя. При этом, виртуализируясь, терроризм становится зависимым от новых технологий. Указанные особенности современного терроризма необходимо досконально исследовать, поскольку декодирование сущности терроризма как таковое представляется одним из способов борьбы с ним.

Существует весьма высокая вероятность того, что адресность указанного глобального феномена деструктивной активности в цифровом пространстве может составлять десятки тысяч абонентов информационных ресурсов, а также отдельные державы в целом. К настоящему моменту подтверждена прямая пропорциональная зависимость числа преступлений, совершаемых в киберпространстве, от количества пользователей сетей.

С понятием терроризма в коммуникационных системах и сетях связано множество сложностей.

Во-первых, отсутствует методика однозначного определения числа пострадавших от насилия и возможность полноценного, гарантированного удостоверения их личности ввиду контекста виртуализации. В данном контексте большинство преступников, совершивших противоправные акты террористической направленности в сетях, не отождествляют себя именно с личностью террористов. С другой стороны, отдельные преступные сообщества стремятся однозначно идентифицировать себя и свои деяния именно как кибертеррор.

¹ © Гущина А. А., 2020.

² © Пакляченко М. Ю., 2020.

Во-вторых, толкование терроризма как эквивалента военизированных преступных деяний в мирное время опосредует его восприятие не как разовой акции какой-либо группы, связанной с манифестацией определенной акции, а как действия, эмитирующего в своем содержании именно боевую, разрушающую или уничтожающую активность в отношении выбранной цели. Данное действие совершается целенаправленно, динамично и возможно на некой регулярной основе. Таким образом, можно говорить о цифровой революции на базисе трансформации военных действий [1, с. 15], где кибертерроризм выступает как новая форма ведения борьбы между государствами.

Нынешние террористические группировки, как правило, применяют информационно-коммуникационные технологии на регулярной основе, наряду с тривиальными средствами совершения терактов, что стремительно сокращает временные рамки трансформации угрозы в ее результирующее воплощение в форме реального совершенного акта. Таким образом, для нынешних реалий характерно смещение акцента среды совершения терроризма в сфере масс-медиа и социальных сетей, где реализуются различного рода деструктивный контент идеологического, насильственного, политического или иного содержания, который ориентирован скорее не на уничтожение, а скорее на всеобщность и значимость своего информационного освещения.

В связи с развитием масс-медиа и цифровизацией деятельности мирового сообщества терроризм приобрел возможность своего проявления в режиме online, яркий тому пример – трагические события 11 сентября 2001 г. в США [2, с. 34]. К настоящему моменту можно говорить о терроризации медиаконтента, которому свойственен фокус на различного рода проявления насилия, афиширование жертв терактов. Причем указанные процессы, хотя и в контексте описания борьбы с ними, могут освещаться на нетрадиционных медийных площадках, например в федеральных новостях, либо при сюжетах о прогнозе погоды. Перечень таких нетрадиционных для проявления кибертерроризма площадок (не ассоциирующихся с террористической деятельностью) в сфере медиа может быть дополнен социальными (пользовательскими) приложениями (user generated content). В подобном контенте чаще всего воплощается рекрутство, идеологические идеи, пропаганда, которые доступны «по клику». Например, довольно часто кибертеррористы используют цифровые журналы, доступные для просмотра на мобильных устройствах или компьютере, с целью максимальной интеграции подписчиков в освещаемые истории идейного содержания, что способствует значительной по масштабам деморализации пользователей. Дополнительным примером может быть использование террористами интерактивного инструментария (стикеров опроса или тестирования) социальных сетей. Такое действие определяет глубокую интеграцию и опосредует мощнейшую рефлекссию, сопряженную с возбуждением заинтересованности сторонних пользователей с порождением последующего интереса к террористической деятельности, который может проявиться как последствия ввиду соответствующего вовлечения.

Таким образом, очевидны масштабы влияния, оказываемого сетью Интернет и передовыми ИТ-технологиями на сознание пользователей, модифицированное умелым использованием террористических группировок, которые, в свою оче-

редь, трансформировались из иерархических в сетевые. Сама же медиатизация терроризма может быть охарактеризована зависимостью от репрезентации, формата правил медиаплощадки, а также переправлением, определенной трансформацией медиасреды в некую деструктивную сущность.

Говоря о тактиках противодействия кибертерроризму в сети, можно очертить следующие стратегии. Необходима минимизация распространения подобного деструктивного медийного контента, т. е. персонифицированный отказ каждого пользователя от тиражирования или трансляции подобного рода информации. Следующий, коррелирующий с указанным ранее шагом, подход заключается, на первый взгляд, в весьма примитивном цифровом просвещении пользователей, кибер- или информационной гигиене, грамотности в киберпространстве. Данный аспект находится на границе объективно существующих социоинформационных потребностей и одной из многочисленных целей государственной деятельности, заключающейся в повышении конкурентоспособности российской медиаотрасли и уровня освоения гражданами современных средств массовой коммуникации.

Следовательно, одинаковые по своему содержанию тактики информирования могут быть применимы как во благо, так и для достижения преступных целей. С данной точки зрения крайне важно увеличить массивы информации просветительного содержания, способы их надежной доставки до широкого круга респондентов, корректность их представления, что требует очевидной координации усилий людей и государств в мировом масштабе на регулярной основе.

Библиографический список

1. Pollitt M., CYBERTERRORISM – Fact or Fancy? FBI Laboratory [электронный ресурс]. – URL: <http://www.cs.georgetown.edu/~denning/infosec/pollitt.html> (дата обращения: 04.12.2020).
2. Степанов, О. А. Противодействие кибертерроризму в цифровую эпоху : монография / О. А. Степанов. – М. : Юрайт, 2020. – 103 с. – (Актуальные монографии). – ISBN 978-5-534-12775-1. – Текст : электронный // ЭБС Юрайт [сайт]. – URL: <https://urait.ru/bcode/448300> (дата обращения: 04.12.2020).

Лустин В. И.¹,

старший преподаватель кафедры информационной безопасности

учебно-научного комплекса информационных технологий

Московского университета МВД России

имени В.Я. Кикотя, полковник полиции

ОТДЕЛЬНЫЕ АСПЕКТЫ ПРОТИВОДЕЙСТВИЯ ТЕРРОРИЗМУ В ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ

В начале XXI века важной проблемой социального развития мирового сообщества стала необходимость дальнейшего совершенствования противодействия терроризму и экстремизму в различных формах их проявления. К объективным и субъективным причинам возникновения угроз национальной безопасности государства природного и техногенного характера добавляются угрозы террористического характера как влияющие на развитие существующей цивилизации.

Основной угрозой экстремистского характера является распространение идеологии политического, этнического и религиозного экстремизма, и это представляет существенную опасность для соблюдения конституционных интересов личности, общества и государства. Эта тенденция является актуальной как для отдельного государства, так и для всего мирового сообщества.

Немаловажным является и тот факт, что средства массовой информации, игравшие на всех этапах своего существования важнейшую роль в жизни общества как источника информации и средства идеологического влияния на массы, получили в свои руки такой мощнейший инструмент, как информационно-телекоммуникационные сети. Использование таких сетей в различных сферах деятельности государства позволят говорить о создании в настоящее время цифровой экономики, а также информатизации общества.

Более того, можно рассматривать выделение информационных телекоммуникационных сетей в самостоятельную отрасль, о чем свидетельствует дальнейшее развитие веб-сайтов, мессенджеров, социальных сетей, составляющих конкуренцию традиционным средствам массовой информации. Причем широкие группы населения основным источником новостей и информации, заслуживающей доверия, считают Интернет.

Использование информационно-коммуникационных технологий в различных сферах общественной жизни является основой для создания единого информационного пространства на основе использования информационных технологий и коммуникаций для обмена, сбора, накопления, обработки и хранения информации. При этом распространение идей терроризма и экстремизма через информационно-телекоммуникационную сеть Интернет и средства массовой информации названо одним из основных факторов, способствующих возникновению и распространению терроризма в Российской Федерации[1].

Совместная работа правоохранительных органов и общественных организаций по противодействию экстремизму и терроризму должна осуществляться по следующим направлениям:

¹ © Лустин В. И., 2020.

- противодействие распространению идеологии терроризма путем использования информационных технологий и телекоммуникационных сетей;
- выявление и пресечение деятельности источников финансирования ресурсного обеспечения террористических организаций;
- предупреждение, выявление и пресечение проявлений экстремистских и террористических действий;
- блокировка сайтов, распространяющих террористическую идеологию;
- выявление и устранение причин и условий, способствующих распространению преступлений экстремистского и террористического характера.

В настоящее время в мире наблюдается возникновение конфликтов на межэтнической и межконфессиональной основе. Нельзя допустить проникновение в российское общество отрицательных экстремистских настроений и проявлений терроризма при осуществлении государственной политики интеграции в мировое сообщество. Такие проявления экстремизма и его крайней формы, терроризма, представляют угрозу национальной безопасности государства.

Выявление случаев межнациональной розни и религиозного раскола, способных привести к дестабилизации социальной и политической обстановки в стране, является основой для проведения эффективного противодействия экстремизму и терроризму как на государственном уровне, так и для конкретного субъекта Российской Федерации.

Экстремизм служит идеологической основой и социальной базой для терроризма. При этом отличительной чертой экстремизма в современных условиях является оперативное приспособление к окружающей обстановке. Террористы активно используют современные методы формирования террористических движений – группировки складываются через Интернет путем поиска единомышленников в соответствующих блогах[4]. Такая ситуация складывается потому, что в современном мире ни отдельная личность, ни социальная группа практически не может отказаться от электронных СМИ как своеобразного способа утоления информационного голода[2]. Учет сложившейся ситуации необходим при планировании мероприятий по противодействию терроризму в информационном пространстве.

Информационное противодействие экстремизму и терроризму представляет собой деятельность по вскрытию сущности и разъяснению опасности экстремизма и терроризма, оказанию воздействия на граждан (группы граждан) с целью воспитания у них неприятия идеологии насилия и привлечения их к участию в противодействии терроризму. Такая деятельность включает в себя и сбор, накопление, систематизацию, анализ, оценку информации об угрозах экстремистских проявлений и террористических актов, обмен ею и выдачу ее потребителям такой информации[5].

Таким образом, противодействие правоохранительных органов экстремизму и терроризму в информационном пространстве должно базироваться на сбалансированном ресурсном обеспечении. А в качестве приоритетных направлений деятельности противодействия терроризму можно обозначить выявление субъектов преступной деятельности, пресечение их действий, устранение причин и условий возникновения и распространения этих противоправных деяний.

Идеология терроризма и экстремизма, воздействуя на массовое сознание, формирует определенные социальные группы, используя для этого, в том числе, информационно-коммуникационные сети. Силовые методы правоохранительных органов необходимо дополнять организационными, правовыми, профилактическими и воспитательными мерами с использованием ресурсов не только государственных органов, но и общественных организаций. В рамках противодействия терроризму в информационном пространстве необходимо информировать различные социальные группы населения о недопустимости идеологии экстремизма, о формах ее проявления и последствиях.

Для повышения эффективности информационного противодействия экстремизму и терроризму необходимо: дальнейшее совершенствование системы мониторинга как на государственном, так и на региональном уровне; широкое использование средств телекоммуникаций для информирования населения, для профилактики и противодействия экстремистским и террористическим проявлениям, целевую направленность проводимых мероприятий в информационном пространстве по противодействию экстремизму и терроризму; обеспечение эффективного межведомственного взаимодействия, сотрудничества с общественными организациями, в том числе и на международном уровне.

Реализация таких мероприятий позволит получить объективное представление о деятельности и составе организаций экстремистской направленности, подготовить и осуществить мероприятия по информационному противодействию в отношении группировок экстремистского толка, устранить причины и условия, способствующие развитию экстремизма на государственном и региональном уровне, осуществить эффективное взаимодействие правоохранительных органов, использовать ресурсы общественных организаций в обеспечении общественной безопасности.

Библиографический список

1. Концепция противодействия терроризму в Российской Федерации : Утверждена Президентом Российской Федерации 5 октября 2009 г. // Российская газета. – 2009. – 20 окт.
2. Бабинцев, В. П. Этнический экстремизм в молодежной среде: диагностика и перспективы преодоления / В. П. Бабинцев, Б. В. Заливанский, Е. В. Самохвалова // Мир России. – 2011. – № 1. – С. 47–56.
3. Вдовин, Е. А. Проблема противодействия распространению идей экстремизма и терроризма в сети Интернет / Е. А. Вдовин // Молодой ученый. – 2019. – № 16. – С. 13–18.
4. Епифанцев, В. А. Государственная система противодействия экстремизму в условиях современного российского общества / В. А. Епифанцев, Д. В. Сочнев // Информатизация и информационная безопасность правоохранительных органов. – М., 2010.
5. Заливанский, Б. В. Технологии информационного противодействия экстремизму / Б. В. Заливанский // Современные научные исследования и инновации. – 2014. – № 3. – С. 62–71.

Архипова И. А.¹,

заместитель начальника кафедры криминалистики
Московского университета МВД России имени В.Я. Кикотя,
кандидат юридических наук, доцент,
полковник полиции

Шаров А. В.²,

начальник кафедры криминалистики
Московского университета МВД России имени В.Я. Кикотя,
кандидат юридических наук, доцент,
полковник полиции

ВОПРОСЫ ВЗАИМОДЕЙСТВИЯ ПРИ ПРОВЕДЕНИИ КОНТРТЕРРОРИСТИЧЕСКИХ ОПЕРАЦИЙ

Анализ сложившейся в настоящий момент общественно-политической обстановки в мире позволяет сделать обоснованный вывод, что одной из важнейших проблем для целого ряда государств является борьба с терроризмом. К сожалению, она не обошла и нашу страну, которая столкнулась с этим негативным явлением во всех его проявлениях, включая такую форму как незаконные вооруженные формирования. На территории России возникли зоны, на которые не распространяется действие государственных органов власти, ставшие средой формирования разнообразных преступных сообществ[1].

К сожалению, на протяжении 15 лет актуален тезис А. Новикова: «...особую озабоченность вызывает то обстоятельство, что на сегодняшний день преступные и террористические группировки, действующие на территории России, сумели установить обширные международные связи, обеспечивающие им материальную и техническую поддержку из-за рубежа. Руководители террористических организаций предпринимают попытки по вовлечению в сферу своей деятельности представителей исполнительной, законодательной и судебной властей. Используя сепаратистские лозунги в качестве идеологического прикрытия своей деятельности, преступные и террористические сообщества изобрели фактически новую форму преступного бизнеса, когда получение финансовых средств осуществляется только за ведение войны на территории своего государства»[2]. В настоящее время ситуация усугубляется в связи с широким применением в террористической деятельности «высоких технологий».

В этой связи представляется интересным мнение Г. А. Майстренко: «... эффективное противодействие данному негативному явлению может быть осуществлено только при условии организации четкого взаимодействия целого ряда государственных структур. Основой для такого взаимодействия должна стать система нормативных актов, включающая в себя документы, принятые на федеральном, региональном и внутриведомственном уровне»[3].

Основные принципы антитеррористической деятельности:

¹ © Архипова И. А., 2020.

² © Шаров А. В., 2020.

1) закрепление за каждой структурой определенного направления антитеррористической деятельности;

2) всесторонний обмен информацией в ходе проведения контртеррористических операций;

3) согласование действий, направленных на борьбу с терроризмом;

4) обобщение накопленного опыта по борьбе с терроризмом;

5) отработка совместных действий.

По нашему мнению, подход к управлению контртеррористическими операциями в первую очередь определяется целым рядом параметров. В этой связи мы предлагаем выделить основные этапы проведения контртеррористических операций, а также классифицировать их в зависимости от масштабов (локальные или регионального уровня), характера, выдвигаемых террористами требований (корыстные или политического свойства), а также обстановки, на фоне которой возникает необходимость проведения операции¹.

Например, при захвате заложников, в результате неудавшейся попытки ограбления банка, целью которого является уход от ответственности, для разрешения кризиса вполне достаточным станет привлечение сил МВД России, МЧС России и Минздрава. Привлечение в подобных случаях ФСБ России представляется нецелесообразным. Подобный подход имеет существенное значение, поскольку акции подобного рода могут играть роль отвлекающего маневра, и использоваться террористами для отвлечения основных сил и средств спецслужб к месту происшествия, что создает благоприятные условия для нанесения основного удара по другому объекту. Кроме того, одновременное присутствие руководителей различных ведомств равнозначного уровня может привести синхронной отдаче несогласованных между собой распоряжений. Очевидно, что руководство оперативным штабом, создаваемым при проведении контртеррористических операций, должно осуществляться представителем «профильного» с точки зрения возникшей ситуации ведомства, по запросам которого возможно привлечение сил и средств других структур, которые поступают в полное и безоговорочное подчинение руководителя штаба. Численность и объемы привлекаемых сил и средств должны носить обоснованный характер. Практика показывает, что злоупотребление усиленным режимом работы приводит к существенному снижению ее эффективности, поскольку накапливающаяся у людей усталость способствует формальному исполнению ими служебных обязанностей.

Приведенные соображения со всей очевидностью свидетельствуют о настоятельной необходимости разработать документ, детально регламентирующий порядок взаимодействия силовых структур при проведении контртеррористических операций. Обеспечение взаимодействия и достижение максимального эффекта за счет упорядочения действий каждой из задействованных силовых структур, что особенно важно именно в первые часы работы, осуществляемой по

¹ Здесь мы, прежде всего, имеем в виду отношение населения данной территории к требованиям террористов, а также реакцию населения страны в целом и освещение складывающейся ситуации в СМИ и международных структур, если в качестве потенциальных жертв выступают граждане иностранных государств.

«горячим следам», когда вероятность задержания преступников максимальна, весьма эффективно.

В ходе проведения контртеррористических операций взаимодействие может осуществляться и с другими правоохранительными органами: Прокуратурой, Министерством юстиции Российской Федерации, а также Минатомом, органами государственной власти, департаментами и комитетами по информации и связям с общественностью, по делам женщин, семьи и молодежи, образования, органами местного самоуправления.

Основной задачей при этом является предотвращение террористических актов, в первую очередь за счет своевременного получения информации о передвижениях террористов и их замыслах, что обуславливает необходимость организации на постоянной основе сбора оперативной информации, а с учетом имеющихся у террористических группировок международных связей – и обеспечение взаимодействия с СВР и направление в необходимых случаях соответствующих запросов в МИД России для организации работы с зарубежными структурами по тем или иным фактам.

В связи с настоятельной необходимостью отработки юридических и физических лиц, подозреваемых в причастности к деятельности террористических формирований, преступных групп и сообществ, следует детально проработать вопрос оптимизации сбора и обмена оперативной информацией МВД России, ФСБ России, СВР, ГРУ МО России.

Одним из слабых мест в контртеррористической работе является недостаточный уровень взаимодействия при проведении оперативно-разыскных мероприятий в ходе расследования уголовных дел о терроризме.

Следует всесторонне наращивать целевые оперативные позиции и укреплять взаимодействие следственных подразделений силовых ведомств, учитывая, что судебная перспектива данных уголовных дел в значительной степени зависит от качества их оперативного сопровождения. При этом необходимо обратить особое внимание на то, что зачастую значительная часть дел, связанных с терроризмом и экстремизмом заводится по линии преступлений в сфере экономики и незаконного оборота наркотических средств. Хотя в большинстве случаев ни разрабатываемые по ним фигуранты, ни объекты хозяйствования не привязаны к основным задачам подразделений.

Детальный анализ оперативной обстановки по противодействию проявлениям терроризма показывает, что основные пути устранения недостатков и повышения результативности оперативной работы лежат в плоскости дальнейшего совершенствования взаимодействия между всеми подразделениями полиции и других министерств и ведомств, определения приоритетов и предметных зон ответственности как для органов внутренних дел в целом, так и для отдельно взятых подразделений.

Библиографический список

1. Бутаев, М. Я. Доказывание по делам о преступлениях террористического характера на досудебных стадиях уголовного процесса : теоретико-прикладной аспект : автореферат дис. ... канд. юрид. наук : 12.00.09 / Бутаев Мурадали Яку-

бович ; [Место защиты: Моск. акад. экономики и права]. – Москва, 2016. – 35 с.
// Президентская библиотека имени Б.Н. Ельцина. URL: <https://www.prilib.ru/item/677532>. (дата обращения 11.12.2020).

2. Майстренко, Г.А. Факторы, способствующие распространению терроризма на территории России // Web of Scholar: RS Global Sp. z O.O. (Варшава). – 2018. – № 6 (24). – С.50–52. https://www.elibrary.ru/download/elibrary_35281631_98044106.pdf (дата обращения 11.12.2020).

3. Конференция по противодействию финансированию экстремизма и терроризма : вступительное слово заместителя Министра внутренних дел России генерал-лейтенанта милиции Андрея Новикова // Российская газета [электронный ресурс] URL: <https://rg.ru/67993-anons.html>. (дата обращения 11.12.2020)

4. Майстренко, Г.А. Факторы, способствующие распространению терроризма на территории России // Web of Scholar: RS Global Sp. z O.O. (Варшава). – 2018. – № 6 (24). – С.50–52. URL: https://www.elibrary.ru/download/elibrary_35281631_98044106.pdf. (дата обращения 11.12.2020).

Коратаев П. В.¹,

старший преподаватель кафедры авиационных систем

и комплексов радионавигации и радиосвязи

Военного учебно-научного центра ВВС

«Военно-воздушная академия имени профессора Н.Е. Жуковского

и Ю.А. Гагарина» кандидат технических наук, капитан

Пакляченко М. Ю.²,

старший преподаватель кафедры специальных

информационных технологий учебно-научного

комплекса информационных технологий

Московского университета МВД России

имени В.Я. Кикотя, кандидат технических наук,

капитан полиции

СТАНДАРТИЗАЦИЯ ПОНЯТИЙ И ОСНОВНЫХ ПОЛОЖЕНИЙ ПО ВОПРОСАМ РАБОТЫ С КОМПЬЮТЕРНЫМИ АТАКАМИ КАК С ФОРМАМИ ПРОЯВЛЕНИЯ ТЕРРОРИЗМА В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Трансформация экстремизма и терроризма в любых вариантах своего воплощения в современных реалиях воспринимается как одна из наиболее опасных и деструктивных по своим последствиям проблем.

Терроризм остается колоссальной угрозой национальной безопасности государства в масштабах своего совершения, приобретая в собственный арсенал способов воплощения все более изощренные формы, алгоритмы и средства, в том числе передовые достижения в области ИТ-технологий. Так, перечень традиционных террористических актов, таких, как похищение людей, взятие заложников, активация взрывных устройств, можно расширить за счет киберугроз, в том числе насильственного характера, нацеленных на масштабные разрушения инфраструктур государства либо на оказание влияния на сознание интернет-идеологий. Таким образом, можно признать существование вместе с исключительно положительными и прогрессивными процессами цифровизации общества, экономики, отдельных процессов деятельности социума и государства цифровизованной преступности в виртуальном пространстве (киберпреступности) и, следовательно, терроризма в информационной среде.

Для борьбы с изучаемым явлением, выполнения проактивной и реактивной защиты от его деструктивного воздействия определены и регулярно совершенствуются основные направления деятельности государства, осуществляемые его отдельными органами в форме работы по государственным программам, реализации дорожных карт, проектов и пр. При этом равными для всех остаются такие задачи как улучшение и оптимизация степени безопасности жизни и здоровья граждан, охрана имущества государства или муниципалитета, физических и

¹ © Коратаев П. В., 2020.

² © Пакляченко М. Ю., 2020.

юридических лиц. Наряду с этим приоритетными направлениями признаются обеспечение безопасности государства в целом, внедрение передовых ИТ-технологий в различных, в том числе инновационных, секторах государственной деятельности, преимущественно в экономике.

Рассматривая вопросы достижения обозначенных выше целей с позиции нормативной реализации, можно утверждать, что в сложившей обстановке нормативно-методический базис находится в стадии своего формирования. Так, анализ стандартизированной базы, содержания нормативных правовых источников и методических рекомендаций доказал актуальность разработки и (или) унификации понятий и терминов с последующим созданием на их базе единого категориального аппарата планов и стратегий в части проведения ряда работ по борьбе с проявлениями терроризма в информационной среде, иначе говоря, с киберугрозами, реализующимися в форме компьютерных атак и инцидентов информационной безопасности.

Отмечается активная работа регулятора в нынешнем году в данном направлении. Так, на официальном сайте ФСТЭК России летом 2020 г. для общественного обсуждения были размещены два проекта национальных стандартов [1, 2] (далее – проекты). Документы в идейном плане призваны сформировать основы и единую терминологию, которые обеспечат взаимопонимание между заказчиками, организаторами и исполнителями работ в области обеспечения информационной безопасности, в том числе по направлениям защиты от кибертерроризма. Регуляторы преследуют цель повышения эффективности и результативности известных мероприятий по детектированию, превенции, сдерживанию и ликвидации исходов компьютерных атак, рефлексии на компьютерные инциденты, созданию полноценного информационного обслуживания процессов управления безопасностью.

Несмотря на то, что положения проектов имеет характерную целевую ориентированность¹, многие из них заслуживают рассмотрения по своей академической сущности и актуальности для текущей обстановки динамичной борьбы с проявлениями терроризма в информационных системах, компьютерных сетях и глобальной сети Интернет.

Доводом в пользу востребованности нормотворческой проработки категориального аппарата в данном направлении можно привести данные статистики, представленные в форме аналитических отчетов некоторых известных вендоров [3, 4]. Основные тезисы о происшедших в 2020 г. кибератаках таковы.

Количество инцидентов выросло на 2,7 %. Доля целевых атак увеличилась с 63 % до 70 %. Отмечается скачок числа кибератак на организации с использованием шифровальщиков (при этом 42 % атак злоумышленники преследовали финансовую выгоду). С начала 2020 г. количество атак на промышленность держится на высоком уровне (по числу инцидентов отрасль занимает второе место, лидером продолжает быть финансовый сектор), при этом большинство атак проводилось АРТ-группировками и операторами шифровальщиков.

¹ Подразумевается ориентированность на субъектов КИИ и участников системы ГосСОПКА.

Зафиксирован всплеск атак на медицинские учреждения (половину всех инцидентов составили атаки шифровальщиков, спекулирующие данными пациентов и лишаящие больницы возможности работать, отрезая доступ к информационным системам, листам назначений и осмотров). Атакам подвергались также исследовательские центры, занимающиеся разработкой вакцины от коронавируса. Поквартальная доля кибератак с использованием методов социальной инженерии, в которых затрагивалась тема COVID-19, существенно сократилась (ранее в фишинговых рассылках предлагались средства защиты от вируса, стал эксплуатироваться интерес к вакцине).

В связи с пандемией и переходом на удаленную работу компании вывели на периметр дополнительные сервисы, которые не всегда надежно защищены. Таким образом, у преступников появилось больше возможностей для кибератак и иного проявления кибертерроризма.

Указанные данные подтверждают принципиальную значимость эшелонированной обороны и защиты от угроз различным информационным системам как частных, так и государственных организаций. Отправной точкой в данном направлении является формирование единого терминологического языка, необходимого для того, чтобы участники системы защиты информации обладали возможностями однозначного понимания современных реалий в сфере информационной безопасности и выработки единых подходов, политик и стратегий для осуществления киберзащиты.

Во избежание тривиального цитирования положений анализируемых проектов приведем сравнительную таблицу базовых терминов, изложенных в уже действующих документах нормативного и информационного характера (табл. 1).

Таблица 1

**Толкование терминов «событие» и «инцидент»
в информационной безопасности**

Источник / термин	ГОСТ Р ИСО/МЭК 27001-2006	ГОСТ Р ИСО/МЭК ТО 18044-2007	ГОСТ Р ИСО/МЭК 27000-2012	Энциклопедия Касперского
Событие информационной безопасности	Наличие или возникновение совокупности обстоятельств	Идентифицированное (выявленное) появление определенного состояния системы, сети, сервиса (услуги), указывающего на возможное нарушение политики информационной безопасности (нарушение) или отказ защитных мер (мер и средств контроля и управления) или возникновение неизвестной ранее ситуации, которая может иметь отношение к безопасности		Любое идентифицированное явление в сети или системе

Инцидент информационной безопасности	Любое непредвиденное либо нежелательное событие, может нарушить деятельность или информационную безопасность	Одно или несколько нежелательных или неожиданных событий информационной безопасности, которые со значительной степенью вероятности приводят к компрометации операций бизнеса и создают угрозы для информационной безопасности	Угроза нарушения или нарушение информационной безопасности компании
--------------------------------------	--	---	---

Определения события информационной безопасности и инцидента информационной безопасности, предлагаемые в проекте [1], незначительно отличаются:

Событие (информационной) безопасности – зафиксированное состояние информационной (автоматизированной) системы, сетевого, телекоммуникационного, коммуникационного, иного прикладного сервиса или информационно-телекоммуникационной сети, указывающее на возможное нарушение безопасности информации, сбой средств защиты информации или ситуацию, которая может быть значимой для безопасности информации.

Инцидент информационной безопасности – непредвиденное или нежелательное событие (группа событий) безопасности, которое (которые) привело (привели) к негативным последствиям для актива организации.

Отдельно приведено толкование компьютерного инцидента как факта нарушения и (или) прекращения функционирования информационного ресурса либо нарушения безопасности, обрабатываемой таким информационным ресурсом информации, в том числе произошедший в результате компьютерной атаки.

В проектах лаконично определены основные понятия в направлении борьбы с существующими киберугрозами, которые также перечислены в весьма обширном перечне. Проект отличается своей иллюстративностью в части графической интерпретации взаимосвязи терминов, что весьма положительно может сказаться на оперативном переходе лиц, реализующих положения стандарта от общей ситуационной оценки к детальному анализу содержанию стандарта.

Таким образом, регулятором предпринята попытка сформировать терминосистему, определить и упорядочить основные дефиниции в области детектирования, превенции и ликвидации исходов компьютерных атак, рефлексии на компьютерные инциденты, которые в определенных случаях могут считаться проявлениями кибертерроризма, и реагирования на компьютерные инциденты. Однако судить о результативности применяемых мер по обнаружению, предупреждению и ликвидации последствий киберугроз и деструктивного воздействия на информационные системы, о мерах по реагированию на них за счет создания единой терминологии в данной области станет возможным спустя определенное время после официального принятия проектов, введения их в действие и формирования определенных практик применения указанных документов.

Библиографический список

1. Проект национального стандарта ГОСТ Р Защита информации. Обнаружение, предупреждение и ликвидация последствий компьютерных атак и реагирование на компьютерные инциденты. Термины и определения [Электронный ресурс] // Электронный фонд правовой и нормативно-технической документации [официальный сайт]. – URL: <http://docs.cntd.ru/document/565455348> (дата обращения: 03.12.2020).
2. Проект национального стандарта ГОСТ Р Защита информации. Мониторинг информационной безопасности. Общие положения [Электронный ресурс] // Федеральная служба по техническому и экспертному контролю [официальный сайт]. – URL: <https://fstec.ru/component/attachments/download/2438> (дата обращения: 03.12.2020).
3. Актуальные киберугрозы: III квартал 2020 года [Электронный ресурс] // Positive Technologies [официальный сайт]. – URL: <https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020-q3> (дата обращения: 03.12.2020).
4. Развитие информационных угроз в третьем квартале 2020 года. Статистика по ПК [Электронный ресурс] // Лаборатория Касперского [официальный сайт]. – URL: <https://securelist.ru/it-threat-evolution-q3-2020-non-mobile-statistics/99309/> (дата обращения: 03.12.2020).

Некрасов Д. Е.¹,

*начальник кафедры уголовного права и криминологии Рязанского филиала Московского университета МВД России имени В.Я. Кикотя,
кандидат юридических наук, доцент, полковник полиции*

ДУХОВНО-ПРАВСТВЕННЫЙ КОМПОНЕНТ В ЛИЧНОСТИ РАСОВО-ЭТНИЧЕСКОГО ЭКСТРЕМИСТА И ВОЗДЕЙСТВИЕ НА НЕГО РЕСУРСОВ ИНФОРМАЦИОННО- ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ «ИНТЕРНЕТ»

Экстремистов следует относить к группе лиц, обладающих особыми негативными свойствами и качествами, проявившимися в преступном поведении (в этом случае они представлены в криминальной личности) или проявление которых потенциально возможно (в этом плане их наличие обуславливает криминогенность личности). При этом в основе экстремизма лежат мотивационные процессы, порождаемые специфическими убеждениями и установками, обуславливающие устойчивый характер направленности личности экстремиста. Указанная направленность проявляется в выражении асоциальных взглядов и готовности к совершению экстремистских актов. Поэтому лица, придерживающиеся этих убеждений, в целом являются потенциальными носителями угрозы общественной безопасности, особенно те, у которых укоренившиеся убеждения трансформировались в прочную систему установок – в экстремистский фанатизм. При этом свои внутренние убеждения данные лица демонстрируют не только совершая преступления, но и посредством элементов, входящих в особую разновидность криминогенной субкультуры (татуировок, жестов, песен, лозунгов и т. д.), распространение которой осуществляется, в том числе, с использованием информационно-коммуникационных технологий.

По механизму своего поведения, по содержанию и объему внутренних деформированных качеств экстремисты представляются весьма сложными для изучения. Среди этих составляющих особенно уникальными являются вопросы их нравственного сознания, ценностей, эмпатических проявлений в нравственных отношениях и их влияния на мотивационную направленность и действия.

На наш взгляд, ключом к проблеме является то, что экстремисты находятся на определенной социально-психологической дистанции от общества и его нравственно-правовых ценностей. В этом контексте отчужденность от общечеловеческих этнокультурных ценностей выступает общим фактором, стимулирующим определенный вектор восприятия и активности экстремиста по отношению к окружающим, обществу в целом с его требованиями, правами и ограничениями и к себе самому [1, с. 27–30].

Во многом это заложено в разных составляющих экстремистской идеологии, поэтому ее распространение крайне опасно. Наиболее распространенными являются разновидности экстремистской идеологии, масштабно проявившиеся в истории (например, фашизм и нацизм), явившие своими последствиями миллионы жертв и официально осужденные на мировом уровне. Поэтому возникает вопрос:

¹ © Некрасов Д. Е., 2020.

имеются ли вообще какие-либо составляющие нравственности в человеке, придерживающемся экстремистских взглядов? Речь идет о составляющих личности, формируемых под воздействием поступающей информации.

Сегодня ситуация приобретает более опасные характеристики, учитывая, что экстремистские взгляды, убеждения и идеология распространяются с использованием информационно-телекоммуникационной сети «Интернет». Это самая объемная информационно-смысловая среда в современном информационном обществе, формирующая знания, влияющая на представления, взгляды, идеи людей. Посредством всемирной сети адресатом экстремистской информации становится неограниченный круг лиц. Практике уже известны случаи, когда от ее восприятия до реализации в действиях проходили считанные часы.

Сегодня следует говорить об особых составляющих общественной опасности экстремизма в сети «Интернет», где он имеет организованный и публичный характер, формирует в обществе устойчивые экстремистские движения, сопровождаемые попытками их легализации, в том числе на международном уровне. Все чаще экстремистские акции преследуют цель дестабилизации социально-политической обстановки, контент сети «Интернет» становится руководством к действию. Указанное вкладывает особенные признаки в современную «цену» экстремизма, что влияет и на выбор механизмов противодействия, преимущественно уголовно-правовых.

Надо признать, что реагирование на данные факты уголовно-правовыми средствами началось относительно недавно. Так, 28 июня 2014 г. Федеральным законом №179-ФЗ в ст. 282 «Возбуждение ненависти либо вражды, а равно унижение человеческого достоинства» в содержание объективной стороны состава преступления, предусмотренного частью 1, добавлен отдельный способ: с использованием сети «Интернет». Им же в ст. 280 «Публичные призывы к осуществлению экстремистской деятельности» уточнены квалифицирующие обстоятельства: совершенные с использованием сети «Интернет». 21 июля 2014 г. Федеральным законом № 274-ФЗ в ст. 280.1 УК РФ также внесены изменения, предусматривающие ответственность за публичные призывы к осуществлению действий, направленных на нарушение территориальной целостности Российской Федерации, совершенные с использованием средств массовой информации либо электронных или информационно-телекоммуникационных сетей (включая ИТС «Интернет»). Федеральным законом от 6 июля 2016 г. № 375-ФЗ в ст. 205.2 УК РФ «Публичные призывы к осуществлению террористической деятельности или публичное оправдание терроризма» также скорректировано квалифицирующее обстоятельство: с использованием сети «Интернет».

Вне всяких сомнений, среди целей подобных изменений уголовного закона – удержание людей от совершения преступления угрозой наказания. Однако, как показывает практика, эффективность ее достижения невысокая. Дело в том, что к современным условиям, способствующим проявлениям экстремизма, также следует отнести существующие деформации индивидуальной и общественной психологии по отношению к праву, выражаемые в легкомысленном отношении к нормам права, правовом нигилизме, вплоть до проявлений правового негативизма, пренебрежения уголовно-правовыми запретами. При этом в сети «Интер-

нет» имеется контент, формирующий подобные деформации личности (например, давая ответы на соответствующие поисковые запросы: как воспользоваться тем или иным правовым пробелом, как «безнаказанно» не подчиниться законным требованиям представителя власти и т. д.).

В настоящее время к числу наиболее распространенных видов экстремистов следует относить лиц, совершающих преступления по мотивам расовой и этнической ненависти и вражды. Для экстремистов с ярко выраженной направленностью мотивов и поведения характерно замыкание на круге лиц со сходной характеристикой взглядов. Деформация социальных позиций и ролей у подобных лиц характеризуется следующими моментами: деформация внутренней нравственно-психологической сферы конкретного лица происходит под влиянием процесса изменения социализации человека, включающего усвоение им убеждений, установок, предрассудков, взглядов на жизнь и ценностей группы, проповедующей различного рода дискриминационные меры по отношению к «не своей», «чужой» национальности. При этом субъект в деянии ассоциирует себя с групповыми интересами своей социальной общности, нации и фактически, собственные деформированные духовно-нравственные стереотипы предлагает к рассмотрению «от имени» общности, к которой он относится [2, с. 101–102]. Во многом это позволяет говорить о парадоксальности такого явления как экстремизм в целом, и уникальных криминологических особенностях личности экстремиста, в частности. Информационно-коммуникационные технологии облегчили поиск «единомышленников», при этом оставаясь анонимным, не быть идентифицированным по социально-демографическим признакам, подлежащим государственному учету. Это, в свою очередь, является существенным условием для правонарушающей деятельности.

У личности, обладающей убеждениями (как положительными, так и отрицательными), имеется определенная линия поведения, устойчивость и постоянство которой во многом зависит от степени укоренения этих убеждений в сознании человека. При этом формирующиеся у личности экстремистские убеждения могут сказаться на ее поведении далеко не сразу. Может пройти немалое количество времени, пока накапливающаяся «асоциальная энергия», «пораженная» область сознания личности, в виде совокупности взглядов, мнений и т.д., выльется в конкретный поступок. Во многом это будет зависеть от субъективных факторов и особенно от стимулирующего мотива, побуждающего к определенным действиям. В любом случае, степень готовности личности к экстремистским проявлениям будет тем выше, чем более устоялись соответствующие убеждения и окрепла уверенность человека в их состоятельности и необходимости придерживаться и следовать им.

Важно не допустить формирования у личности экстремистских убеждений, по своей сущности являющихся продуктом крайне искаженной психологии и мировоззрения в области восприятия и соблюдения норм человеческого поведения. Отметим, что соответствующие убеждения, как и общая направленность личности, определяются потребностями и интересами, которые также складываются в ходе формирования личности [3, с. 96–115]. Антиобщественные потребности и интересы уже сами по себе могут привести к выбору формы поведения,

запрещенной законом и противоречащей нормам морали. В свою очередь, имеющиеся криминальные убеждения, в частности экстремистские, могут выступить в роли катализатора и фиксатора подобного выбора.

К сожалению, многие факторы, существующие в современной действительности, способны породить или способствовать порождению деформированных потребностей и интересов. В современном обществе продолжаются изменения в характере мышления и образе жизни. Многие существовавшие традиции, идеи и взгляды утрачиваются, в том числе под влиянием сети «Интернет».

Так, среди состояний массового сознания можно выделить фрустрацию, вакуум, утрату смысла жизни у некоторых представителей общества, что в свою очередь порождает социально опасные формы мышления, в том числе и деформированные взгляды на межэтнические отношения. Подобные социально-психологические явления привели к тому, что к настоящему времени в обществе проявляются несколько центров некой субъективной активности вместе с продуцируемыми ими типами жизни. Каждый из них имеет свое поле притяжения разнородных сил. Взаимодействуя между собой, образуя сочетания разных типов жизнедеятельности, они формируют определенные, вполне выявляемые черты личности, мотивации, потребности, образцы восприятия и отношения к миру. Одним из таких центров активности авторам и видится экстремизм. Еще в начале 2000-х годов, специалисты отмечали, что экстремистское мироощущение продолжает проникать в массовое сознание, овладевая образом жизни все большего числа людей [4, с. 16].

В контексте рассматриваемой проблемы, основной аспект массового влияния сети «Интернет» на личность, на наш взгляд, заключается в наличии в ней информации, прямо или косвенно создающей у человека негативное восприятие лиц, отличающихся по каким-либо социальным признакам или связанных с ними явлений, а также выражающей неуважение к ним, чаще всего на расово-этнической почве. При публичном характере этот контент следует относить к разновидности экстремистских материалов, определение которых в качестве таковых в соответствии с изменениями, внесенными Федеральным законом от 28 ноября 2018 г. № 451-ФЗ, осуществляется в соответствии с гл. 27.2 Кодекса административного судопроизводства Российской Федерации (КАС РФ).

Разумеется, особую опасность такие материалы представляют для сознания личности несовершеннолетнего. Суть указанного воздействия видится в направленном, а иногда и завуалированном информационном влиянии, следствием которой становится принятие даже ранее неизвестных интересов, взглядов, переосмысление перспектив, ценностей, отношения к некоторым объективно необходимым составляющим социума (этносам, расам и их элементам, признакам).

Полагаем, что в целом опасность подобных материалов заключается в том, что в зависимости от степени влияния на личность они либо побуждают экстремистские настроения, либо формируют или укрепляют экстремистские взгляды. Таким образом, они обладают криминогенным воздействием, играют немаловажную роль в структуре детерминант криминогенной мотивации, как в непосредственном ее развитии, так и в формировании конкретного побуждения к преступлению экстремистского характера [5, с. 117–118].

К сожалению, сегодня у некоторых представителей, прежде всего, лиц несовершеннолетнего и молодежного возраста, наблюдается либо недостаточное получение и закрепление необходимых социальных стереотипов, либо их искаженное восприятие. Между тем подобные пробелы у личности могут заполняться антиобщественными установками, в том числе и экстремистскими. Ситуация осложняется тем, что в последние годы многие экстремистские акции направлены на призыв неограниченного круга лиц к осуществлению соответствующих действий, на пополнение своих рядов новыми членами, носят пропагандистский характер.

Высоконравственная личность, обладающая правильными представлениями о правилах человеческого общежития, о важности обеспечения должного уровня организации общественных отношений, правомерных механизмах участия в них, менее склонна к восприятию и усвоению экстремистских взглядов и убеждений. Поэтому всестороннее нравственное воспитание личности следует относить к элементам, составляющим профилактику экстремизма.

Таким образом, причины и условия, проявлений крайних взглядов в области расово-этнических взаимоотношений и равноправия, формируемые посредством сети «Интернет», действительно являются значимыми в общем причинном комплексе обозначенного явления, в первую очередь в силу его преимущественной сущности, лежащей в плоскости массового сознания, психологических аспектов. Однако рассмотренные причины и условия взаимосвязаны с иными причинами, в том числе социально-экономического, политического, организационно-управленческого, воспитательного и правового характера. Осуществляя разработку и применение соответствующих профилактических мер, необходимо учитывать подобную комплексность и специфичность разнообразных детерминант расово-этнического экстремизма и его связь с иными негативными явлениями.

В заключение необходимо отметить, что необходимость наличия у субъектов противодействия экстремизму глубоких специальных познаний относительно природы, сущности и видов этого явления, осуществления специализированных мероприятий, направленных на предупреждение, раскрытие и расследование преступлений экстремистского характера предопределяет организацию специального обучения, также требующего соответствующих ресурсов педагогического и научного плана.

Библиографический список

1. Кораблев, С. Социально-психологические особенности личности носителей экстремистского мировоззрения / С. Кораблев // Профессионал: популярно-правовой альманах МВД России. – 2015. – № 6. – С. 27–30.
2. Абдуллаева, Э. С. Возбуждение ненависти либо вражды, а равно унижение человеческого достоинства (уголовно-правовой и криминологический анализ): дис. ...канд. юрид. наук. – Махачкала, 2004.
3. Кудрявцев, В. Н. Причины правонарушений. – М. : Наука, 1976. – 286 с.
4. Козлов, А. А. Феномен экстремизма. – СПб.: Изд-во СПбГУ, 2000. – 85 с.
5. Некрасов Д. Е. Расово-этнический экстремизм: криминологический аспект: дис. ... канд. юрид. наук. – Рязань, 2006. – 28 с.

*Гулевский А. Н.¹,
доцент кафедры философии
Волгоградской академии МВД России,
кандидат философских наук, доцент*

О НЕНАСИЛЬСТВЕННЫХ МЕТОДАХ БОРЬБЫ С ТЕРРОРИЗМОМ

Развитие информационных технологий, как и любых других, создает поле возможностей в политическом пространстве. Не секрет, что технический прогресс не столько несет обществу мирную жизнь, сколько порождает новые риски и угрозы безопасности. Изобретение динамита и других компактных взрывоопасных смесей способствовало росту терроризма в мире не меньше, а может и больше, чем наличие национальных или религиозных противоречий. Развитие информационных систем дало терроризму еще один мощный толчок. Теперь компактное оружие стало не только мощным, но и «умным», управляемым дистанционно, как, например, беспилотные летательные аппараты малого размера. Оружие научилось получать и даже анализировать информацию и самостоятельно принимать решения. Появление в руках террористов в будущем малоразмерного ядерного оружия поставит мир в затруднительное положение. Немалую помощь терроризму оказывают и новые возможности демонстрировать преступления в информационном пространстве, что позволяет популяризировать свою деятельность и запугивать мирных граждан, раздувая масштабы своих действий в сознании тех, кто смотрит новости или выложенные в интернете видео.

Разумеется, современные информационные технологии позволяют также и правоохранительным органам вести охоту за террористами, отслеживая их сообщения, перехватывая разговоры, исследуя интернет-пространство на предмет поиска вербовщиков и проповедников экстремизма и терроризма. Схватку выигрывает тот, кто более качественно подготовлен технически, организационно и морально, однако в этой борьбе, ведущейся жесткими силовыми методами, трудно победить окончательно, если кто-то извне продолжает, как из рога изобилия вкачивать средства в распространение терроризма. Исходя из этого, необходимо осознать, важность использования других, альтернативных полей на доске этой древней борьбы. Уже довольно давно говорят о действии так называемой «мягкой силы», под которой американский политолог Д. Най понимает достижение целей благодаря добровольному участию, симпатии, привлекательности. Иными словами в нашем случае важно сделать так, чтобы выбор человека в пользу экстремизма и терроризма стал непривлекательным, несимпатичным, и он добровольно и сознательно стремился бы к другому выбору – стать законопослушным гражданином. Выбор человека зависит от множества обстоятельств и повлиять на то или иное решение значит, по сути, предотвратить, упредить возможную ошибку. Речь идет не только о профилактике преступлений и правонарушений, которая в настоящее время утратила у нас то значение и действенность, что были в СССР, и которую необходимо возрождать и использовать, но и о более широком круге проблем.

¹ © Гулевский А. Н., 2020.

Проблема борьбы с терроризмом имеет не только техническую, но и идейную основу. Борьба с этим опасным явлением должна вестись не только вооруженным путем, но и на уровне формирования мировоззрения населения. Ряды террористов формируются из числа наших собственных граждан, значит, следует признать, что хотя бы в определенной мере это недоработка нашей внутренней политики. В борьбе с терроризмом необходимо препятствовать информационному воздействию на наше население, противодействовать его вербовке и тем самым уменьшить число потенциальных террористов.

Разумеется, определенная работа в этом направлении уже ведется. В социальных сетях ведется антитеррористическая пропаганда, создаются телепередачи и блоги с участием популярных людей, осуждающих проявления терроризма, СМИ подключаются к освещению деятельности террористических организаций в негативном свете, осуществляется популяризация терпимости к иным культурам, проходят патриотические акции, по типу Бессмертного полка, акции, посвященные Дню Победы или Дню России и т. д.

Все эти мероприятия вносят вклад в дело противодействия экстремизма и терроризма, но являются бессистемными, непостоянными, неуниверсальными, а потому скорее симптоматическими мерами. Так, телепередачи на одну и ту же тематику постепенно утрачивают популярность и поддержку рекламы, блоги могут появляться и исчезать по разным причинам, а новая коронавирусная инфекция способна повлиять на отмену любых массовых мероприятий. Важно также отметить, что они собирают, как правило, тех, кто уже сочувствует и симпатизирует своему государству и желает помочь власти в его управлении. Те, кто не доверяет своему правительству и обижен или недоволен своим социальным положением, такие мероприятия не посещает, программы, и передачи не смотрит или уходит в другие, альтернативные информационные ресурсы.

К главной группе риска, подвергающейся наиболее сильному вредоносному информационному воздействию, следует отнести молодежь. Именно ее используют в качестве ударной силы различные экстремистские и террористические организации. Люди старшего возраста, как правило, прошли через систему советского обучения и воспитания или имеют постоянный доход, семью, дом, и им не хочется этим рисковать. Молодежь – это самое слабое место, которое мало чем в настоящее время укреплено. Нужно признать, что, по сути, в России нет какой-то внятной хорошо продуманной, перспективной, молодежной и детской политики.

В СССР существовали, к примеру, пионерские и комсомольские организации, продуманная система воспитания будущих советских граждан. Вместе с крушением коммунистической идеологии ничего похожего по функциям в России создано не было. В деидеологизированном обществе прежние ценности и идеалы утратили свое значение и превратились в нечто отжившее и ненужное. Вместо них провозглашался навязанный извне культ свободы, индивидуализма и материальных ценностей. Общество лишилось прежней заботы и опеки со стороны государства, которое в новой России должно было, как можно меньше вмешиваться в личное пространство и жизнь индивидуума. Свобода трактовалась как вседозволенность. Прежние моральные ценности были подорваны. Как след-

ствие – массовое нарушение закона, рост преступности, формирование преступных организаций и сообществ, в том числе террористических. Одни желали украсть миллион, а другие – оторвать целую республику, причем на попытку осуществить последнее давались щедрые деньги геополитическими противниками России. Коллективные ценности были подвергнуты обструкции из-за коммунистического прошлого, а ценность индивида не подразумевала идею создания большого и сильного государства, она проповедовала простой и быстрый способ личного обогащения по принципу «рви и беги». Парад суверенитетов, разгул преступности, формирование экстремистских организаций стали следствием нашей собственной непродуманной внутренней политики. И если в настоящее время большинство указанных выше факторов были осмыслены и купированы, то проблема воспитания молодежи остается актуальной и нерешенной.

Еще в 90-е гг. 20 в. в России был нанесен мощный удар по гуманитарному образованию, которое стало ненужным и неважным для будущего гражданина страны. Многие при этом задавали резонный вопрос, зачем изучать историю и культуру своей страны или познавать философские теории. Действительно, чтобы зарабатывать деньги, эти знания не очень помогут. В итоге профессия учителя и преподавателя гуманитарных дисциплин стала низкооплачиваемой и непопулярной, чем-то вроде хобби. В то же время гуманитарные дисциплины несут важное для граждан мировоззренческое и воспитательное значение, в котором заинтересовано правительство, так как это именно его масштаб видения и сфера интересов. В то же время, как справедливо отмечает С. В. Дашкова, для террористической идеологии характерно «искаженное восприятие действительности вплоть до его отрицания; радикальность во взглядах и экстремальность выбора способов действий; фанатизм, одержимость какой-либо идеей; утопизм и абсолютная вера в достижимость поставленных целей; мифологичность сознания, угрозо-ориентированное восприятие мира; дуализм, поляризация («мы против них»), восприятие «Другого» в образе «Врага»; бескомпромиссность, крайняя нетерпимость к оппонентам, стремление навязать им свои ценности; – догматизм, притязание на полное и исключительное обладание истиной» [1, с. 143]. Таким образом, у приверженцев террористической идеологии особый тип мировоззрения, понимания и восприятия окружающего мира. Этот тип мировоззрения формируется в определенных условиях, при помощи определенных методов, приемов. Мифологическое сознание свойственно, как правило, людям, не имеющим светского высшего образования, не изучавшим естественные науки и философию, которая показывает, что мифология есть форма мировоззрения, свойственная первобытным, а не современным обществам. Фанатичная одержимость, какой-либо идеей и утопизм говорят о несформированности критического мышления, неумении подвергать сомнению выводы других людей, неумении мыслить самостоятельно, основываясь на собственном опыте и построении собственных выводов. Радикальность взглядов говорит о неумении слушать оппонента и извлекать нечто рациональное из его доводов, непонимании того, что мир сложен и простые или радикальные решения не могут быть объективными и общезначимыми. Восприятие «Другого» в образе «Врага» говорит, что нет понимания того, что мыслящий иначе, чем мы, не обязательно враг, но возможно,

будущий друг, помощник, учитель, ученик или оппонент в дискуссии. Догматизм и притязание на полное и исключительное обладание истиной говорит о том, что носители такого мировоззрения не знакомы с философскими теориями истины, не знают критериев истинного знания и не осознают того, что большинство истин носят относительный характер, что исчерпывающее и всестороннее знание о мире недостижимо в реальности и служит скорее идеалом и т. д. Бескомпромиссность и нетерпимость говорит о том, что человек не имеет навыков социального общения и диалога, не понимает того, что успех в современном поликультурном обществе невозможен без уступок и проявления терпения к инакомыслящим. По сути, носитель подобного экстремистского мировоззрения не смог бы сдать экзамен по философии, этике, логике, религиоведению, если бы попытался их сдать объективно. Так, например, идея превосходства одной религии над другой могла и должна была пресекаться на занятиях религиоведением. Идея неразрывного единства религии и политики – политологией и историей. В школах курсы обществознания и истории также должны формировать на начальном этапе подобное мировоззрение. Однако в действительности реализация гуманитарных курсов осуществляется достаточно формально. Времена СССР, когда несдача экзамена по научному коммунизму или марксистско-ленинской философии грозила весьма серьезными последствиями для студентов или, тем более, курсантов, а непринятие в пионеры было позором для школьника, канули в лету. Вместе с крушением идеологической системы произошел и обвал того, что называется формированием мировоззрения молодежи. Демократизация открыла дорогу лжи, мракобесию, радикализму и прочему в рамках инакомыслия, которое стало чем-то важным и защищаемым. Именно в это время начался и процесс фальсификации истории. Либерализация проникла во все сферы жизни через поощрение аморального, культ насилия, внедрение в сознание идей индивидуализма, прав человека, которые стали выше интересов общества и государства. В таких сложившихся условиях воспитание молодежи, забота о формировании ее мировоззрения стала уделом лишь семьи и, по сути, устранена от государственных забот. Ректора некоторых вузов России сокращают курсы философских и исторических дисциплин, считая, что их выпускникам нужно больше знаний узкопрофессиональной направленности, не понимая, что без формирования мировоззрения невозможно сформировать ни облик патриота, ни рационально мыслящую, ни моральную или как минимум социально ориентированную личность. В то же время безнравственность видится основной причиной совершения преступления. Работа с молодежью представляет собой то поле, которое упускается из виду нашими политиками. В то же время тревожные звонки уже прозвучали на Украине во время майдана и в Белоруссии во время выборов в 2020 г. Как справедливо отмечает Е. А. Матвиенко, не все можно взвалить только на плечи силовых органов, и «главная битва разворачивается сегодня в информационном пространстве, идет сражение за души людей, и прежде всего – за души молодых людей (причем, как показывает практика, отнюдь не только «мусульман по рождению»)» [2, с.183]. Террористы в Сирии, террористы-смертники в России – это в массе своей молодежь. В эпоху современной информационной цивилизации такой подход не выдерживает критики, ибо развитие

коммуникационных систем позволяет управлять как отдельными индивидами, так и толпой через мобильные сети, посредством дезинформации.

Следует помнить, что обеспечение безопасности государства невозможно ограничивать лишь укреплением вооруженных сил новой техникой и подготовкой к войне. Конфликты будущего имеют тенденцию перехода в область чисто информационную, посредством влияния на сознание, интеллект, способность управлять совершением выбора, посредством определенных манипуляций в информационном пространстве. Холодная война не закончилась, она будет вестись против нас и основной ее смысл в том, чтобы атаковать наши слабые поля, которые мы сами и предоставляем. В то же время терроризм – это «прежде всего война, ведущаяся незаконными, преступными средствами» [3, с.98]. Победить в такой войне можно тогда, когда в государстве есть как можно больше ответственных, законопослушных, патриотично настроенных, интеллектуально развитых граждан, стремящихся созидать новое ради своей страны, а не просто потребляющих продукты чужих культур и восхищающихся этими культурами.

Когда О. Бисмарк говорил, что народное образование играет решающую роль в войнах и что школьный учитель одного государства побеждает в войне школьного учителя другого государства, он имел в виду как раз то, что именно образование выковывает из молодежи кадры, способные к борьбе за свою Родину. Х. К. Мольтке развил идею О. Бисмарка, указав, что не просто образование, но воспитание побеждает в войне, так как одним знанием нельзя привести человека к той высоте, которая позволит ему смело пожертвовать своими интересами ради своей Родины, идеалов и принципов, заложенных в культуре своего народа.

Библиографический список

1. Идеология современного терроризма / С. В. Дашкова // Вестник Калмыцкого университета. – 2017. – № 1. – С. 141–148.
2. Исламский радикализм как глобальная проблема современности / Е. А. Матвиенко // Вестник Волгоградской академии МВД России. – 2015. – № 4. – С. 179–184.
3. Терроризм как современная форма войны: социально-философский анализ : монография / А.Н. Гулевский. – Волгоград: Волгоградская академия МВД России, 2016. – 168 с.

*Левандовская М. Г.¹,
доцент кафедры уголовного права
Московского государственного юридического университета
имени О.Е. Кутафина (МГЮА),
кандидат юридических наук, доцент*

ВОВЛЕЧЕНИЕ В ТЕРРОРИСТИЧЕСКУЮ ДЕЯТЕЛЬНОСТЬ С ИСПОЛЬЗОВАНИЕМ СОЦИАЛЬНЫХ СЕТЕЙ

Социальные сети – это те сферы взаимодействия людей, которые пользователями идентифицируются как область, предназначенная для общения в группах и сообществах, иных формах обмена информацией и идеями, мнениями, инкогнито или с использованием своих персональных данных (имен и фамилий).

Безусловно, они отличаются тем, что их контент создают непосредственно сами пользователи сетей. Сети очень разнообразны по своей сути, так как являются IT-сервисами, как, например:

- WhatsApp и Viber;
- социальные сети «ВКонтакте» и «Одноклассники».

Их особенности порождает их разнообразие. Однако есть и общее свойство – они формируются и создаются путем выкладывания контента их авторов.

В настоящее время кодифицированный нормативный акт, непосредственно регулирующий деятельность социальных сетей в Российской Федерации, не принят. Существует лишь проект² федерального закона № 145507-7, но дата введения его в действие до сих пор неизвестна.

В то же время в российской правоприменительной практике имеются отдельные положения, напрямую касающиеся деятельности социальных сетей. К примеру, Минпросвещения России письмом от 29.03.2019 № 03-393 направило Методические рекомендации по реализации мер, направленных на обеспечение безопасности детей в сети Интернет. В указанных Рекомендациях, в частности, поисковым системам рекомендуется исключить из результатов поиска персональные данные детей в форме ссылок на аккаунты в социальных сетях.

В остальном социальные сети, равно как и иные распространители информации, обязаны руководствоваться законодательством Российской Федерации об информации и информатизации.

Рассмотрим вопросы вовлечения в террористическую деятельность с их помощью и существующие проблемы в указанной области.

Проблематика раскрытия и расследования преступлений террористической направленности отчетливо прослеживается, если разделить их на явные и конспиративные. К явным следует отнести те преступления террористической направленности, объективную сторону которых составляют действия публичного характера. Конспиративные – это преступления террористической направлен-

¹ © Левандовская М. Г., 2020.

² Проект Федерального закона № 145507-7 «О правовом регулировании деятельности социальных сетей и внесении изменений в отдельные законодательные акты Российской Федерации» // КонсультантПлюс. – URL: <http://www.consultant.ru>.

ности, которые характеризуются тайным, подпольным характером преступной деятельности. Это, например, преступления, предусмотренные ст. 205.1 «Содействие террористической деятельности» Уголовного кодекса Российской Федерации [1] (далее – УК РФ) и др. Отметим имеющиеся в рассматриваемой тематике проблемные положения, например, терминологического характера.

Значения терминов «социальная группа», «склонение», «вербовка» и «иное вовлечение» не только вызывают сложности в доказывании, но и являются основной причиной разрозненности судебной практики по такого рода делам. Уточнение значения первого из этих терминов прошло путь от обобщения судебно-экспертной практики [2] до подачи многочисленных жалоб в Конституционный Суд Российской Федерации. Рассмотрение этих жалоб закончилось не в пользу заявителей.

Анализ разъяснений Верховного Суда Российской Федерации также не проясняет ситуацию с терминологической неопределенностью. В постановлении Пленума Верховного Суда Российской Федерации от 9 февраля 2012 г. № 1 [3] дается следующее разъяснение:

«При рассмотрении судами уголовных дел о преступлениях, предусмотренных статьей 205.1 УК РФ, под склонением, вербовкой или иным вовлечением определенного лица (группы лиц) в совершение хотя бы одного из преступлений, перечисленных в ч. 1 ст. 205.1 УК РФ, следует понимать, в частности, умышленные действия, направленные на вовлечение определенного лица (группы лиц) в совершение одного или нескольких указанных преступлений, например, путем уговоров, подкупа, угрозы, убеждения, просьб, предложений (в том числе совершенные посредством размещения материалов на различных носителях и распространения через информационно-телекоммуникационные сети), применения физического воздействия или посредством поиска лиц и вовлечения их в совершение хотя бы одного из указанных преступлений».

Резюмируя, Верховный Суд Российской Федерации не разграничивает содержание терминов «склонение», «вербовка» и «иное вовлечение», оставляя правоприменителям чрезмерную широту усмотрения, особенно при привлечении к ответственности за некое «иное вовлечение».

Еще один проблемный вопрос: неподготовленность правоохранительных органов к производству по данной категории дел.

Даже по делам о явном терроризме, когда публикация материала террористической направленности была осуществлена в сети Интернет, правоприменители сталкиваются с проблемами доказывания обстоятельств на виртуальном месте происшествия, когда все следы преступления представляют собой компьютерную информацию. Это является общей проблемой правоприменительной практики по делам о преступлениях в сфере компьютерной информации, причины которой связаны с неумением применять метод моделирования.

Расследование преступления террористической направленности, совершенного в сети Интернет, как раз и представляет собой ситуацию для моделирования, [6. С. 124].

Если же речь идет о доказывании по делам о конспиративном терроризме (например, исследование переписки в социальных сетях с призывом вовлечения

в деятельность террористической организации), то ключевое место в процессе доказывания занимает использование специальных знаний при производстве судебных экспертиз и привлечении специалиста.

К сожалению, взаимодействие с компетентными лицами и без того вызывает у правоприменителей сложности, а по делам о преступлениях террористической направленности нередко становится неразрешимой проблемой.

Отчасти второй вопрос связан с первым, поскольку сложности в доказывании часто вызывает необходимость назначения экспертиз для установления, например, терминологически неопределенных обстоятельств склонения / вербовки / иного вовлечения.

Под вовлечением понимается общее понятие, включающее склонение, вербовку и иные действия. Вовлекать – побуждать, привлекать к участию в работе, деятельности. Вербовка (наем) – вовлечение:

- 1) путем обещания платы;
- 2) в систематическую деятельность по поиску новых участников;
- 3) поиск лица для совершения конкретного преступления.

Вовлечение путем склонения непосредственно связано с механизмом убеждения, побуждения к преступной деятельности. Для установления фактических обстоятельств по делам, связанным с вовлечением путем склонения, важно ставить нижеуказанные вопросы.

1) Имеются ли в представленном материале (тексте, фонограмме, песне, клипе и проч.) высказывания, направленные на побуждение кого-либо (участника зафиксированных переговоров) к чему-либо (приводится описание элементов объективной стороны состава)?

2) Если да, то в какой форме выражена информация в этих высказываниях? Данный вопрос следует ставить для того, чтобы конкретизировать способы речевого (в виде, например, звукового сообщения в социальной сети) или иного информационного воздействия на адресата высказывания, например: просьба, предложение, призыв, угроза и т. д.

Иное вовлечение охватывает психическое и физическое воздействие с целью возбудить желание совершить преступление террористической направленности, при этом оно не связано с вербовкой либо склонением.

И если факт физического принуждения доказывается путем назначения судебно-медицинской экспертизы и какой-либо специфики по данной категории дел не имеет, то для проверки версии о психическом принуждении помимо типовых вопросов к эксперту-психологу следует формулировать еще и вопросы к эксперту-лингвисту, например:

1) Содержатся ли в представленном тексте из социальной сети сведения, направленные на возбуждение желания совершить такие-то действия (например, погром, избиение и проч.)?

2) Если да, то каковы лингвистические характеристики этих сведений?

По нашему мнению, перекося правоприменительной практики связан с направленностью противодействия только на самые явные проявления терроризма. Они не вызывают проблем в расследовании и доказывании в суде, а также формируют положительную динамику раскрываемости.

Отметим опасность вовлечения в отдельные подвиды терроризма. Так, значительное количество материалов террористического характера в социальных сетях часто очень сложно отличить от материалов, содержание которых направлено на распространение религиозных воззрений мирного характера.

Например, при выявлении пропаганды исключительности, необходимо различать пропаганду исключительности самой религии и пропаганду исключительности качеств людей, исповедующих эту религию. Первый случай имеет место в подавляющем большинстве религиозных текстов и составляет важную особенность религиозного дискурса (проповедческое начало): «Только мы знаем правду! Только наша вера истинная!». Во втором случае имеет место гиперидентичное отношение к представителям других религий, читателя убеждают в неполноценности всех остальных. Например: «Представители определенной религии – самые порядочные, честные люди». Учитывая вышеизложенное, полагаем, что следует критически оценивать тезис о том, что «в религии нет экстремизма (как проявления терроризма)» [7. С. 290-291].

Очевидно, что разрешение вопроса о наличии в религиозных текстах социальных сетей признаков, свидетельствующих о присутствии в высказываниях формы призывов, негативной оценки, направленности на унижение чести и умаление достоинства, на возбуждение розни и проч., нередко представляет собой сложную лингвистическую задачу, основывающуюся на нормативно-правовых предписаниях, так как часть вопросов прописывается в методиках экспертного исследования, например, вопрос о наличии или отсутствии признаков, описанных нормативно-правовым текстом.

В вопросах же правовой квалификации общественно опасного терроризма религиозной направленности следует учитывать следующие обстоятельства:

- применение насилия;
- осуществление противоправной деятельности, направленной на слом существующего политического режима;
- пропаганда нетерпимости и практика реализации подобных убеждений в политической жизни;
- сущностный антидемократизм, антиплюрализм, отрицание прав и свобод человека.

Исходя из анализа существующей судебной практики можно утверждать, что в социальных сетях вовлечение в террористическую деятельность начинается с оправдания терроризма.

Ярким иллюстрирующим примером этому является Апелляционное определение Судебной коллегии по делам военнослужащих Верховного Суда Российской Федерации от 16.01.2020 № 225-АПУ19-5 [4], согласно которому Калинин И.Г. был осужден за публичное оправдание терроризма, совершенное с использованием информационно-телекоммуникационной сети «Интернет». Это было установлено судом и подтверждалось как свидетельскими показаниями, так и заключением лингвистической экспертизы.

По нашему мнению, размещенная обвиняемым информация являлась особенно опасной, так как находилась в свободном для неограниченного круга пользователей социальной сети доступе.

Таким образом, следует сделать промежуточный вывод об особой общественной опасности использования социальных сетей с целью пропаганды террористической деятельности.

Приведенный нами пример показал, что распространение незаконной информации осуществилось буквально мгновенно, набрав 68 просмотров. Особенно негативным является то, что кто-то из просмотревших лиц поставил «лайк», одобряя и поддерживая подобную деятельность.

Вместе с тем, можно говорить о том, что многие лица активно вовлекают иных граждан в террористическую деятельность.

Согласно Апелляционному определению Судебной коллегии по делам военнослужащих Верховного Суда России от 14 января 2020 № 225-АПУ19-4 [5], Водянский С. А. признан виновным в публичном оправдании терроризма в социальной сети «ВКонтакте», совершенных в пос. Озеро Учум Ужурского района и в г. Ужур Красноярского края путем размещения 29 апреля, 4, 13 и 14 мая, 14 и 22 июля, 10 и 13 августа 2018 г. посредством имеющихся у него в пользовании мобильного телефона «НТС» и ноутбука «НР» на созданной им в социальной сети «ВКонтакте» персональной странице <...>, открытой для свободного доступа неограниченному кругу лиц, фотографий, текстовых комментариев и сообщений, призывающих к осуществлению террористической деятельности и оправдывающих терроризм, а также в незаконном хранении с 4 часов 40 минут до 8 часов 29 января 2019 г. в своем жилище в г. Ужур Красноярского края огнестрельного оружия – обреза гладкоствольного охотничьего одноствольного ружья 16 калибра модели ИжК.

В процессе судебного разбирательства обвиняемый пытался избежать наказания, выражая несогласие с выводом суда об отсутствии необходимости в получении судебного решения по причине открытого доступа к своей личной странице в социальной сети, поскольку такой доступ ограничен участниками данной сети и невозможен для других пользователей, к тому же в материалах дела отсутствуют сведения о том, что оперативный сотрудник, проводивший ОРМ, являлся пользователем социальной сети «ВКонтакте».

Вина в совершении действий по вовлечению в террористическую деятельность и призывов к ней подтверждена нижеследующими доказательствами:

- протоколами получения компьютерной информации от 14 сентября 2018 г., согласно которым на персональной странице пользователя «А.» социальной сети «ВКонтакте» обнаружены материалы, подтверждающие размещение названным пользователем 29 апреля, 4, 13 и 14 мая, 14 и 22 июля, 10 и 13 августа 2018 г. фотографий, текстовых комментариев и сообщений, призывающих к осуществлению террористической деятельности и оправдывающих терроризм;

- сведениями из ПАО «Мегафон» о принадлежности Водянскому абонентского номера и о его соединениях;

- протоколом осмотра документов от 18 января 2019 г., согласно которому Водянскому с указанного абонентского номера 29 апреля, 4, 13 и 14 мая, 14 и 22 июля, 10 и 13 августа 2018 г. предоставлялись соединения с ИТС «Интернет» и он пользовался персональной страницей социальной сети «ВКонтакте»;

– сообщением ООО «ВКонтакте» об отсутствии несанкционированных входов на персональную страницу «А.» и обращений пользователя с жалобами или заявлениями по данному вопросу;

– показаниями Водянского о принадлежности ему страницы в социальной сети «ВКонтакте» под названием «А.», о ежедневном посещении им этой страницы с принадлежащих ему мобильного телефона и ноутбука, об отсутствии случаев взлома его страницы, о нахождении ключей от квартиры, где в его присутствии был обнаружен обрез охотничьего ружья, с декабря 2018 г. только у него, а также о предполагаемом характере его суждений о том, что уголовное преследование обусловлено его отношением к религии;

– показаниями свидетелей М. и З. о свободном доступе на личную страницу пользователя «А.» в социальной сети «ВКонтакте», который под фотографией вооруженного мужчины, находящейся в новостной ленте одного из сообществ, разместил свои комментарии о необходимости перечисления денег по номеру банковского счета в целях оказания помощи религиозным «братьям», убывающим на войну и стремящимся стать шахидами, а на его странице имелись записи с негативными высказываниями против русских, агрессивными призывами убивать «неверных», вести «джихад» в России и оправдывающие деятельность «братьев из Исламского государства»;

– показаниях свидетеля З. (псевдоним), допрошенной о ее знакомстве с Водянским, который в социальной сети «ВКонтакте» использовал имя «А.», а на личной странице, свободной для доступа других лиц, размещал записи о войне мусульман («джихаде»), негативные высказывания про русскую нацию и лиц, не исповедующих ислам, призывы к их уничтожению.

На телефонные звонки свидетелю всегда отвечал Водянский и только он пользовался страницей «А.».

Также свидетель подтвердила приверженность Водянского идеологии радикального ислама, поскольку он оправдывал и поддерживал деятельность террористической организации «ИГИЛ» и идеи терроризма, высказывал намерение уехать в Сирию для участия в боевых действиях на стороне указанной террористической организации.

Также в процессе доказывания вины осужденного в том, что он целенаправленно занимался вовлечением в террористическую деятельность с использованием социальной сети «ВКонтакте», использовались иные свидетельские показания и заключение комплексной психолого-лингвистической судебной экспертизы, которая установила, что обвиняемый занимался побуждением мусульман к насильственным вооруженным действиям над лицами, не исповедующими ислам, в том числе над русскими, к участию в вооруженной борьбе в целях изгнания их с территории «земель Халифата» и уничтожения, т. е. по признаку национальной принадлежности и отношения к религии, обоснование необходимости вооруженной борьбы и физического уничтожения русских и немусульман, создания халифата в России, победы над «неверными» на территории России и Сирии, им пропагандировалась и оправдывалась террористическая деятельность, идеи и цели террористической организации «Исламское государство», а также

действия «шахидов», он побуждал к финансированию «джихада» посредством перечисления денег на указанный пользователем банковский счет.

К сожалению, с материалами и призывами террористического характера Водянского ознакомилось большое количество пользователей: с материалами, размещенными 29 апреля, 4, 13 и 14 мая, 14 июля и 10 августа 2018 г., ознакомилось в каждом случае более 100 человек, с размещенными 22 июля 2018 г. материалами ознакомилось 73 пользователя, а 13 августа 2018 г. – 23 пользователя.

Таким образом, в завершение следует еще раз подчеркнуть опасность несвоевременного выявления описанной противоправной деятельности в социальных сетях, поскольку вовлечение в террористическую деятельность с использованием социальных сетей нами оценивается как преступление особой общественной опасности.

Библиографический список

1. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (ред. от 30.12.2020) // СПС «КонсультантПлюс». – URL : http://www.consultant.ru/document/cons_doc_LAW_10699.
2. Определение Конституционного Суда Российской Федерации от 27 июня 2017 г. № 1411-О «Об отказе в принятии к рассмотрению жалобы Носика Антона Борисовича на нарушение его конституционных прав статьей 282 Уголовного кодекса Российской Федерации» // СПС «Консультант Плюс». – Режим доступа: по заказу документа.
3. Постановление Пленума Верховного Суда Российской Федерации от 9 февраля 2012 г. № 1 (ред. от 03.11.2016) «О некоторых вопросах судебной практики по уголовным делам о преступлениях террористической направленности» // СПС «КонсультантПлюс». – URL: http://www.consultant.ru/document/cons_doc_LAW_125957.
4. Апелляционное определение Судебной коллегии по делам военнослужащих Верховного Суда Российской Федерации от 16.01.2020 № 225-АПУ19-5 // СПС «Консультант Плюс». – Режим доступа: по заказу документа.
5. Апелляционное определение Судебной коллегии по делам военнослужащих Верховного Суда Российской Федерации от 14.01.2020 № 225-АПУ19-4 // СПС «Консультант Плюс». – Режим доступа: по заказу документа.
6. Волчецкая, Т. С. Криминалистическая ситуалогия / под ред. Н. П. Яблокова. – М. ; Калининград, 2016. – С. 124.
7. Лаза, В. Д. Корни и профилактика религиозного экстремизма // Вестник Пятигорского государственного лингвистического университета. – 2008. – № 2. – С. 290–291.

Федосеева О. И.¹,

доцент кафедры психологии и педагогики

Нижегородской академии МВД России,

кандидат психологических наук, доцент

ПРОПАГАНДА ТРАДИЦИОННЫХ ДУХОВНО-НРАВСТВЕННЫХ ЦЕННОСТЕЙ КАК ОСНОВА ПРОТИВОДЕЙСТВИЯ ИНФОРМАЦИОННОМУ ВОЗДЕЙСТВИЮ

В современном мире среди причин повсеместного распространения идеологии политического, религиозного и этнического экстремизма выделяется развитие различных информационных технологий и их воздействие на сознание молодежи. Информационными сервисами, явно или скрытно распространяющими идеи экстремизма и терроризма, являются различные мессенджеры и информационные приложения (такие, как Facebook, Telegram и другие), микроблоги, социальные сети, а также «темный (глубокий) интернет» DarkNet, с помощью которого пропагандируется экстремистский контент, осуществляется продажа оружия и т. д.

Жертвами информационного воздействия становятся молодые люди подросткового и юношеского возраста – по данным анализа А. Д. Рубан, это преимущественно лица в возрасте от 14 до 29 лет [5]. Данный возраст характеризуется активным формированием системы ценностей, определяющей поведение человека в дальнейшей жизни. Согласно исследованию С. С. Бредихина 16,10 % молодых людей имеют высокий уровень вербуемости [1]. К основным факторам, способствующим потенциальной уязвимости перед вербовочной деятельностью экстремистских организаций, автор относит обостренное чувство одиночества, собственного несовершенства, несправедливости, готовность вступить в организацию, способную дать им силу, уверенность и материальное благополучие, а также активное использование социальных сетей. По мнению И. А. Михеева «именно дистанционное информационное участие позволяет террористическим организациям формировать децентрализованную сеть распространения радикальной идеологии в глобальном масштабе» [4].

Механизм, обеспечивающий постоянный приток молодежи в сети экстремистских и террористических организаций, носит название «воронки вовлечения», в англоязычной версии – модель AIDA (Attention, Interest, Desire, Action – внимание, интерес, желание, действие). Этот механизм изначально разрабатывался в маркетинговых исследованиях как средство привлечения новых покупателей, но затем был поставлен на службу экстремистской идеологии. Методика мобилизации общественной поддержки и вовлечения больших масс в протестное движение описана ИТ-инженером, директором по маркетингу компании Google на Ближнем Востоке и в Северной Африке, одним из организаторов протестных акций в Египте В. Гонимом в книге «Революция 2.0». В аннотации к ее русскоязычному изданию говорится: «Летом 2010 года созданная Ваэлем Гонимом страница в Facebook стала своеобразным местом встречи зарождающегося

¹ © Федосеева О. И., 2020.

в Египте оппозиционного движения. В первый день ее посетило чуть более десяти человек. Всего шесть месяцев спустя от имени трехсот пятидесяти тысяч подписчиков эта страница призвала к восстанию» [2].

Воронка вовлечения, обеспеченная информационными технологиями, включает следующие стадии:

1) стадия внимания – размещение информации протестной, экстремистской направленности в социальных сетях, привлечение подписчиков;

2) стадия интереса – взаимодействие подписчиков с контентом («лайки», комментарии), использование специфического сленга, символики, девиза и т. п.;

3) стадия желания – подписка на контент, скачивание информационных материалов, «получение» знаков отличия (имени, номера, виртуального портрета);

4) стадия действия – объединение подписчиков в закрытые группы, формирование «спящих ячеек», нагнетание напряженности и призывы к действию (насилию).

На наш взгляд, каждая стадия, помимо ее технологического содержания, обладает характеристиками, раскрывающими сущность процесса подмены и навязывания системы идей, ценностей, позволяющими идеологам экстремизма привлекать в свои ряды новых последователей.

На первой стадии информационные материалы активно провозглашают и «отстаивают» ценности свободы, справедливости, расовой чистоты и т. п. Наличие виртуальной среды и интернет-посредника является основой возникновения у пользователя экстремистского контента эффекта деиндивидуализации – утраты запретов и ограничений, боязни оценки, физической «анонимности» – человеку кажется, что он «растворен» в виртуальном пространстве.

Стадия интереса активизирует подписчиков, при этом к идеям свободы и справедливости, характерным для первой стадии, добавляется пропаганда идей исключительности, консенсуса. Включается психологический эффект поляризации – усиления «рискованных», отрицательных точек зрения.

На третьей стадии информационное воздействие становится более агрессивным, радикальным: пропагандируются идеи необходимости борьбы с инакомыслящими; люди, имеющие противоположные ценности, обезличиваются. Работает психологический эффект группового фаворитизма – формируется стереотипизированное видение «врага», эмоциональная приверженность собственным идеям, идеалам, проявление негативного, враждебного отношения к инакомыслящим.

Последняя стадия, стадия действия, оказывается по своему ценностно-смысловому информационному наполнению весьма далекой от первоначальных материалов: это обеспечивается эффектом огруппления мышления у пользователей контента – иллюзией неуязвимости, не подвергаемой сомнению верой в нравственность собственных целей и средств их достижения, склонностью отбрасывать альтернативные точки зрения, избеганием рассмотрения возможных этических проблем принимаемых решений, рационализацией (оправданием) собственных действий.

Опасность работы такого механизма заключается в его дистанционном, растянутом во времени эффекте, постепенном вовлечении человека «без его «формального» и «непосредственного» вхождения в организационные структуры ра-

дикальных организаций и объединений» [4]. Таким образом, идеологи экстремизма и терроризма, опираясь на психологические особенности юного поколения (нигилизм, тотальное отрицание, нонконформизм, клиповое мышление, стремление к активным действиям, низкий уровень критического мышления), воздействуют на сознание молодежи, нивелируя традиционные ценности.

В. А. Емелин, анализируя размывание идентичности человека и утрату устойчивых ориентиров в современном обществе, в качестве первопричины этого явления называет социально-политические следствия идей толерантности и равнозначности мнений, позиций и ценностей. Он отмечает, что принцип плюрализма, предполагающий культивирование идей неограниченного выбора, приводит к размыванию и разрушению ценностей, делая любое мнение, отношение равновеликим. Таким образом, возникают ценности, навязанные меньшинством. В. А. Емелин описывает технологию навязывания власти меньшинства, получившую название «Окна Овертона». В ее основе лежит идея уравнивания значимости ценностных альтернатив и их продвижения по цепочке: область немыслимого – область радикального – область возможного – область рационального – область популярного [3]. По нашему мнению, эту идею можно развить. Ценности в процессе информационного экстремистского воздействия тоже меняются: свобода и справедливость – исключительность и консенсус – стереотипизированное видение «врага» – иллюзия неуязвимости, не подвергаемая сомнению вера в нравственность собственных целей и средств их достижения.

Мы полностью согласны с мнением ряда исследователей о необходимости развития системы контрпропаганды и просвещения, в том числе в виртуальной среде, «нужны не только блокировки, но и выстроенная контрпропагандистская работа, так как идеологии можно победить только двумя путями – либо физическим уничтожением носителей (что в современном информационном мире сделать невозможно – авт., либо другой идеологией (или системой идей)» [1].

О важности формирования ценностей говорится в Стратегии национальной безопасности Российской Федерации: к угрозам национальной безопасности в области культуры, согласно указанному документу, относятся размывание традиционных российских духовно-нравственных ценностей и ослабление единства многонационального народа Российской Федерации путем внешней культурной и информационной экспансии (включая распространение низкокачественной продукции массовой культуры), пропаганды вседозволенности и насилия, расовой, национальной и религиозной нетерпимости. Среди общих духовно-нравственных ценностей, формирующих фундамент государственности, в Стратегии перечислены свобода и независимость России, гуманизм, межнациональный мир и согласие, единство культур многонационального народа Российской Федерации, уважение семейных и конфессиональных традиций, патриотизм. К традиционным российским духовно-нравственным ценностям Стратегия относит приоритет духовного над материальным, защиту человеческой жизни, прав и свобод человека, ценности семьи, созидательного труда, служения Отечеству, нормы морали и нравственности, гуманизм, милосердие, справедливость, взаимопомощь, коллективизм, историческое единство народов России, преемственность истории нашей Родины [6].

Библиографический список

1. Бредихин, С. С. Механизмы вербовочной и пропагандистской деятельности экстремистских организаций в условиях развития новых медиа / С. С. Бредихин // Противодействие идеологии терроризма в образовательной сфере и молодежной среде : материалы Всероссийского форума. – М. : МГИМО-Университет, 2019. – С. 164–166.
2. Гоним, В. Революция 2.0. – СПб. : Лениздат, 2012. – 352 с.
3. Емелин, В. А. Кризис постмодернизма и потеря устойчивой идентичности // Национальный психологический журнал. – 2017. – № 2(26). – С. 5–15.
4. Михеев, И. А. Профилактика распространения деструктивной идеологии в образовательных организациях // Противодействие идеологии терроризма в образовательной сфере и молодежной среде: материалы Всероссийского форума. – М. : МГИМО-Университет, 2019. – С. 14–17.
5. Рубан, А. Д. Деятельность ОВД России по противодействию распространению идеологии терроризма и экстремизма в молодежной среде // Противодействие идеологии терроризма в образовательной сфере и молодежной среде : материалы Всероссийского форума. – М.: МГИМО-Университет, 2019. – С. 52–55.
6. Указ Президента Российской Федерации от 31 декабря 2015 г. № 683 «О Стратегии национальной безопасности Российской Федерации» // СПС «КонсультантПлюс». – URL: http://www.consultant.ru/document/cons_doc_LAW_191669.

Носова Д. Х.¹,

*старший преподаватель кафедры права и обществознания
Башкирского государственного педагогического университета
имени М. Акмуллы,*

Давлетов В. И.²,

*преподаватель кафедры огневой
и тактико-специальной подготовки
Уфимского юридического института
МВД России*

НАПРАВЛЕНИЕ ПРОТИВОДЕЙСТВИЯ ПРОЯВЛЕНИЯМ ТЕРРОРИЗМА И ЭКСТРЕМИЗМА В СЕТИ «ИНТЕРНЕТ»

Проблема, связанная с распространением и развитием терроризма в сети Интернет, согласно отчетам We Are Social и Hootsuite[3] о глобальном состоянии цифровых технологий на 2019 год, в настоящее время приобретает очень большие обороты. В течение дня с января 2018 года около одного миллиона человек открывали для себя пространства сети Интернет, а это – 11 человек в секунду. Терроризм в настоящее время поменял форму, изменяется тактика терроризма, затяжные войны и открытые столкновения перестали интересовать террористов. Происходит трансформация терроризма в целом, так как времена тайных встреч ушли, сейчас вербовка и общение происходит открыто в социальных сетях.

На сегодняшний день в связи с расширением аудитории сети Интернет повышается роль Интернета в жизни человека и общества. Вследствие широкого распространения социальных сетей и мессенджеров эти средства позитивной коммуникации между людьми становятся мощным оружием и инструментом, которые могут использовать также террористические организации.

Существует множество определений понятия «терроризм», но ни одно из них не может быть признано классическим, так как многие авторы не приводят различий между такими смежными понятиями, как «террор», «терроризм», «террористический акт» и другими схожими категориями, что значительно осложняет выработку единообразного подхода к пониманию проблем терроризма.

По мнению В. П. Емельянова[1] террор – это деятельность государственной власти в различные периоды существования государства. При этом помимо государственной власти другие силы могут насаждать повсеместный террор, внушая страх и ужас всем и каждому. Таким образом, террор может быть государственным и негосударственным и олицетворяет собой акции массового насилия над находящимся в их поле деятельности социальным контингентом. Также следует согласиться с мнением А. И. Моисеенко[2], что терроризм – не уголовно-правовое понятие, а социально-политическое явление, включающее в себя террористически направленную идеологию, организационную структуру и практическую террористическую деятельность.

¹ © Носова Д. Х., 2020.

² © Давлетов В. И., 2020.

По нашему мнению, терроризму как уголовно-правовому явлению свойственны следующие отличительные признаки:

- терроризм всегда носит публичный и демонстративный характер;
- терроризм создает и поддерживает обстановку паники, подавленности, страха и парализует социально полезную деятельность населения, нормальное функционирование органов власти и управления, а также общественных формирований и объединений;
- создается общая опасность для неопределенного круга лиц, гибель или наступление иных общественно опасных последствий;
- создаваемая обстановка действует на поведение людей и принуждает их к каким-либо действиям в интересах террористов, в данном случае насилие и давление играют решающую роль при принятии решения;
- психологическое воздействие играет большую роль, именно насилие вынуждает человека действовать непосредственно, так как создаются специальные условия при которых создается вынужденная обстановка страха.

Таким образом, представляется правильным определить терроризм, во-первых, как идеологически обоснованное насилие; во-вторых, как периодическое, т. е. систематическое, насилие; в-третьих, терроризм априори имеет политический характер.

Исходя из анализа выше приведенных мнений, предлагаем следующее определение терроризма: терроризм – это идеологически обоснованное систематическое насилие в отношении граждан для выполнения социально-политических условий.

Интернет на сегодняшний день является идеальной средой для пропаганды террористической и экстремистской деятельности по нескольким причинам:

- возможность оставаться анонимом;
- высокая скорость распространения информации;
- возможность без значительных затрат создавать собственные пропагандистские интернет-ресурсы;
- использование «лазеек» в несогласованности в законодательствах стран в области «компьютерного права»;
- шифрование сообщений и материалов.

После изучения обзора «Национального центра информационного противодействия терроризму и экстремизму в образовательной среде и сети Интернет»[5] за 2019 г. можно сделать следующие выводы.

1. Аудитория русскоязычного сегмента сети Интернет увеличивается. Если в 2011 г. количество интернет-пользователей составляло 49 % от населения России, то в 2019 г. уровень проникновения интернета находится на отметке 76 % – 109,6 миллионов интернет-пользователей.

2. Рост преступлений экстремистской направленности связан с усилением деятельности террористических организаций в информационной среде. Вербовка проходит через популярные мессенджеры.

В 2018 г. американское издание The Wall Street Journal[4] разместила список мобильных приложений и мессенджеров для общения, отсортированных по сте-

пени их безопасности террористическими группировками. Некоторые из них признаны хорошо защищенными от перехвата спецслужбами и рекомендованы последователям терроризма для координации действий и передачи информации. В частности считают безопасными приложения для зашифрованной связи Telegram, SilentCircle и Signal. А вот популярные приложения WhatsApp, Viber или WeChat считаются небезопасными по передаче информации абонентами.

То есть лица, причастные к террористической деятельности, используют шифрование – преобразование текста для обеспечения секретности передаваемой информации таким образом, что только авторизованные стороны могут получить к нему доступ для связи. Кроме того, распространив данные сообщения в интернет-ресурсах, они в дальнейшем удаляют или архивируют эти данные с целью сокрытия их.

Процесс радикализации, в результате которого человек приходит к пропаганде терроризма и экстремистской идеологии, не является статичным, а развивается со временем. Поэтому терроризм – не просто крайняя форма религиозных убеждений, но и полная смена сознания человека, его ценностных ориентаций и убеждений, в результате которых первоочередное значение играет влияние окружающего общества.

Представители разных социальных сетей часто понимают терроризм и экстремизм по-своему. Например, определение терроризма на Facebook – это любая неправительственная организация, которая совершает преднамеренные акты насилия в отношении лиц или собственности, чтобы запугать гражданскую, государственную или международную организацию с целью достижения политической, религиозной или идеологической цели. Это определение было позже отредактировано, чтобы уточнить, относится ли оно к террористическим организациям. Однако мы знаем, что террористические группы часто используют экстремистские идеи, разработанные экстремистскими организациями.

На платформах социальных сетей определения терроризма и экстремизма подразделяются на две отдельные группы. Экстремизм – это приверженность человека крайним взглядам и методам действий. Например, негативные высказывания на Facebook рассматриваются как нападение на человека в зависимости от его расы, этнической принадлежности, национального происхождения, религиозной принадлежности, сексуальной ориентации, пола, гендерной идентичности, серьезных заболеваний или инвалидности. Экстремистский контент обычно охватывает данную категорию негативных высказываний, поскольку она часто способствует и призывает к насилию, а также совершает различные действия, направленные на лишение прав принадлежности к человеческому роду.

Интернет-пространство в первую очередь расценивается террористами как новый вид инструмента для достижения своих целей, экстремистов воспитывают не в подпольных лагерях и конспиративных квартирах, а проникая через компьютеры и смартфоны в головы будущих террористов. Именно используя мессенджеры, вербовщики дают указания, где провести террористический акт и как собрать взрывное устройство, происходит интеграция идей в приложения. Людей, которых планируют завербовать, находят при помощи своих специальных сайтов, а именно собирают информацию о пользователях которые заинтересованы

в деятельности организации, после чего добавляют под каким-либо предлогом в друзья в социальной сети, начинается безобидное бытовое общение, и постепенно начинают склонять сначала к одобрению террористической деятельности, переходят в закрытые группы с высокой степенью криптозащиты, где непосредственно происходит уже полная вербовка. Следует понимать, что работает не один террорист-вербовщик, а целая информационно-пропагандистская сеть профессиональных психологов с использованием методов психологической обработки. Материалы, используемые в качестве пропаганды и оправдания терроризма, подготовлены на профессиональном оборудовании, создают подмену понятий и создание образа позитивного экстремизма. Создаются так называемые «спящие» ячейки с целью внезапной активации к действиям в будущем или оказания пособнической помощи.

В сети «Интернет» сайты и платформы, пропагандирующие и распространяющие материалы способствующие развитию экстремизма и терроризма, можно разделить на следующие группы:

- непосредственно распространяющие идеи терроризма и экстремизма (через данные ресурсы международные террористические организации проводят пропаганду, а также находят людей, интересующихся терроризмом. Как правило, вербуют под предлогом борьбы с терроризмом, как это было в Сирии, когда турецкие вербовщики, обещая, что будут бороться с терроризмом на стороне Ливийской национальной армии, вербовали и заманивали людей в террористические ячейки подконтрольные так называемому «Правительству национального согласия»);
- информационные ресурсы, через которые происходит финансовая поддержка террористических организаций;
- сайты, содержащие контент, направленный на разжигание ненависти на основе расовой или национальной принадлежности.

На данных террористических сайтах можно найти подробную информацию о том, как в кустарных условиях изготовить химические соединения, обладающие высокой токсичностью или как собрать самодельное взрывное устройство из бытовых предметов. Даются рекомендации по тактике проведения террористических акций либо же по вербовке новых членов преступных организаций. Интернет-сайты, относящиеся к этой группе, могут располагаться в любой точке сети, так как содержащаяся в них информация представляется как справочная. По природе такие сайты многочисленны и недолговечны, так как часто меняют доменные имена.

Проблема обнаружения и ликвидации сетевых центров (серверов, доменов, веб-сайтов) является главной причиной использования террористами интернет-технологий. Используются особенности технической организации Интернета, позволяющие создавать доменные имена сайта в одной стране, а размещать информацию в другой. При этом доступ к нему может быть обеспечен практически из любой точки мира, имеющей подключение к сети. Данное обстоятельство позволяет членам преступных организаций создавать закрытые каналы для передачи информации.

В настоящее время в таких социальных сетях, как Facebook и Twitter, отсутствуют категории разграничения информации, чтобы отмечать или сообщать о террористическом контенте на своих платформах. На видеохостинговом сайте YouTube можно пометить только одну категорию. Например, видео может быть отмечено как: «насильственное или отвратительное», «пропаганда терроризма» и «ненавистный или оскорбительный контент». Эта проблема требует разрешения в целях недопущения развития терроризма в сети Интернет.

Для пресечения деятельности террористических организаций через сеть Интернет мы предлагаем технологическим компаниям сделать следующее.

Во-первых, глобальные информационные и технологические компании должны создавать определенные группы, системы упорядоченности и автоматизации информации, которые позволили бы автоматически сгенерировать такие категории распространения информации, как «экстремизм» или «терроризм», в рамках своих существующих систем отчетности. Это позволило бы пользователям сообщать о подобных материалах и отмечать многочисленные проблемы в целях их своевременного решения.

Во-вторых, следует создать более совершенный и более последовательный процесс подачи апелляций и механизм обратной связи. Пользователи должны иметь возможность непосредственного взаимодействия с лицами, представляющими данные компании и принимающими решения в области размещения, распространения информации на данном ресурсе. Эти решения должны быть подробно, отчетливо и объективно обоснованы, с уточнением, почему некоторые материалы получили доступ на размещение, а другие материалы нет. Однако не все компании игнорируют данные проблемы, многие из них все же публикуют ежеквартальные отчеты или сообщения в блогах по тому или иному вопросу. Делается это для того, чтобы создавать благоприятную обстановку на своей платформе, обеспечивать безопасность пользователей, основанную на доверии и чувстве непосредственного общения.

В-третьих, в случае распространения и пропаганды террористического или экстремистского контента на определенные группы людей информационные компании должны обеспечить пользователей сети Интернет своевременной помощью и поддержкой, такой как консультация, онлайн-беседа, введение возрастных ограничений, возможность ограничения просмотра и комментирования. Американская транснациональная публичная корпорация Google является лидером в этом направлении, применяя метод «перенаправления» и предоставляя различные ограничения для пользователей в отношении определенного контента, включая контент с ограничением по возрасту, где удаляются комментарии или предлагаемые видео.

В настоящий момент при нынешнем развитии технологий и методов передачи информации в сети «Интернет» возникает необходимость в превентивной антиэкстремистской работе. Данная мера позволит оперативно воздействовать на каналы распространения такой информации и нивелировать эффект от ее воздействия. Использование технологий сетевого маркетинга (Social Media Marketing – SMM) позволит расширить аудиторию охвата и увеличит уровень лояльности к данному контенту. Таким образом, лишь осознав сущность разви-

тия данной проблемы, вовлекая определенные службы и совершенствуя системы, мы можем более эффективно выявлять экстремистский и террористический контент и обеспечивать их нераспространение. С этой целью возможно использование популярных в сети «Интернет» блоггеров и известных личностей, которые могли бы проводить информирование пользователей сети Интернет об опасности терроризма, тем самым формируя антитеррористическое сознание у населения нашей страны.

Библиографический список

1. Емельянов, В. П. Терроризм и преступления с признаками терроризирования. – СПб, 2010. – С. 17.
2. Моисеенко, А. И. Уголовно-правовая и криминологическая характеристика терроризма (по материалам Южного федерального округа России) : дис. ... канд. юрид. наук. – Ставрополь, 2006. – С. 9.
3. Simon Kemp. Digital 2019: Global Internet Use Accelerates [электронный ресурс] // We are social : global socially-led creative agency. – URL : <https://wearesocial.com/blog/2019/01/digital-2019-global-internet-use-accelerates>. (дата обращения: 20.03.2020).
4. Шифровка для террориста: одобренные приложения для защищенной связи и новый раунд дебатов о безопасности [электронный ресурс] // Настоящее время. – URL : <https://www.currenttime.tv/a/isis-communication-apps-privacy-vs-security/27373082.html>. (дата обращения: 19.03.2020).
5. Национальный центр информационного противодействия терроризму и экстремизму в образовательной среде и сети Интернет [электронный ресурс] // URL: <https://ncpti.su>. (дата обращения: 15.03.2020).

*Шалюгина Е. С.¹,
старший преподаватель кафедры
психологии и педагогики
Нижегородской академии МВД России*

ИНФОРМАЦИОННЫЙ ТЕРРОРИЗМ – МАНИПУЛЯЦИЯ СОЗНАНИЕМ БОЛЬШИНСТВА

Развитие современного общества, доступность и многообразие информационных источников приводит к осведомленности социума о механизмах и тенденциях политических течений в мировом масштабе. Общественность, черпая информацию самостоятельно, на добровольной основе ввергается в «информационную зависимость», формируя у себя определенную мировоззренческую позицию. Получив крупную информацию, общество не отслеживает манипуляционных тенденций со стороны источника этой информации. Не углубляясь в осознание проблемы, поверхностно рассуждая о глобальных вещах, в подтверждение своего мнения цепляет из информационного потока факты, носящие тождественный (с его мнением) характер. Психика человека устроена таким образом, что из окружающей действительности нас интересуют, беспокоят, привлекают внимание только те обстоятельства, которые находят отражение в нашем внутреннем плане. Это позволяет стороннему наблюдателю диагностировать болевые точки каждого из нас, в субъективном плане – осознавать возможности, брать на себя ответственность, мотивировать себя, формируя жизненную позицию.

Но человек социальное существо. Без окружения он не желает существовать. Социум дает человеку ощущение безопасности, комфорта, стабильности, принятия, признания его важной единицей взаимодействия, способной формировать ценности общества. При этом человек не замечает более сильного влияния (давления) общества на его мнение. Конформистские характеристики личности формируют механизмы психологии масс. Группа, заинтересованная в реализации некой идеи, превосходно эти механизмы запускает, манипулируя сознанием общества. Манипуляции в этом случае могут быть мягкими (подкидывание информационного повода в нужный момент в «кострище» общественного мнения), или агрессивными (распространение пугающих слухов, дозирование информации, муссирование только необходимых фактов). Техник манипуляции великое множество, и все они достаточно действенны, особенно когда они применяются в отношении большой группы. Общество самостоятельно усиливает любую технологию в сотни раз, поскольку на бессознательном уровне запускает механизмы психологии масс: заражение, подражание или внушение.

В настоящее время уже неактуальным является применение жестких карательных мер для погружения общества в состояние страха, и как следствие, бездумного подчинения. Для этого достаточно использовать информационные потоки: радио, телевидение, интернет и прочие. Любые коммуникативные системы являются неотъемлемой частью жизнедеятельности человека, а это значит, что

¹ © Шалюгина Е. С., 2020.

человек в обязательном порядке подпадает под это влияние. Дело остается за малым – сконструировать идею и запустить в сознание, и там она, подхваченная сознательными и бессознательными процессами, укореняется и разрастается до глобальных размеров, превращаясь в идею фикс.

Играя на нереализованных потребностях общества, можно ввергать людей в различные состояния. Новизна, специфичность, неординарность информации, продолжительное обсуждение животрепещущих фактов, неопределенность ситуации привлекают внимание людей, структурируют представление о проблеме, а при наличии пробелов заполняют пустоты вымыслом, причем не в положительном аспекте (в плане разрешения проблемы), а в устрашающей форме (приписывая все более серьезные, жестокие и неправомерные особенности), тем самым загоняя еще сильнее в состояния агрессии, паники или депрессии. Хотя эти состояния общества различны по форме реализации и протекания процессов, они позволяют заинтересованным лицам эффективно реализовать террористические стратегии.

Террористические организации черпают рекрутов для себя из социума. Там еще нет идейно подготовленных или неимоверно запуганных, или безысходно затравленных исполнителей, но уже есть интересующиеся, любопытствующие, романтично настроенные или отверженные социумом. Затронув «живые струны» психики, террористические организации просто ждут прибытия новобранцев для «реализации» их несбывшихся надежд. Информационный вихрь захватывает сознание человека, перегружая психику, что приводит к утрате контроля. Рекрутолог всегда обладает навыками убеждения, которые основаны на способности понять чувства и мысли другого человека или толпы, контролировать свое поведение и чувства, влиять на людей и вести за собой; на артистизме; на интеллекте. Эти «ярмарочные зазывалы» интригуют и манят прекрасными перспективами реализации тех потребностей человека или общества, которые находятся в угнетенном состоянии, обещают исполнения всех желаний при минимальном приложении усилий. А мы помним, что ничто так не привлекает человека, как возможность обогатиться (ментально или материально) без труда. «Бесплатный сыр в мышеловке» срабатывает всегда. Рекрут отчасти становится слепой пешкой в чужой игре, которую в дальнейшем используют как разменную фигуру, не имеющую никакой ценности.

Основной группой риска, пополняющей террористические организации, по-прежнему остается молодежь. Особенности мировосприятия, незрелость социально-психологических установок, неустойчивая идентичность, выраженный поиск себя, склонность к риску и проявлению всякого рода форм протестных реакций делают их наиболее восприимчивыми для воздействия информации экстремистского характера. Понимание мотивов и побуждений возникновения экстремизма среди молодежи, позволяют сформировать платформу для реализации социально-психологических условий, которые не позволят укорениться в сознании подрастающего поколения идеологии террора.

Возрастной особенностью подрастающего поколения является повышенная эмоциональность. Ввиду гормональной нестабильности контролирующие функции нервной системы снижены, что провоцирует конфликтное взаимодействие

с окружающими. Эти проявления обличаются в форму юношеского максимализма и обостренного стремления к справедливости, что становится ключами доступа для манипулирования сознанием молодежи. Рекрутологи террористических организаций всегда умело используют психологические качества рекрута для внедрения в сознание идей культивирования принципа силы, агрессии в отношении окружающих, непримиримости к инакомыслящим (вплоть до насилия и убийства).

Нетерпимость к «иным» у подростков формируется быстрее в связи с дисбалансом эмоционального состояния. Перепады от низкой самооценки, неспособности к эмпатии, неумения адекватно выражать свои эмоции до яркой бравады и демонстративности поведения толкают молодежь ради признания своего авторитета на все.

В своей работе Н. В. Завьялова, анализируя экстремистские установки среди учащихся, делает выводы о наличии ярко выраженных характеристик молодежи, попадающей под влияние экстремистских организаций: низкая самооценка, низкая правовая культура, высокая агрессивность, отсутствие занятости в свободное от учебы время [1, с.7]. Привычка к праздному ведению жизни приводит к угасанию имеющихся способностей и деградации личности. У подрастающего поколения просто не развивается аналитическое мышление, что не дает возможности критически оценивать как происходящие события, так и поступающую в сознание информацию. Интеллектуальная ограниченность, создает ощущение того, что только «Я» и «Моё» сообщество являются обладателями абсолютной истины, которая рассматривается незыблемой. Крайности является характерным проявлением примитивного мышления молодежи.

Социальный фактор также играет не последнюю роль в формировании экстремистской направленности молодежи. Материальная неудовлетворенность формирует негативное отношение к социуму и требует выплеска этой энергии. А благоприятные материальные условия и состоятельность семьи провоцирует желание заявить о себе, как компенсация чувства собственной несостоятельности в обществе.

Оказываясь под влиянием различных факторов, подрастающее поколение остается беззащитным в поиске собственной идентичности, которая складывается по упрощенной схеме «мы – они». Его психика неустойчива, оно легко подвергается внушению и манипулированию. Неприспособленная к определенным условиям жизни в социальном, психологическом, правовом плане, молодежь демонстрирует обществу не всегда адекватные попытки самовыражения. Возникающий в поведении психологический барьер «свой – чужой» увеличивает тревогу перед «непохожими» на себя, что повышает агрессию по отношению к нему [2, с.55].

Любые контртеррористические мероприятия должны выстраиваться и планироваться с учетом психологических особенностей субъектов задействованных в ситуации. Тонкая грань между поспешными действиями и рутинным разматыванием хитросплетений террористической направленности может быть разрушена ввиду отсутствия понимания психологической структуры личности и механизмов психологии масс.

Основная цель любой контртеррористической операции – ликвидация террористической деятельности организации, минимизация жертв и ущерба. Выявлять, пресекать и профилировать любые проявления деятельности террористических организаций, которые посредством насильственной, скрытой или обманной тактики изменяют направления активности других людей. Если перекрыть каналы поступления новых ресурсов, любая организация прекратит свое существование. Но на этом этапе мы опять возвращаемся к вечному вопросу *Cui prodest?* (кому выгодно?) [3]. Никто в своей жизни не осмеливается стать преступником без расчета и пользы для себя.

Библиографический список

1. Завьялова, Н.В. Образовательная среда как пространство профилактики экстремизма / Н. В. Завьялова // Историческая и социально-образовательная мысль. – № 1. – СПб., 2014. – С. 7.
2. Зуйкова, А. А. Основные факторы, способствующие вовлечению подростково-молодежных групп в экстремистское сообщество / А. А. Зуйкова, Е. С. Шалюгина // Психологическая безопасность образовательной среды : материалы III международной научно-практической конференции (Нижний Новгород, 20 февраля 2020 г.) / отв. за вып. проф. Г. В. Сорокоумова. – Н. Новгород: НГЛУ, 2020. – С. 52–57.
3. Латинско-русский и русско-латинский словарь крылатых слов и выражений : 8-е изд. / Н. Т. Бабичев, Я. М. Боровской. – М. : Дрофа, 2008. – 994 с.

Гурьянова В. Р.¹,

*доцент кафедры управления в органах внутренних дел
Уфимского юридического институт МВД России,
кандидат физико-математических наук*

СТРАТЕГИЯ АНТИТЕРРОРИСТИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ В УСЛОВИЯХ ПАНДЕМИИ

Развитие информационных технологий привело к развитию экстремизма и терроризма в киберпространстве. Понятие «киберэкстремизм» и «кибертерроризм» были введены О. А. Голиком как обозначение использования компьютеров в качестве оружия или средством достижения целей политически мотивированных международных или национальных групп либо организаций, причиняющих или угрожающих причинить ущерб и посеять панику для воздействия на население или правительство [1, с.36].

Также в этом направлении проводили исследования С. Я. Лебедев, П. Н. Кобец, Е. Н. Молодчая, А. Г. Волеводз и др. Киберпространство в грядущем тысячелетии стало очень удобным для распространения радикальных взглядов, апробации новых способов вербовки и манипулирования общественным сознанием. Таким образом, научный интерес к вопросам выявления, предупреждения и нейтрализации экстремистских и террористических угроз на сегодняшний день стал очень актуальным, особенно в условиях пандемии. Социальное дистанцирование вынудило людей все больше проводить время дома за компьютером, что привело к возникновению новых радикальных идей у террористов.

Создание системы международной информационной безопасности необходимо на уровне межправительственного сотрудничества на таких площадках как: ООН, БРИКС, ШОС и др. По данным Центра по изучению проблем терроризма Jane's (JTIC) в 2018 г. террористические группировки действовали в 90 странах мира, в то время как в 2017 г. активность наблюдалась в 116 странах. Система обеспечения безопасности в киберпространстве на международном уровне развивается и является главным вопросом каждого государства.

Генеральный секретарь Совета безопасности ООН Антонио Гутерриш на июльском заседании отметил, что условия пандемии коронавируса породили новые идеи у террористических группировок для расширения своего влияния по всему миру. Они используют глобальную нестабильность как тактическое преимущество.

По данным американской организации Moonshot CVE, с начала официального введения пандемии в США посещение страниц Google, связанных с экстремистскими материалами увеличились на 13 %, увеличилась также интернет-активность в социальной сети Facebook и активизировались действующие Telegram-каналы.

«Боевики Исламского государства (ИГ) начали использовать тему COVID-19 в качестве пропаганды, превознося вирус как божественное наказание Западу», – объяснил старший научный сотрудник Проекта по борьбе с экстремизмом (СЕР)

¹ © Гурьянова В. Р., 2020.

Джош Липовски. Сначала ИГ призывали своих сторонников избегать районов заражения, но затем они поняли, что могут извлечь выгоду из страха, вызванного пандемией. Примерно в это же время свою агитацию начали и террористы из «Аль-Каиды». Стали распространяться слухи, что китайский Ухань является испытательным полигоном для новой технологии 5G, и это стало причиной возникновения заболевания COVID-19. Эксперты ЕС по терроризму говорят о «технофобах», на которых они возлагают ответственность за несколько поджогов вышек сетей 5G в Великобритании и Нидерландах [3]. Таким образом, пандемия коронавируса послужила поводом для рождения новых идей в экстремистской и террористической деятельности.

Теория и практика антитеррористической деятельности, конечно, приводит к ограничению прав и свобод граждан, но используя накопленный опыт правоохранительными органами и международными организациями стран и правильно понимая сложившуюся ситуацию, необходимо с нового ракурса взглянуть на угрозу безопасности и устойчивого развития общества. Необходимо выстроить более эффективную политику. В частности, усилить борьбу в период кризиса и увеличить инвестиционные вливания в контртеррористические программы. Более активно использовать новые методы противостояния террористическим угрозам и тенденциям. Не допустить, чтобы террористы использовали психосоциальную, политическую и экономическую стрессовую ситуацию, связанную с COVID-19. Должен быть четкий обмен данными между странами в период пандемии. Ужесточить механизмы контроля цифровой социальной коммуникации людей. Распространить внедрение цифровой биометрической идентификации человека на основе алгоритмов и вычисляемых персональных кодов (id человека) на международном уровне. В целях противодействия терроризму безналичное денежно-финансовое обращение должно иметь прямую связь с id человека. Система биометрической идентификации человека должна быть единообразным и универсальным инструментом во всех странах интеграционных образований на основе общих технических регламентов и стандартов [3, с. 82].

Библиографический список

1. Голик, О. А. Противодействие идеологии терроризма и экстремизма в информационном пространстве // Противодействие терроризму. Проблемы XXI века – Counter Terrorism. 2015. – № 1.
2. РИА-Новости // Эксперты: количество терактов в мире в 2018 году снизилось на треть [электронный ресурс]. URL: <https://ria.ru/20190124/1549807290.html> (дата обращения: 23.05.2020).
3. Тагиров З. И., Трофимов Ю. В. Направления совершенствования организации международного межведомственного правоохранительного сотрудничества по противодействию терроризму (на опыте стран Европейского союза) / З. И. Тагиров, Ю. В. Трофимов // Академическая мысль. – 2019. – № 2(7).

Еськов А. В.¹,

*профессор кафедры информационной безопасности
Краснодарского университета МВД России,
доктор технических наук, профессор*

Кальницкая В. М.²,

курсант Краснодарского университета МВД России

ПРОФИЛАКТИКА ЭКСТРЕМИЗМА И ТЕРРОРИЗМА В МОЛОДЕЖНОЙ СРЕДЕ КАК АКТУАЛЬНАЯ ПРОБЛЕМА В ИНФОРМАЦИОННО-КОММУНИКАЦИОННОМ ПРОСТРАНСТВЕ

Согласно Конституции Российской Федерации, принятой всенародным голосованием 12 декабря 1993 г., с изменениями, одобренными в ходе общероссийского голосования 1 июля 2020 г.: «Мы многонациональный народ Российской Федерации, соединенные общей судьбой на своей земле...» [1]. В соответствии с Всероссийской переписью населения, проведенной в 2010 г., на территории современной России проживает свыше 160 национальностей и около 194 этносов, что порождает в своей совокупности конфликты.

В соответствии с Федеральным законом от 25 июля 2002 г. № 114-ФЗ «О противодействии экстремистской деятельности» под экстремизмом принято понимать комплекс действий, направленных на изменение конституционных основ и строя насильственным путем, принятие террористической деятельности, ее пропаганда, активное стремление к социальным, расовым, национальным или религиозным враждебным отношениям с использованием нацистской атрибутики и символики и публичным призывам к осуществлению такой деятельности на территории Российской Федерации [2].

Что касается терроризма и террористической деятельности, то Федеральный закон от 6 марта 2006 г. № 35-ФЗ (в ред. от 18 марта 2020 г.) «О противодействии терроризму» четко разделяет данные понятия. Под терроризмом рассматриваемый нормативно-правовой акт понимает идеологию насильственных действий, направленных на воздействие на органы государственной власти, с целью принятия ими необходимых для террористической организации решений, путем применения устрашающих населения действий. В то же время, террористическая деятельность – организация (планирование, подготовка и реализация) террористического акта, подстрекательство и пропаганда насильственных действий террористического характера, подготовка террористов, их вербовка и обучение. Из этих двух понятий можно выделить понятие террористического акта, которое в своей совокупности объединяет два рассматриваемых ранее понятия – совершение насильственных действий, устрашающих население и создающих угрозу их жизни и здоровью, осуществлению конституционных прав и свобод человека и гражданина, причинение имущественного вреда и деорганизация органов государственной власти и местного самоуправления путем осуществления поджога, взрыва и других подобных действий [3].

¹ © Еськов А. В., 2020.

² © Кальницкая В. М., 2020.

Отсюда можно сформулировать вывод, что экстремизм – более широкое понятие по сравнению с терроризмом, поскольку не ставит перед собой цели, касающейся претворения в жизнь общества насильственных действий, а только предусматривает ущемление прав человека, в зависимости от его национальной, расовой, социальной или религиозной принадлежности.

Актуальной проблемой современного российского общества является вовлечение молодежной среды в экстремистскую и террористическую деятельность, что диктуется отсутствием адаптации молодежи в социуме и тем самым создания благоприятной «почвы» для развития асоциальных взглядов в их среде, вызывающих противоправное поведение. Согласно социологическим и психологическим мнениям, наиболее опасным возрастом «вхождения» в экстремистские и террористические взгляды является период от 14 до 22 лет. Это объясняется психологическим обществом, стремлением молодого человека к поиску собственной тождественности в обществе, нахождении «себе подобных», и неустойчивой психике, которая достаточно просто подвергается внушению и манипулированию со стороны подготовленных, ранее завербованных молодых людей или взрослых, которые создают круги неформальных объединений, несущих в общих случаях экстремистскую или террористическую направленность, что диктуется также стремлением неуверенных подростков к нахождению ответственных в их бедах и неудачах.

В настоящее время вербовка молодежной среды со стороны экстремистов или террористов осуществляется значительно легче, чем, например, 10 или 15 лет назад, ввиду развития информационно-коммуникационного пространства.

Как отмечают ведомственные органы Российской Федерации, сеть «Интернет» – наиболее распространенный способ вербовки молодежи, который включает в себя общение через тематические сайты, социальные сети, форумы и блоги. Особым каналом радикального течения является, где сторонники экстремистских и террористических взглядов, распространяющих аспекты противоправной деятельности, освещают, как спланировать и скоординировать такую деятельность. Удаленный и виртуальный формат позволяет вербовщикам таких организаций осуществить первичный отбор кандидатов, их дальнейшее общение через «секретный чат» в Telegram [5].

Еще одним способом вовлечения молодежной среды в террористическую и экстремистскую деятельность служат компьютерные игры в режиме онлайн, предусматривающие возможность общения в формате текстовых, голосовых и видеочатов. Компьютерные игры, которые предусматривают выполнение заданий в реальном времени, представляют наибольшую опасность, поскольку в такие «игры» выступают в роли катализатора к совершению актов насилия над отдельным человеком и обществом в целом, погромов, поджогов и иных противоправных действий.

Примером вовлечения молодежной среды в экстремистскую деятельность через компьютерные игры онлайн формата является проект «Большая игра. Сломай систему» сообщества «Северное братство», идея которого заключается в вербовке большого числа участников данной игры с целью проведения диверсий против существующего в Российской Федерации режима и строя. «Большая игра.

Сломай систему» предусматривает конкретные задания в зависимости от категории и роли игрока: «интернет-боец» или «уличный боец», начиная от нанесения надписей на городские здания, повреждения общественного транспорта до унижения человеческого достоинства и избиения мигрантов, которых такое сообщество называло «пришельцами». Отчеты о своих действиях участники должны были присылать на сайт данной компьютерной игры. В архивах «Большой игры» правоохранные органы насчитали десятки тысяч видеосюжетов о «выполненных» действиях, несущих экстремистский характер. Организатор игры, предприниматель А. Мухачев, был осужден по статье уголовного законодательства Российской Федерации за организацию экстремистского сообщества [5].

Что касается террористических организаций, то они привлекают в сравнительном большинстве молодежь, которая «жаждет» власти, самоутверждения и общения с «себе подобными». Такие организации рекламируют себя через Telegram путем применения специально психологически подготовленных видеороликов, комиксов, картинок, демонстрирующих доминирование данной организации и побуждающих неустойчивую, несформированную психику молодого человека вступить в ряды и осуществлять деятельность, путем навязывания им возможности стать «властителями мира» и «героями» в ближайшем будущем.

Как же террористические и экстремистские организации находят «нужных» людей? Ответ прост: они вычисляют молодежь, находящуюся на «социальной обочине», людей, имеющих материальные и психологические проблемы. Например, молодой человек получил достойное высшее образование, но не смог найти высокооплачиваемую работу, не получается обустроить личную жизнь или проблемы в семье.

К проявлению терроризма и экстремизма в молодежной среде является создание виртуальных суицидальных групп в социальных сетях, называемых «группами смерти». Они преимущественно осуществляют свою деятельность в социальной сети «ВКонтакте», где администраторы таких групп, в значительности закрытого доступа, склоняют подростка к акту самоубийства. Выявленными правоохранными органами «группами смерти» являются «Синий кит», «Тихий дом» и «f57», использовавшие игровые и аутоагрессивные методы воздействия на психику подростка [8].

Основные профилактические меры, направленные на предупреждение и пресечение проявлений экстремизма и терроризма в молодежной среде, согласно Стратегии противодействия экстремизму и терроризму в Российской Федерации до 2025 года (утв. Президентом Российской Федерации 28.11.2014 № Пр-2753) являются: создание и включение на региональном и муниципальном уровне мероприятий, воспитывающих у молодежи уважительное отношение ко всем религиям и этносам; создание условий для культурного и спортивного развития подростков; принятие воспитательных мер по развитию патриотизма, мирного поведения, терпимости и др.; включение в стандарты высшего образования по профилю «Журналистика» правил освещения вопросов противодействия экстремизму и терроризму и т. п. [4].

В настоящее время в информационно-коммуникационном пространстве Российской Федерации созданы «горячие линии» «Центра безопасного Интернета»

и «Лиги безопасного Интернета», которые в молодежной среде стремятся создать «кибердружины» для выявления групп, объединений и чатов, направленных на склонение молодежи к экстремистской и террористической деятельности, и проводят информационно-разъяснительные беседы с подростками.

Самой уязвимой к привлечению в деятельности террористических и экстремистских организаций является молодежная среда, наиболее восприимчивая к новшествам общественного и технологического развития, тем самым становясь легко поддающейся манипуляции средой для правонарушителей.

Библиографический список

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) // СПС «КонсультантПлюс». – URL: http://www.consultant.ru/document/cons_doc_LAW_28399.
2. Федеральный закон от 25 июля 2002 г. № 114-ФЗ «О противодействии экстремистской деятельности» (с изм. и доп. от 31.07.2020). // СПС «Гарант». – URL: <https://base.garant.ru/12127578>.
3. Федеральный закон от 6 марта 2006 г. № 35-ФЗ «О противодействии терроризму» (ред. от 18.03.2020) // СПС «КонсультантПлюс». – URL : http://www.consultant.ru/document/cons_doc_LAW_58840.
4. Стратегия противодействия экстремизму и терроризму в Российской Федерации до 2025 года (утв. Президентом Российской Федерации 28.11.2014 № Пр-2753). // Нижегородская академия МВД России [официальный сайт]. – URL : https://на.мвд.пф/upload/site128/document_file/Strategiya_protivodeystviya_ekstremizmu_v_Rossiyskoy_Federaci.pdf.
5. Казанцев А. А. Проблема вербовки и возврата боевиков-террористов: опыт Европы и перспективы России. Рабочая тетрадь РСМД / А. А. Казанцев. – М. : РСМД, 2016. – 41 с.
6. Петрищев, В. Е. Профилактика терроризма // Терроризм в современном мире. 2-е изд. / под ред. В. Л. Шульца; Центр исслед. проблем безопасности РАН. М.: Наука, 2011. С. 321.
7. Кудайбергенов, К. Ш. Особенности вербовки в террористические организации // Материалы VII Региональных экспертных консультаций представителей органов безопасности, специальных служб и правоохранительных органов государств – участников СНГ по борьбе с терроризмом и иными насильственными проявлениями экстремизма и расширенного пленарного заседания Научно-консультативного совета при АТЦ СНГ : сборник материалов. – СПб. : Русь, 2017. – С. 103.
8. Амелина, Я. «Группы смерти» как угроза национальной безопасности России : аналитический доклад. / Кавказский геополитический клуб. – М. : ИП Воробьев А. В., 2017.
9. Мартынов, К. Террористы опростились [электронный ресурс] // Новая газета. – URL : <https://www.novayagazeta.ru/articles/2017/09/16/73875-terroristy-oprostilis>.

Еськов А. В.¹,

*профессор кафедры информационной безопасности
Краснодарского университета МВД России,
доктор технических наук, профессор*

Сергеева В. А.²,

курсант Краснодарского университета МВД России

ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ДЕЯТЕЛЬНОСТИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ В СФЕРЕ ПРОТИВОДЕЙСТВИЯ ПРОЯВЛЕНИЯМ ЭКСТРЕМИЗМА В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Экстремизм является угрозой общественной безопасности, поэтому его профилактике уделяется особое внимание. Актуальность данной темы заключается в необходимости усовершенствования правового обеспечения деятельности ОВД в сфере противодействия проявлениям экстремизма, так как именно законодательное регулирование играет решающую роль в предотвращении развития данного вида преступлений.

Необходимость внесения изменений в нормативное регулирование обусловлена информатизацией общества, а также возникновением глобального информационного пространства, распространением информационных услуг и доступностью информационного пространства.

Под экстремизмом понимают приверженность радикальным взглядам, отличным от общества. Особенность борьбы с экстремизмом в современном мире заключается в том, что обработка информации осуществляется компьютерами, а обмен данными – через сети, из-за чего возникает необходимость создания норм поведения при нахождении в сети на законодательном уровне. [8, с. 103]

В России, по данным социологической компании ООО «ФОМ», активная аудитория Интернета (пользователи, выходящие в сеть хотя бы раз за сутки) составляет 50,1 % от социально активного населения страны, или 58,4 млн. человек. Если весной 2003 г. за сутки Интернетом пользовалось 3,2 млн. чел., то в 2015 г. – 61,5 млн. чел., а весной 2017 г. – 71,6 млн. чел. [7, с.5]

Такой рост популярности использования глобальной сети способствовал развитию информационного экстремизма. Данное явление представляет собой социально-психическое воздействие на общество, с целью достижения противоправных целей посредством информационных технологий. Такое воздействие посягает на конституционные права граждан. [1]

Далее рассмотрим основные нормативные акты, которые регулируют деятельность по борьбе с экстремизмом.

В Федеральном законе от 25 июля 2002 г. № 114-ФЗ «О противодействии экстремистской деятельности» содержится определение, какие действия следует относить к экстремистским. [5]

¹ © Еськов А. В., 2020.

² © Сергеева В. А., 2020.

В Федеральном законе от 7 февраля 2011 г. № 3-ФЗ «О полиции» указано, что сотрудники обязаны предупреждать, пресекать и выявлять экстремистскую деятельность. [4]

Согласно Указу Президента Российской Федерации от 6 сентября 2008 г. № 1316 «О некоторых вопросах Министерства внутренних дел Российской Федерации», в органах внутренних дел были образованы подразделения по противодействию экстремизму. [6]

В сфере противодействия экстремизму имеются международные акты, которые также действуют на территории Российской Федерации.

Нельзя не отметить Уголовный Кодекс и Кодекс об Административных правонарушениях, которые определяют отнесение действий экстремистского характера к противоправным и назначают ответственность за их совершение.

Согласно КоАП РФ к правонарушениям, описанным в ст.ст. 20.3, 20.29 можно отнести деятельность, которая направлена на распространение экстремистских материалов посредством электронных изданий. Однако в Кодексе отсутствует формулировка, уточняющая, каким образом можно квалифицировать правонарушения, если они были совершены в сети «Интернет» или через средства массовой информации. [3]

В ст.ст. 280, 282 УК РФ есть уточнение по поводу совершения преступления с использованием средств массовой информации или сети «Интернет». [2] Осложняет процесс привлечения к ответственности своеобразие общения в Интернете, а именно такие признаки, как: анонимность, высокая скорость передачи сообщения, отсутствие территориальных границ. Самая большая трудность возникает при определении вида ответственности, а также порядка привлечения к ней, так как в законодательстве, как было приведено выше, отсутствуют четкие формулировки, указывающие, какие именно действия влекут ответственность.

Следует отметить элементы взаимодействия в сети, которые могут оцениваться с точки зрения экстремистской направленности: основное изображение владельца социальной сети; картинки на страницах в социальных сетях; статус в социальной сети; выражения отношения к опубликованным другими пользователями материалов в общедоступном формате; копирование публикаций на свою страницу, комментирование публикаций, которые созданы другими пользователями. [9, с. 8]

Современное законодательство не в полной мере позволяет определить сам факт совершения правонарушения. Помимо неочевидности наличия состава правонарушения возникает проблема при определении, какие из вышеописанных действий в сети в какой степени нарушают нормы права.

Для повышения эффективности правового обеспечения деятельности ОВД при противодействии экстремизму в информационных системах необходимо внести ряд изменений в законодательство. Во-первых, следует изучить все действия в сети и дать им оценку с точки зрения противоправности. Далее необходимо определить степень общественной опасности и вид ответственности. В завершение — добавить в кодексы юридическую ответственность за каждое действие. Из-за отсутствия четкого регламента возникает как возможность наказания невиновных, так и опасность безнаказанности виновных лиц.

Таким образом, быстрое внедрение глобальных сетей в жизнь общества требует радикальных изменений в законодательстве государства с целью обеспечения защиты прав и свобод граждан.

Библиографический список

1. Конституция Российской Федерации (принята всенародным голосованием 12 декабря 1993 г.) (с учетом поправок, внесенных Законами Российской Федерации о поправках к Конституции Российской Федерации от 30.12.2008 г. № 6-ФКЗ, от 30.12.2008 г. № 7-ФКЗ, от 05.02.2014 г. № 2-ФКЗ, от 21.07.2014 г. № 11-ФКЗ) // СПС «Гарант-Сервис» [электронный ресурс]. – URL: <https://base.garant.ru/10103000>.
2. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (с изм. и доп. от 12.04.2020 г.) // СПС «КонсультантПлюс» [электронный ресурс]. – URL: http://www.consultant.ru/document/cons_doc_LAW_10699.
3. Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ (ред. от 24.04.2020 г.) // СПС «КонсультантПлюс» [электронный ресурс]. – URL: http://www.consultant.ru/document/cons_doc_LAW_34661.
4. Федеральный закон от 7 февраля 2011 г. № 3-ФЗ «О полиции» // СПС «КонсультантПлюс» [электронный ресурс]. – URL: http://www.consultant.ru/document/cons_doc_LAW_110165.
5. Федеральный закон от 25 июля 2002 г. № 114-ФЗ «О противодействии экстремистской деятельности» (с изменениями и дополнениями) // СПС «Гарант-Сервис» [электронный ресурс]. – URL: <https://base.garant.ru/12127578/>
6. Указ Президента Российской Федерации от 6 сентября 2008 г. № 1316 (ред. от 05.09.2011) «О некоторых вопросах Министерства внутренних дел Российской Федерации» // СПС «КонсультантПлюс» [электронный ресурс]. – URL: http://www.consultant.ru/document/cons_doc_LAW_79834.
7. Золоева, З. Т. Некоторые проблемы правового противодействия экстремистским проявлениям в информационно-телекоммуникационной сети Интернет / З. Т. Золоева, Б. Г. Койбаев // Гуманитарные и юридические исследования. – 2018. – №4. – URL : <https://cyberleninka.ru/article/n/nekotorye-problemy-pravovogo-protivodeystviya-ekstremistskim-proyavleniyam-v-informatsionno-telekommunikatsionnoy-seti-internet> (дата обращения: 11.12.2020). – 13 с.
8. Уголовное право. Общая часть. Практикум : учебное пособие для вузов / [И. Я. Козаченко и др. ; под ред. И. Я. Козаченко]. – 2-е изд., перераб. и доп. – М. : Юрайт, 2020. – 355 с. – (Высшее образование). – ISBN 978-5-534-05393-7. – Текст : электронный // ЭБС Юрайт [сайт]. – URL: <https://urait.ru/bcode/450042> (дата обращения: 11.12.2020).
9. Шакирьянов, М. М. Пути повышения эффективности расследования преступлений экстремистской направленности в сети Интернет / М. М. Шакирьянов // Вестник Казанского юридического института МВД России. – 2018. – № 4 (34). – URL: <https://cyberleninka.ru/article/n/puti-povysheniya-effektivnosti-rassledovaniya-prestupleniy-ekstremistskoy-napravlenosti-v-seti-internet> (дата обращения: 11.12.2020). – 15 с.

*Агеенков А. А.¹,
начальник кафедры оперативно-разыскной деятельности
Рязанского филиала Московского университета МВД России
имени В.Я. Кикотя, кандидат юридических наук*

ОСОБЕННОСТИ ПРОВЕДЕНИЯ ОПЕРАТИВНО-РАЗЫСКНЫХ МЕРОПРИЯТИЙ В ИНФОРМАЦИОННО- КОММУНИКАЦИОННОЙ СРЕДЕ В ПЕРИОД ДЕЙСТВИЯ ПРАВОВОГО РЕЖИМА КОНТРТЕРРОРИСТИЧЕСКОЙ ОПЕРАЦИИ

Оперативно-разыскные мероприятия, проводимые в целях проверки почтовой, телеграфной и другой коммуникации, прослушивание разговоров по телефону, снятие данных с телекоммуникационных каналов при режиме контртеррористической операции (далее – КТО) реализуется с учетом нормы контроля коммуникаций по различным каналам передачи информации, а также поиска данных в почтовых и электронных переписках для нахождения сведений о террористической деятельности, о персоналиях, замешанных в ее реализации, а также для превентивных мер в отношении террористических атак.

Уполномоченные сотрудники государственных служб выполняют снятие данных с технических коммуникационных каналов и осуществляют прослушивание разговоров неопределенного числа граждан, которые находятся в районе режима КТО.

Более того, в зависимости от обстоятельств прослушивание переговоров по телефону может производиться тремя путями. Первый предполагает прослушивание всей телефонной коммуникации в зоне КТО. Второй – прослушивание переговоров, в которых фигурируют определенные фразы или словосочетания (названия вооружений, боеприпасов, службы госбезопасности и др.). Третий – контроль коммуникации только в той области, где совершенно точно присутствуют лица, причастные к террористической деятельности. Все три пути требуют от оперативников наличия определенных технических и административных ресурсов. Следует отметить, что нередко органы суда не дают своего согласия на реализацию подобных мероприятий, если лица, переговоры которых должны прослушиваться, четко не определены. В подобных ситуациях необходимо действовать согласно постановлению ВС РФ от 05.06.2014, где говорится, что в определенных ситуациях в запросах на реализацию оперативно-разыскной деятельности, которая ущемляет в правах население, необязательно присутствие информации о конкретном гражданине, в отношении которого такая деятельность планируется. Более того, это постановление допускает выполнение оперативно-разыскной деятельности в отношении нескольких граждан, личности которых не установлены.

Рассматривая вопрос приостановления оказания услуг связи юридическим и физическим лицам или ограничения использования сетей связи и средств связи, следует учитывать тот факт, что в соответствии с постановлением Правительства

¹ © Агеенков А. А., 2020.

Российской Федерации от 31 декабря 2004 г. № 895 при приостановлении использования сетей связи и средств связи предусматривается полное прекращение их использования другими пользователями на время проведения работ по ликвидации чрезвычайных ситуаций, а при ограничении использования любых сетей связи и средств связи предусматривается сокращение их использования другими пользователями (изменение режимов работы средств связи, объемов оказываемых услуг связи и т. д.) на время проведения работ по ликвидации чрезвычайных ситуаций. Таким образом, приостановление оказания услуг связи осуществляется в отношении конкретного абонента и несет за собой полное прекращение использования этим лицом услуг связи, указанных в постановлении. В свою очередь, ограничение использования сетей связи и средств связи осуществляется в отношении широкого круга лиц и предусматривает возможность отключения только некоторых функций связи.

В соответствии с ч. 3 ст. 64 Федерального законодательного акта глава госоргана, реализующего ОРД, или служб по обеспечению госбезопасности Российской Федерации в ситуациях, предусмотренных актуальным федеральным законодательством, может направлять письмо операторам сотовой связи с аргументированным требованием о прекращении предоставления коммуникационных услуг определенным физлицам или юрлицам. [1]

Более того, на основании ч. 1 ст. 15 Федерального законодательного акта об оперативно-разыскной деятельности, органы правопорядка могут использовать эту меру, если существует объективная опасность для жизни и состояния здоровья гражданина, а введение режима КТО в перечне оснований не присутствует, невзирая на то, что КТО в большинстве случаев происходит уже после террористического акта, в то время, когда опасность для здоровья и жизни граждан снизилась.

Об ограничении доступа для граждан в Федеральном законодательном акте «О Коммуникациях» говорится только в ст. 66 и только в контексте природных или технологических чрезвычайных происшествий и никак не затрагивает аспект противодействия государства террористической деятельности.

Проблема состоит в неполном раскрытии текущим законодательством процесса реализации двух последних мер уполномоченными на осуществление ОРД госорганами.

Так, согласно Указу Президента Российской Федерации, ограничивать доступ граждан к средствам телефонной коммуникации и прослушивать переговоры по ним имеют право только соответствующие подразделения Федеральной службы безопасности Российской Федерации. [2]

Если у сотрудников ФСБ России нет возможности реализовать подобную деятельность, задача по ее реализации ложится на плечи МВД России. В то же время декреты Министерства внутренних дел Российской Федерации не предусматривают проведения подобных действий, хотя в отдельных нормативных актах выдвигается предложение о скоординированной работе ПСТМ, ФКУ НПО «Специальная техника и связь» МВД России и Федеральной службы безопасности Российской Федерации по разработке механизма быстрого ограничения доступа определенным пользователям к каналам коммуникации при сложных опе-

ративных ситуациях в определенном субъекте Российской Федерации для дестабилизации деятельности лиц, планирующих реализацию экстремистских актов.

В ситуациях, когда контртеррористическая операция с самого начала связана с необходимостью освобождения заложников или когда такая необходимость возникает в ходе операции, организация оперативно-разыскного обеспечения зависит от варианта их захвата и удержания. В случае, когда захваченные террористами заложники содержатся на определенном объекте, органам власти или правоохранительным органам предъявляются требования как условие их освобождения. Такая обстановка сводит к минимуму возможности оперативно-разыскного обеспечения. Основная возможность получения какой-либо информации связывается в основном с ведением переговоров с преступниками. Другой вариант, когда заложники удерживаются в месте, скрываемом от правоохранительных органов, а преступники предъявляют требования о выкупе либо принуждения должностных лиц к противоправным действиям. В проводимых оперативно-разыскных мероприятиях преобладают негласные действия. В этих случаях, когда преступниками выдвигаются требования передать им оружие, защитные средства и т. п., такие требования должны отвергаться.[3]

При осуществлении оперативно-разыскной деятельности могут быть получены данные о намерениях тех или иных групп террористов совершить захват заложников, подготовке к захвату воздушного судна или иных террористических актах, поступить информация о подготовке массовых беспорядков и т. п. К этому необходимо добавить и задачи обеспечения информацией руководителей операции для принятия оптимальных управленческих решений, проведения конкретных оперативно-разыскных мероприятий, направленных на создание благоприятных условий ведения операции, освобождение заложников или их части, склонение, насколько это возможно, террористов и экстремистов к отказу от преступных действий и добровольной сдаче. Конечно, в современных условиях такой благоприятный исход является скорее исключением, чем правилом, однако не следует пренебрегать даже малейшей возможностью, чтобы завершить операцию без жертв либо свести их к минимуму.[4]

Оперативно-разыскные мероприятия, проводимые в ходе контртеррористической операции в информационно-коммуникационных сетях, позволяют получать сведения, которые в итоге могут послужить основанием для проведения следственных действий. На основе полученных результатов оперативно-разыскной деятельности могут быть собраны такие доказательства по уголовному делу, которые в результате позволят решать вопросы о привлечении к уголовной ответственности обвиняемых в совершении преступлений террористической направленности, уменьшении последствий (возмещения вреда) от террористических актов, предупреждении экстремистской, террористической иной противоправной деятельности.

Библиографический список

1. Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи» // СПС «Консультант Плюс». – URL: http://www.consultant.ru/document/cons_doc_LAW_43224.

2. Указ Президента Российской Федерации от 1 сентября 1995 г. № 891 «Об упорядочении организации и проведения оперативно-розыскных мероприятий с использованием технических средств» // Собр. законодательства Рос. Федерации. – 1999. – № 24. – Ст. 2954.

3. Василега, О. П. Вопросы оперативно-розыскного обеспечения действий органов внутренних дел в особых условиях // Совершенствование управления ОВД в особых условиях. – Труды Акад. МВД СССР. – 1991. – С. 57–62.

4. Анищенко, А. Ю. Тактико-специальная подготовка сотрудников органов внутренних дел к действиям при чрезвычайных обстоятельствах : учебное пособие. – М., 2006. – С. 193–198.

Желнов И. И.¹,
 заведующий кафедрой информационной
 безопасности Института Государственного
 управления, права и инновационных технологий,
 кандидат военных наук

Голубев А. Ю.²,
 профессор кафедры информационной
 безопасности Института Государственного
 управления, права и инновационных технологий,
 кандидат философских наук

Агнистов Н. Г.³,
 студент Института Государственного
 управления, права и инновационных технологий

КЛАССИФИКАЦИЯ СПЕЦСЛУЖБ, КОНТРОЛИРУЮЩИХ ИНТЕРНЕТ (НА ПРИМЕРЕ США)

Для полного понимания достаточности контроля Интернета необходимо на примере других стран рассмотреть спектр организаций, ведомств и подразделений, задействованных в выявлении и предотвращении проявлений экстремизма и других противоправных действий в сети. По административной принадлежности такие службы можно разделить на федеральные, ведомственные, общественные и частные организации. По выполняемым задачам они условно подразделяются на ведомства, призванные защищать сетевые сегменты от вторжений и выявлять противоправную деятельность в сетях, а также на ведомства, проводящие оперативно-разыскную деятельность в сфере сетевых технологий.

К федеральным организациям можно отнести следующие.

1. NIPC (National Infrastructure Protection Center), Центр защиты национальной инфраструктуры. Занимается координационной деятельностью по защите критически важных элементов инфраструктуры США, к которым отнесены сети электроснабжения, транспортные сети, нефтегазовые комплексы, системы водоснабжения, службы государственной безопасности и правительственные учреждения, финансовые и банковские системы. К этому же перечню отнесены телекоммуникационные и компьютерные системы и сети как часть информационной инфраструктуры США. В части своих функций, NIPC контролирует стратегически важные телекоммуникационные компании, которые организовывали защиту сетей с непосредственным участием правительственных ведомств, в частности ФБР. Также NIPC ведет перечень телекоммуникационных и компьютерных сетей и поддерживающих их компаний, составляющих основу информационной инфраструктуры США.

¹ © Желнов И. И., 2020.

² © Голубев А. Ю., 2020.

³ © Агнистов Н. Г., 2020.

Под эгидой NIPC функционируют некоторые общественные формирования государственного масштаба, содействующие сбору важной для защиты инфраструктуры США информации частного сектора. Так, согласно перечню элементов инфраструктуры, организованы соответствующие центры анализа и распространения информации (ISACs, Information Sharing and Analysis Centers). Есть ISAC, занимающийся сбором, анализом и распространением информации о случаях, представляющих опасность для телекоммуникационной и компьютерной сетевой информационной инфраструктуры крупнейших коммерческих организаций страны. К этому центру присоединилось множество банков и финансовых учреждений США.

2. FedCIRC (Federal Computer Incident Response Center), Федеральный центр реагирования на компьютерные инциденты. Центр ориентирован на защиту национальной сетевой инфраструктуры, находится под эгидой ФБР, тесно взаимодействует с NIPC. В задачи центра входят:

- организационная деятельность на федеральном уровне, по объединению различных государственных структур США в противодействии компьютерным инцидентам, связанным с вторжением в сети;
- обеспечение заинтересованных сторон и организаций информацией по вторжениям в сети и мерам по их защите;
- решение различных вопросов безопасности компьютерных сетей на уровне государства во взаимодействии с NIPC (разработка государственных систем защиты сетей, выявление угроз национальной сетевой инфраструктуре).

Если федеральные ведомства в основном занимаются координационной и информационной деятельностью по рассматриваемым здесь вопросам, то ведомственные организации, призванные контролировать Интернет, являются непосредственными исполнителями.

1. NIPC (National Information Protection Center), Национальный центр защиты информации.¹ Являясь подразделением ФБР, занимается вопросами защиты информационной инфраструктуры США, а именно той ее части, которую составляют телекоммуникационные и компьютерные сети и технологии.

2. NCCS (National Computer Crime Service), Национальная служба по борьбе с компьютерными преступлениями. Организационно входит в ФБР, в NIPC, имеет свои подразделения в крупных городах США. Расследует преступления и случаи мошенничества, связанные в основном с компьютерной средой. В перечень преступлений, которыми занимается эта служба, относятся и другие преступления, связанные с высокими технологиями. К таковым можно отнести кражи номеров кредитных карточек, бесплатное пользование телефонными и другими услугами связи, финансовые мошенничества и незаконные азартные игры в компьютерной сетевой среде.

3. CITAC (Computer Investigation and Infrastructure Threat Assessment Center, Центр расследования компьютерных преступлений и оценки угрозы инфраструктуре). Является подразделением ФБР. В отличие от NCCS занимается борьбой с преступлениями, связанными с безопасностью информационной ин-

¹ Не путать с National Infrastructure Protection Center.

фраструктуры и сетями управления других инфраструктур. СІТАС занимается выявлением и установлением контроля над слабыми местами сетей управления воздушным транспортом, водоснабжением, энергоснабжением, денежными переводами, сетями телефонной и другой связи. Ведет расследование случаев аварий в сетях управления инфраструктурами и крупными предприятиями, а также расследует кражи в банковских сетях.

4. CART (Computer Analysis and Response Team), группа компьютерного анализа и реагирования. Подразделение ФБР. Задействуется в расследовании всех видов преступлений, там, где необходима поддержка других отделов и служб в сфере компьютерных технологий. Проводит экспертизы и формирует улики для подразделений ФБР, в том числе и для СІТАС.

5. JTFCND (Joint Task Force for Computer Network Defense). Объединенная целевая группа по защите компьютерных сетей. Организация Министерства обороны США. По своим функциям эквивалентна NIPC (ФБР). Занимается защитой компьютерных сетей Министерства обороны. При обнаружении подозрительных действий в сетях, в том числе и общих, используемых Министерством обороны, группа их проверяет на криминал и вторжение в сетевой сегмент управления обороной страны. Действия, классифицированные как криминальные, передаются на разработку для соответствующих подразделений ФБР.

Нами приведены не все государственные организации, службы, отделы и группы США, осуществляющие оперативно-разыскную деятельность в компьютерных сетях и сферах, связанных с ними, а лишь те, которые упоминаются в открытых источниках наиболее часто и чьи задачи по этим источникам можно было здесь сформулировать (таблица).

Таблица

Классификация подразделений спецслужб США, проводящих оперативно-разыскные мероприятия в среде телекоммуникационных сетей и Интернета

Выполняемые задачи	Подразделения	
Выявление сетевых аномалий и защита сетевой инфраструктуры	Федеральный уровень	NIPC (National Infrastructure Protection Center), Центр защиты национальной инфраструктуры; FedCIRC (Federal Computer Incident Response Center), Федеральный центр реагирования на компьютерные инциденты; NIPC (National Information Protection Center), Национальный центр защиты информации
	Ведомственный уровень	JTFCND (Joint Task Force for Computer Network Defense) Объединенная целевая группа по защите компьютерных сетей

Окончание таблицы

Оперативно-разыскная деятельность по расследованию сетевых преступлений	Расследование сетевых преступлений	NCCS (National Computer Crime Service) Национальная служба по борьбе с компьютерными преступлениями
	Расследование преступлений с применением сетей	CITAC (Computer Investigation and Infrastructure Threat Assessment Center) Центр расследования компьютерных преступлений и оценки угрозы инфраструктуре
	Техническое содействие оперативным подразделениям	CART (Computer Analysis and Response Team) группа компьютерного анализа и реагирования

Таким образом, приведенный обзор на примере США позволил классифицировать различные по решаемым задачам, подготовке и оснащению подразделения, задействованные в борьбе с противоправной деятельностью в Интернете.

Желнов И. И.¹,
заведующий кафедрой информационной
безопасности Института Государственного
управления, права и инновационных технологий,
кандидат военных наук

Харьков В. А.²,
студент Института Государственного
управления, права и инновационных технологий

АНАЛИЗ ИСПОЛЬЗУЕМЫХ ЗАРУБЕЖНЫМИ СТРАНАМИ ТЕХНИЧЕСКИХ СРЕДСТВ КОНТРОЛЯ ИНТЕРНЕТА (НА ПРИМЕРЕ США)

Номенклатура технических средств, применяемых для выделения информационных потоков Интернета из потоков данных в сетях электросвязи отображает последовательный процесс демодуляции, декодирования и «распротоколирования». О таком процессе можно судить как по построению системы электросвязи, так и по спектру оборудования, сбора и анализа данных, производимого рядом фирм США для своих спецслужб.

Одними из крупнейших производителей радиоэлектронного оборудования такого рода в США являются такие фирмы, как Applied Signal Technology (AST) (Саннивейл, Калифорния) и IDEas (Мэрилэнд, Колумбия). Крупнейшим заказчиком оборудования этих фирм является Агентство Национальной Безопасности (АНБ).

Наибольшее разнообразие оборудования требуется при несанкционированном съеме данных – перехвате, поскольку выделение и обработка сигналов происходит от самого нижнего уровня – доступа к среде передачи сигналов электросвязи. Различные физические интерфейсы подключения к линиям связи, УКВ и спутниковые антенны, производимые в основном фирмами Lockheed Martin, Spase Systems/Loral, TRW, Raytheon и Bendix не раскрываются.

Полный перечень оборудования можно представить в следующей классификации, на примере изделий фирмы AST.

1. Анализаторы широкополосных сигналов в линиях связи.

Назначение такого класса аппаратуры – определение системы связи, способов уплотнения каналов, используемых стандартов многоканальных линий, выделение отдельных каналов в многоканальных линиях связи.

Эту группу представляют транспондеры, демодуляторы, декодеры, мультиплексоры, анализаторы микроволновых линий связи, системы анализа несущего сигнала и другие виды изделий. Помимо анализа широкополосных сигналов в режиме реального времени предусматривается их запись на скоростях того же порядка, что и в перехватываемых каналах, для их последующей обработки.

¹ © Желнов И. И., 2020.

² © Харьков В. А., 2020.

Модель 196 (AST)	– система определения транспондера.
Модель SNAPER-195 (AST)	– мгновенный анализатор широкополосных сигналов.
Модель 990 (AST)	– универсальное устройство сбора данных.
Модель 256A (AST)	– анализатор микроволновых линий.

Последние две системы способны записывать воспроизводить и анализировать данные на скоростях до 2488 Гбит/сек.

Модель 257E (AST)	– анализатор сигналов в синхронных оптических линиях Sonet.
Демодуляторы	– 245A/F, 245D, 245XP, 255 A/E.
Демультимплексоры	– 245S; 252AF; 257D; B257D.

К таким устройствам может быть подключен блок с сетевыми компьютерными выводами (например, изделие 330NT/300 для Ethernet) для разведения перехваченных данных после их демодуляции и демультимплексирования по компьютерам локальной сети, для их последующего анализа.

Кроме того, перехваченные данные могут направляться в другие, лучше оборудованные подразделения, по собственным распределенным сетям систем радиоперехвата. Такую возможность, например, обеспечивает компьютерный интерфейс B990, формирующий собранные данные в стандарт CSDF (Collected Signals Data Format), предусматривающий описание не проанализированного на предмет протоколов потока данных канала связи.

Приведенный перечень устройств разрабатывается с такими характеристиками, чтобы перекрывать скорости существующих стандартов широкополосных каналов различных линий. Таких как США T1 – T4 до 274 Мбит/с; Sonet (STS1 – STS192) и SDH (STM1 – STM64) до 9953,28 Мбит/с.

2. Многоканальные процессоры и анализаторы протоколов.

Основная функция – анализ каналов передачи данных, выделение видовых каналов (голос, факс, передача данных), определение и анализ протоколов выше канального уровня.

Модель 120 (AST) – (многоканальный процессор) в конфигурациях STARQVAEE, COBRA, COPPERHEAD обрабатывает одновременно до 1000 речевых каналов и автоматически выделяет факс и речь.

Модель 128 (AST) – обрабатывает до 16 каналов E-3 (500 Мбит/сек) и выделяет до 480 видовых каналов.

Модель 132 (AST) – выделяет до 3000 речевых каналов из 567000 каналов связи.

Модель 113A (AST) – разделяет каналы по видам, определяет протоколы сетевого уровня и компьютерных сетей.

В этот же этап входит анализ протоколов высокого уровня. А именно, выделение сессий транспортного уровня, передач сеансового уровня, прикладных протоколов. В перечне, например, указывается станция ELVIRA.

После анализа каналов и используемых протоколов передачи данных различных уровней в этих каналах начинается компьютерная обработка. Данные отправляются на компьютеры со специальным программным обеспечением, для подготовки их к содержательному анализу. Т. е. прежде чем анализировать содержание, необходимо выделить, например, текст. Возможности таких станций

зависят от мощности используемых компьютеров. В перечне оборудования они называются "Fax Image Workstation" (распознавание графических образов факсов), "Data Workstation" (выделение данных) и т. д.

3. Средства содержательного анализа данных.

Для анализа содержания в масштабах реального времени высокоскоростных потоков данных используется не программное обеспечение, а специальные аппаратные реализации, чаще всего как компьютерные платы. В различных материалах приводятся такие изделия как микросхема FDF (Fast Data Finder) фирмы TRW, процессор распознавания образов PRP-9800 (Pattern Recognition Processor) фирмы IDEAS.

В целом, содержательный анализ можно разделить на:

- поточный анализ по ключевым словам и шаблонным данным;
- анализ темы, определяемый частотной встречаемостью слов в документе, не обязательно напрямую связанной с темой;
- анализ содержания аналитиками.

Процесс выделения и обработки потоков данных Интернета из сетей электросвязи с разных технологических уровней подключения контроля, представлен в таблице. Телекоммуникационные сети и системы обозначены сокращением ТКС. Потоки данных любого уровня обозначаются термином «трафик». Криптоанализ данных опускается.

Таблица

Выделение и анализ потоков данных Интернета в сетях электросвязи

Уровень подключения к сети → Этапы обработки данных ↓	I. Перехват (среда передачи)	II. Каналообразующие узлы транспортных сетей	III. Узлы ТКС сетей	IV. Транзитные IP-узлы Интернета	V. Прикладные узлы Интернета
(1) Физическое подключение к линии связи	Специальные антенны и физические интерфейсы	Стандартные физические интерфейсы (антенны, разъемы, и т. д.)			
(2) Выделение каналов много- канальных линий	Специальное оборудование		Стандартное оборудование разделения каналов многоканальных линий связи		
(3) Выделение трафика наложенных ТКС сетей	Специальное оборудование			Стандартное оборудование соответствующих ТКС систем	
(4) Выделение IP трафика, наложенного на ТКС сети	Специальные аппаратно-программные средства				Стандартные программные IP-интерфейсы
(5) Выделение сообщений и фрагментов	Специальные программные средства				

(6) Автоматический анализ а) шаблонный б) образный, смысловой	Специальные программные средства
(7) Работа аналитиков: содержательный анализ; структурный анализ	Аналитические подразделения спецслужбы

Столбцы I – V таблицы представляют технологические уровни узлов электросвязи и аппаратуры, с которых организуется съем потоков данных специальными средствами контроля, от каналобразующей аппаратуры на узлах транспортных сетей (столбец II) до прикладных, – почтовых, FTP, WWW, и других узлов Интернета (столбец V). От технологического уровня контролируемого узла зависит, какой набор стандартных аппаратных и программных средств, входящих в состав узла, либо дополнительно устанавливаемых, а также набор специального оборудования и программ, используется для оснащения его контроля. Такой набор средств, например, «черный ящик» у провайдера Интернета, представляется как *техническая точка контроля*.

Этапы обработки и анализа потоков данных (строки 1–7 таблицы), относительно уровня подключения контроля обозначены серым фоном.

Под структурным анализом связи, в таблице понимается накопление и обработка информации о маршрутах передаваемых данных, временных характеристиках, используемых протоколах, и т. д. Условно говоря, структурный анализ подразумевает выявление «почерка» связи.

Таким образом, рассмотрение структуры Интернета как наложенной на сети электросвязи информационной системы, а также группировка указанных выше технических средств, позволяет представить в обобщенном виде процесс обработки данных от потоков сигналов в линиях связи до содержательной информации, применительно к трафику Интернета. Этот процесс поможет верифицировать спектр адресных, шаблонных и структурных ориентировок на потоки данных, определенных ранее, по которым может работать любая техническая распределенная система, контролирующая часть сетевого пространства.

Охонько Е. А.¹,

начальник кабинета специальных дисциплин

кафедры специальных информационных технологий

Московского университета МВД России имени В.Я. Кикотя,

старший лейтенант полиции

ПРИМЕНЕНИЕ МАССОВЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ЭКСТРЕМИСТСКИМИ ОРГАНИЗАЦИЯМИ

Массовое развитие информационных технологий оказало влияние на политическую жизнь общества. Ведущие державы применяют массовые информационные технологии в военно-политических конфликтах, активно используют их для влияния на общественное мнение, а также поведение людей.

Информационными технологиями в соответствии с Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»² являются процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

На сегодняшний день самым популярным способом предоставления и распространения информации в современном мире являются социальные сети.

Противодействие использованию социальных сетей экстремистскими организациями является важным вопросом для государства. Экстремистские организации используют в своей незаконной деятельности социальные сети по целому ряду причин, начиная от распространения информации экстремистского содержания по сути и пропаганды экстремистских взглядов до финансирования своей деятельности, вербовки и обмена координационной информацией.

Для решения данной проблемы необходимо, во-первых, наладить коммуникацию с создателями социальных сетей, во-вторых, организовать модерацию контента (содержания). Безусловно, возникает вопрос, касающийся свободного выражения мнения и уместности ограничения на свободу слова.

Борьба с экстремистами в социальных сетях требует различных методов, в том числе и принятия соответствующих нормативных правовых актов.

В стратегии национальной безопасности Российской Федерации, утвержденной указом Президента Российской Федерации от 31 декабря 2015 г. № 683, говорится, что деятельность, которую осуществляют экстремистские организации, является одной из основных угроз государственной, а также общественной безопасности[4].

Принимая во внимание угрозы, которые возникают от экстремистских организаций, для обеспечения национальной безопасности Российской Федерации и на основе требований ст.ст. 13, 19 и 29 Конституции Российской Федерации в 2002 году был принят Федеральный закон от 25 июля 2002 г. № 114-ФЗ

¹ © Охонько Е. А., 2020.

² Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СПС «КонсультантПлюс». – URL: http://www.consultant.ru/document/cons_doc_LAW_61798.

«О противодействии экстремистской деятельности» [2]. В упомянутом законе было определено значение федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации и органов местного самоуправления в противодействии экстремистской деятельности [3]. Кроме того, в п. 1 ст. 1 обозначено, что экстремистской деятельностью является насильственное изменение основ конституционного строя.

Также стоит отметить, что Президентом Российской Федерации был подписан Указ Президента Российской Федерации от 29 мая 2020 г. № 344 «Об утверждении Стратегии противодействия экстремизму в Российской Федерации до 2025 года» [5].

Массовые информационные технологии являются на данный момент мощным оружием в руках экстремистских организаций.

В последние годы усилилось явление, часто называемое «подстрекательством к насильственному экстремизму». В основном это касается Интернета в целом и социальных сетей в частности. Попытки предотвратить это явление создали проблемы для свободы слова. Они варьируются от неизбирательных блокировок, чрезмерной цензуры (затрагивающей как журналистов, так и блогеров) и вторжений в частную жизнь – вплоть до подавления средств массовой информации. Но как нам кажется, что эти средства оправданы.

Библиографический список

1. Конституция Российской Федерации (принята всенародным голосованием 12 декабря 1993 г.) (с учетом поправок, внесенных Законами Российской Федерации о поправках к Конституции Российской Федерации от 30.12.2008 г. № 6-ФКЗ, от 30.12.2008 г. № 7-ФКЗ, от 05.02.2014 г. № 2-ФКЗ, от 21.07.2014 г. № 11-ФКЗ) // СПС «Гарант-Сервис» [электронный ресурс]. – URL: <https://base.garant.ru/10103000>.
2. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СПС «Консультант-Плюс». – URL: http://www.consultant.ru/document/cons_doc_LAW_61798.
3. Федеральный закон от 25 июля 2002 г. № 114-ФЗ «О противодействии экстремистской деятельности» (с изм. и доп. от 31.07.2020). // СПС «Гарант». – URL: <https://base.garant.ru/12127578>.
4. Указ Президента Российской Федерации от 31 декабря 2015 г. № 683 «О Стратегии национальной безопасности Российской Федерации» // СПС «КонсультантПлюс». – URL: http://www.consultant.ru/document/cons_doc_LAW_191669.
5. Указ Президента Российской Федерации от 29 мая 2020 г. № 344 «Об утверждении Стратегии противодействия экстремизму в Российской Федерации до 2025 года» // СПС «Гарант-Сервис». – URL: <https://www.garant.ru/products/ipo/prime/doc/74094369>.
6. Барцевич, А. А. Использование информационно-телекоммуникационного пространства (социальных сетей) в экстремистских целях, как элемент современных войн // Сборник статей по материалам LXXVIII международной научно-практической конференции. – М., 2020. – С. 21–28.

7. Ганаева, Е. Э. Использование массовых информационных технологий экстремистскими организациями / Е. Э. Ганаева, Ш. Ш. Муцалов // Армия и общество. – 2014. – № 2 (39). – URL: <https://cyberleninka.ru/article/n/ispolzovanie-massovyh-informatsionnyh-tehnologiy-ekstremistskimi-organizatsiyami>.

8. Музафина, В. М. Массовые информационные технологии как фактор анонимизации сознания молодежи // Дискуссия. – 2016. – №4 (67). – URL: <https://cyberleninka.ru/article/n/massovye-informatsionnye-tehnologii-kak-faktor-anonimizatsii-soznaniya-molodezhi>.

Карпова А. Г.¹,

*курсант 382 учебного взвода
института подготовки сотрудников
для органов предварительного расследования
Московского университета МВД России имени В.Я. Кикотя*

Гончар В. В.²,

*заместитель начальника кафедры информационной безопасности
учебно-научного комплекса информационных технологий
Московского университета МВД России имени В.Я. Кикотя,
кандидат юридических наук, полковник полиции*

ОСОБЕННОСТИ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ КРИПТОВАЛЮТЫ

В наше время особо актуальной является проблема расследования преступлений, которые совершаются с использованием криптовалюты. С каждым днем эволюционные процессы в большем объеме затрагивают все сферы жизнедеятельности общества. Немаловажным является процесс разработки и использования современных технологий и в том числе тесная связь современного человека с финансовыми средствами. Известность криптовалюты, в первую очередь, связана с ее техническими параметрами и возможностями, а именно: вероятностью деления одной единицы на миллионные доли, безвозвратностью транзакции и другими отличительными «маневрами».

Также, с применением информационных технологий в финансово-кредитной системе используются новые технические средства и методы для совершенствования финансовой деятельности и денежных расчетов. Большую роль играет внедрение заочного использования денежных средств с помощью определенных систем, таких как QIWI, Apple pay, WebMoney и др. Важно дополнить, что преступления, совершенные на базе данных электронных кошельков и систем являются тяжело расследуемыми наравне с киберпреступлениями.

Почему же можно сделать вывод, что финансовые технологии вышли на новый уровень, который является, в свою очередь, мировым? Конечно же, об этом свидетельствует распространение криптовалюты, используемой на основе системы «Блокчейн».

В России 22 июля 2020 г. принят закон о «Цифровых финансовых активах» (ЦФА), где появилось официально закрепленное определение криптовалюты, но ее использование, оплата ее услуг и товаров невозможна. В законе говорится, что биткоин – это некая совокупность электронных данных, которые содержатся в информационной системе и могут быть использованы в качестве денежного платежа. Но также в определении отмечено, что он не является денежной единицей Российской Федерации (в соответствии с ч. 1 ст. 75 Конституцией Российской Федерации денежной единицей в Российской Федерации является рубль,

¹ © Карпова А. Г., 2020.

² © Гончар В. В., 2020.

денежная эмиссия осуществляется исключительно Центральным банком России, а введение и эмиссия других денег в Российской Федерации не допускается [1]), иностранных государств, способом инвестиций и др. Данный закон должен вступить в силу с 1 января 2021 г. Мы считаем, что в законе «О цифровых финансовых активах» Российская Федерация нуждалась давно, и расследование уголовных дел станет более активным.

Несмотря на то, что криптовалюта по своей сущности виртуальна, она является собственностью, следовательно, имеет свой рынок, форму реализации (криптообменники и биржи), а это значит, что данная единица должна быть урегулирована на законодательном уровне.

Уголовный кодекс Российской Федерации также соприкасается с криптовалютой. Так, например, в постановлении Пленума Верховного суда Российской Федерации о практике по делам о легализации доходов отмечалось, что запрещено отмывать доходы с помощью криптовалют. Согласно данному постановлению [2] предметом преступлений, предусмотренных ст.ст. 174 и 174.1 УК РФ о легализации преступных доходов, теперь следует считать и преобразованные из виртуальных активов (криптовалюты), которые получены в результате преступной деятельности. Так как криптовалюта не регулируется нормативно ни в одной из стран, ее учет децентрализован. Каждая операция, которая проходит с ее участием, проверяется майнерами. Без их участия криптовалюта существовать не может.

В расследовании преступлений, связанных с криптовалютой, правоохранные органы пользуются тем, что блокчейн максимально доступен и открыт, следовательно, можно без существенных затрат и усилий получить доступ к историям транзакций.

Правоохранительные органы могут также отследить денежные средства непосредственно на основании особенностей биткоина, так как записи относятся к первой транзакции этих средств. То есть отсутствует анонимность, адрес является и номером счета.

В свою очередь, справедливо высказалась О. Скоробогатова: криптовалюта – это «высокорискованный инструмент...не секрет, что 90 % операций связаны с мошенническими операциями. Это не значит, что их надо запретить. Это значит, что сейчас пока больше вопросов, чем ответов» [3].

Организованная преступность отлично ознакомлена о формах, способах и средствах оперативно-разыскной работы. В собственном арсенале содержит высочайшего уровня материально-техническое и экономическое обеспечение, и при изготовлении и совершении преступлений использует не лимитированные возможности сети Интернет. В наши дни в данной сети можно найти все, применяя все особенности технического функционирования.оборот валютных средств не считается исключением. Злоумышленники, применяя криптовалюту, проводят большие валютные переводы через Интернет, чем наиболее четко показывают уход от классических денежных систем, и пользуются ей для совершения не только финансовых преступлений, но и при торговле людьми, сбыте наркотиков, оружия и т. д.

Есть список сведений, которыми должен обладать сотрудник органов предварительного расследования при расследовании преступлений, совершенных с применением криптовалюты:

- информация о платёжной системе;
- сведения о порядке оборота криптовалюты;
- сведения об обороте осуществлений транзакций.

Успешное расследование таких преступлений зависит квалификации специалистов в области IT-технологий.

В том числе следует провести ряд мероприятий, которые помогут установить время и территориальную принадлежность совершения киберпреступлений. Так как установление данных событий содержит особенности, связанные со спецификой данных преступлений. Например, проведение операций с криптовалютами может осложняться тем, что месторасположение правонарушителя с местоположением аппаратных и программных средств совершения преступления совпадать не будут. Относительно времени нужно учитывать, что киберпреступления совершаются в разных часовых поясах и с разной кодировкой.

Тем не менее, в связи с тем, что информация обо всех операциях в Сети находится в открытом доступе, ученые, получив исчерпывающие данные, пришли к выводу, что имеется некая структура, которая свидетельствует о наличии скрытых объединений НОД, основанных в 2012 г. [4].

В свою очередь, биткоин представляет собой большую угрозу всему миру из-за неполного и ненадлежащего контроля за распространением криптовалют. Контроль важен как на федеральном уровне, так и на региональном.

Следовательно, специалистам в области расследования данных преступлений нужно своевременно углублять знания, навыки и умения о различных методиках совершения преступлений с помощью электронных платежных систем, в основе которых лежит криптография.

Важно ввести общую международную юрисдикцию, под которую попадают отношения в отношении криптовалюты и преступников, которые с помощью неё совершают преступления любых категорий, в том числе терроризм, отмывание денег, оборот наркотиков, оборот оружия и др.

Для участия в следственных действиях в соответствии с УПК РФ неотъемлемой частью является привлечение специалистов в области работы с компьютерной информацией, криптографией и т. д. Я считаю, что для правильной подготовки таких специалистов высокого уровня нужно как можно больше создавать направлений обучения в вузах, а также отдельных факультетов, которые будут непосредственно узконаправленными в области информационной безопасности.

Из проведенного анализа следует, что криптовалюту можно использовать не только в целях, которые пагубно отражаются в обществе, но и в положительных аспектах. Так, например, в марте 2020 г. в США предложили использование криптовалюты в борьбе с коронавирусом.

По нашему мнению, современное законодательство должно соответствовать любой обстановке в стране, и было бы неплохо внести поправки в закон «О цифровых финансовых активах», который вступает в силу с 1 января 2021 г., где учитывалась бы эпидемиологическая обстановка и т. п., а также разрешалось

использование криптовалюты в борьбе с пандемией, преступностью и другими пагубными явлениями. Возможно создание определенной цифровой валюты Центральным банком Российской Федерации.

Мы считаем, что современному сотруднику органов внутренних дел необходимо знать тонкости сети Интернет, компьютерных технологий, так как с совершенствованием механизма существования криптовалюты, появляются новые функции и специфические особенности. Они же, в свою очередь, напрямую, связаны с расследованием преступлений с использованием криптовалюты. Считаем целесообразным введение дополнительных курсов по информационной безопасности для борьбы с киберпреступностью и своевременного пресечения преступлений, связанных с криптовалютой.

Библиографический список

1. Конституция Российской Федерации (принята всенародным голосованием 12 декабря 1993 г.) (с учетом поправок, внесенных Законами Российской Федерации о поправках к Конституции Российской Федерации от 30.12.2008 г. № 6-ФКЗ, от 30.12.2008 г. № 7-ФКЗ, от 05.02.2014 г. № 2-ФКЗ, от 21.07.2014 г. № 11-ФКЗ) // СПС «Гарант» [электронный ресурс]. – URL: <https://base.garant.ru/10103000>. (дата обращения 01.07.2020).

2. Постановление Пленума Верховного Суда Российской Федерации от 26 февраля 2019 г. № 1 «О внесении изменений в постановление Пленума Верховного Суда Российской Федерации от 7 июля 2015 года № 32 “О судебной практике по делам о легализации (отмывании) денежных средств или иного имущества, приобретенных преступным путем, и о приобретении или сбыте имущества, заведомо добытого преступным путем”» // Российская газета. – № 51. – 2019. – 7 мар.

3. ЦБ РФ: 90 % операций с криптовалютами связано с мошенничеством // Криптовалюта.Tech [электронный ресурс]. – URL: <https://cryptocurrency.tech/tsbrf-90-operatsij-s-kriptoalyutami-svyazano-s-moshennichestvom/> (дата обращения 01.07.2020).

4. Переверзев К. Кто держит под контролем рынок криптовалют и как этому противостоят обычные трейдеры // Mining-bitcoin: все о криптовалютах [электронный ресурс] – URL: <https://mining-bitcoin.ru/news/kriptoalyuta-kontrol> (дата обращения 01.07.2020).

Луханина А. В.¹,

*курсант Института подготовки сотрудников
для органов предварительного расследования
Московского университета МВД России имени В.Я. Кикотя,
рядовой полиции*

Гончар В. В.²,

*заместитель начальника кафедры информационной безопасности
учебно-научного комплекса информационных технологий
Московского университета МВД России имени В.Я. Кикотя,
кандидат юридических наук*

ПРОТИВОДЕЙСТВИЕ ИСПОЛЬЗОВАНИЮ КРИПТОВАЛЮТЫ В ЭКСТРЕМИСТСКОЙ И ТЕРРОРИСТИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ

В последние несколько лет макроэкономика вышла на новый уровень. Развитие информационных технологий не стоит на месте, что, с одной стороны, является позитивным моментом, а с другой – вызывает беспокойство. Таким образом, возникновение виртуальной валюты, которая на данный момент нередко признается денежным средством, средством платежа, порождает новые проблемы в области безопасности населения и экономики в целом не только отдельно взятой страны, но и всего мира.

Виртуальные денежные средства, которые со временем из простых вычислительных систем превратились в реальное средство платежа и стали участвовать в гражданском обороте, бесспорно, становятся все популярнее в области внедрения и использования в разных сферах существования, в том числе и криминальных. Особое опасение вызывает использование криптовалюты в экстремистской и террористической деятельности, поэтому важно обратить внимание на возможные ограничения, направленные на использование виртуальных денежных средств в целях обеспечения безопасности деятельности государства и населения. Но при этом недопустимо запретить использование виртуальной валюты в результате возможного экономического потенциала. Но операции с криптовалютой кажутся нам высокорискованными.

Создатели криптовалюты уверяют, что использование их изделия надежно и результативно благодаря достоинствам данной валюты, которые, несомненно, привлекает участников экстремистской и террористической деятельности:

1. Криптовалюту нельзя изъять. Собственник, получив ее, может воспользоваться ей в любое время.
2. Отсутствуют комиссии.
3. Эмиссия реализуется строго по заданному алгоритму, что делает криптовалюту независимой от влияния Центробанка и правительства; [4, с. 39].
4. Предусмотрены безмерные возможности транзакции.

¹ © Луханина А. В., 2020.

² © Гончар В. В., 2020.

В то же время необходимо обозначить, что для государства и граждан отсутствие контроля криптовалюты и отслеживания ее движения является несомненным недостатком, но для лиц, осуществляющих террористическую и экстремистскую деятельность, данный пункт может способствовать достижению определенных целей.

В свою очередь, полная анонимность в использовании криптовалюты увеличивает эффективность достижения поставленных целей в экстремистской и террористической деятельности. Соответственно, у пользователя повышается риск быть подвергнутым преступным посягательствам.

Таким образом, встает вопрос о правовом регулировании криптовалюты для предотвращения совершения экстремистской и террористической деятельности. В условиях стремительной информатизации, ускорения и увеличения объема потоков передаваемой информации, изменяется и законодательство. Пласт нормативных актов, направленных на противодействие коррупции, увеличивается с каждым годом.

Так, Российская Федерация встала на новую ступень правового регулирования в сфере оборота криптовалюты. Федеральный закон от 31 июля 2020 г. № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации», но вступит в силу с 1 января 2021 г. Согласно п. 3 ст. 1 под цифровой валютой понимается «совокупность электронных данных (цифрового кода или обозначения), содержащихся в информационной системе, которые предлагаются и (или) могут быть приняты в качестве средства платежа, не являющегося денежной единицей Российской Федерации, денежной единицей иностранного государства и (или) международной денежной или расчетной единицей, и (или) в качестве инвестиций и в отношении которых отсутствует лицо, обязанное перед каждым обладателем таких электронных данных, за исключением оператора и (или) узлов информационной системы, обязанных обеспечивать соответствие порядка выпуска этих электронных данных и осуществления в их отношении действий по внесению (изменению) записей в такую информационную систему ее правилам.» [1]

По мнению председателя Комитета Государственной Думы по финансовому рынку Анатолия Аксакова, криптовалюту надо определить как электронный код, который применяется как средство платежа и средство сбережений, как инвестиция. Но в Российской Федерации его не разрешается использовать для оплаты продуктов и услуг, также под запрет подпадает реклама способов платежа цифровыми деньгами. [2]

Данное определение представляется универсальным и помогает применять его не только к криптоактивам, которые выпущены в отечественных информационных системах под надзором ЦБ РФ в целом, но и, к примеру, к биткоину в отдельности.

По смыслу ст. 10 Федерального закона от 31 июля 2020 г. № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» цифровая валюта признается имуществом. Таким образом, согласно п. 9 постановления Пленума Верховного суда Российской Федерации от 9 июля 2013 г. № 24 «О судебной практике по де-

лам о взяточничестве и об иных коррупционных преступлениях» предметом взяточничества (ст.ст. 290, 291, 291.1, 291.2 УК РФ) и коммерческого подкупа (ст.ст. 204, 204.1, 204.2 УК РФ) вместе с деньгами, ценными бумагами, иным имуществом могут быть нелегальное оказание услуг имущественного характера и предоставление имущественных прав. [3, с. 4]

Таким образом, в Российской Федерации взяткой может считаться передача любой собственности, оказание услуг имущественного характера или предоставление имущественных прав. В связи с этим, информационная валюта по законодательству Российской Федерации является предметом дачи и получения взятки.

В законопроекте сделана отсылка к отдельным законам, которые станут регулировать майнинг, организацию выпуска и обращения электронной валюты в Российской Федерации. В соответствии с Федеральным законом от 31 июля 2020 г. № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» электронная валюта сейчас подлежит указанию в справках о доходах, расходах, об имуществе и обязательствах имущественного характера государственных служащих; должностные лица будут обязаны декларировать существующие у них, их супругов и несовершеннолетних детей электронную валюту и электронные экономические активы, а также раскрывать в сведениях о расходах сделки по их приобретению.

Электронные экономические активы и электронные валюты, которые выпущены в информационных системах, организованных в соответствии с иностранным правом, сейчас отнесены к иностранным финансовым инструментам, и как следствие, отдельным категориям должностных лиц запрещено владеть или пользоваться ими. Таким образом, все вышеуказанные дополнения являются способом борьбы с возможностью использования криптовалюты в экстремистских и террористических целях.

При этом в Налоговый кодекс Российской Федерации поступили поправки, которые вступят в силу с 1 января 2021 г. и касаются использования криптовалют на территории Российской Федерации. Данные поправки имеют своей целью защиту прав и интересов граждан, а также предотвращение преступных операций. Криптовалюта признается имуществом и, соответственно, лица, владеющие данным средством платежа, должны будут представлять отчеты в налоговые органы о приобретении данной валюты, о сделках с ней и об имеющихся остатках в криптокошельке, если операции с криптовалютой превышают 600 тысяч рублей. [5]

Таким образом, изменения в Налоговый кодекс Российской Федерации предусматривают и поправки в Уголовный кодекс Российской Федерации. Если лица, владеющие криптовалютами средствами, сообщат в налоговые органы необходимые данные позднее 30 апреля 2021 г. или не сообщат вовсе, то наказание предусматривает штраф в размере 50 тысяч рублей. За предоставление сведений, не являющихся правомерными, предусмотрено наказание в виде штрафа в размере 10 % от большей суммы криптовалюты в кошельке в денежном эквиваленте. В результате поправок криптовалюта признается объектом налогообло-

жения. Соответственно, за неуплату налога или неполную уплату налоговой суммы предусмотрен штраф в размере 40 % от суммы неуплаченного налога. [6]

Криптовалюта, являясь имуществом, признана законным средством платежа и (или) законным модифицированным средством платежа, на противоправные действия с ней в полной мере распространяется действующее уголовное законодательство.

Таким образом, государство направляет значительные силы на то, чтобы предотвратить нелегальное использование криптовалюты в преступных целях, в том числе и в экстремистской и террористической деятельности. Предпринимаются все необходимые меры, направленные на урегулирование криптовалюты с правовой точки зрения. При этом, принимаются такие меры, чтобы искоренить анонимное использование криптовалюты и установить максимальный контроль над использованием криптовалюты и возможными транзакциями.

Библиографический список

1. Федеральный закон от 31 июля 2020 г. № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» / СПС «КонсультантПлюс». – URL: http://www.consultant.ru/document/cons_doc_LAW_358753. (дата обращения: 05.12.2020 г.).
2. Дума приняла закон «О цифровых финансовых активах». Что важно знать // Официальный сайт «РБК» [электронный ресурс] / URL: <https://www.rbc.ru/crypto/news/5f16c6379a794732b6dd31e7>. (дата обращения: 05.12.2020 г.).
3. Постановление Пленума Верховного суда Российской Федерации от 9 июля 2013 г. № 24 «О судебной практике по делам о взяточничестве и об иных коррупционных преступлениях» // Официальный сайт Верховного Суда Российской Федерации [электронный ресурс]. – URL: <https://www.vsrfr.ru/documents/own/8355>. (дата обращения: 05.12.2020 г.).
4. Федорова, А. Ю. Криптовалюта: аналог реальным деньгам или орудие мошенничества? А. Ю. Федорова, Н. И. Дорожкина // Ученые записки Тамбовского регионального отделения Вольного экономического общества России. – 2017. – Т. 18. – № 1-2. – С. 35–39.
5. Онлайн-кошелек стал тяжелее : криптовалюты получают статус имущества и более строгое регулирование // Официальный сайт «Российская газета», [Электронный ресурс]. – URL: <https://rg.ru/2020/11/26/kriptovaliuty-poluchat-status-imushchestva-i-bolee-strogoe-regulirovanie.html> (дата обращения: 06.12.2020 г.).
6. Минфин перестарался: за криптовалюту могут лишить свободы // Официальный сайт «Газета.ru», [Электронный ресурс]. – URL: <https://www.gazeta.ru/business/2020/11/12/13358401.shtml> (дата обращения: 06.12.2020 г.).

Трушина И. О.¹,

*командир отделения института подготовки
сотрудников для органов предварительного
расследования Московского университета
МВД России имени В.Я. Кикотя,
младший сержант полиции;*

Ярмонова Е. Н.²,

*старший преподаватель кафедры
административного права Московского университета
МВД России имени В.Я. Кикотя,
кандидат юридических наук, майор полиции.*

К ВОПРОСУ ОБ ОПРЕДЕЛЕНИИ ПОНЯТИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ, ИСПОЛЪЗУЕМЫХ В ПРОФИЛАКТИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ СОТРУДНИКОВ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

Информационное пространство в современном мире охватывает все сферы жизнедеятельности общества и государства. Ни одна покупка в интернет-сети не обходится без использования персональных данных граждан. Это свидетельствует об активном совершенствовании технического процесса, глобализации информационных технологий, развитии технологий электронных платежей и «бесбумажного» документооборота, появлении новой формы правонарушений с использованием персональных данных граждан. В первую очередь в таких правонарушениях опасности подвергаются персональные данные граждан. Поэтому деятельность сотрудников органов внутренних дел Российской Федерации в выявлении и профилактике таких деяний, связанных с нарушением прав граждан на защиту персональных данных, очень важна и необходима.

Для определения основных положений деятельности сотрудников полиции и роли сотрудников правоохранительных органов в сохранности персональных данных граждан Российской Федерации, нужно сформулировать понятие «персональных данных», категории персональных данных, критерии отнесения любой информации к персональным данным.

Согласно ст. 3 «Основные понятия, используемые в настоящем Федеральном законе» Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» персональные данные – это «любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)»[1]. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера» описывает персональные данные как «сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность, за исключением сведений, подлежащих распространению в СМИ»[2]. Конкретного перечня данных, которые относятся к персональным данным, в Фе-

¹ © Трушина И. О., 2020.

² © Ярмонова Е. Н., 2020.

деральном законе «О персональных данных» нет. Однако, согласно п. 2.5 приказа Роскомнадзора от 30 мая 2017 г. № 94 «Об утверждении методических рекомендаций по уведомлению уполномоченного органа о начале обработки персональных данных и о внесении изменений в ранее представленные сведения», к персональным данным можно отнести фамилию, имя, отчество гражданина, пол гражданина, дату и место его рождения, адрес постоянного и временного проживания, сведения о его семье и социальном положении, данные о его образовании и профессии, сведения о его доходах и имущественном положении, а также его биометрические личные данные (по ст. 11 Федерального закона № 152-ФЗ «О персональных данных»).

Ст. 10 указанного выше Федерального закона «О персональных данных» предусматривает специальные категории персональных данных. К ним относятся «расовая, национальная принадлежности, политические взгляды, религиозные или философские убеждения, состояние здоровья и интимной жизни».[3]

Вышеуказанные положения предусматривают частную жизнь граждан, на которую каждый гражданин имеет право согласно ст. 23 Конституции Российской Федерации от 12.12.1993 г. «Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускается»[4] и преследуется законом. Например, обеспечение права на сохранение неприкосновенности персональных данных предусматривает ст. 13.11 Кодекса об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ, которая предусматривает административную ответственность за нарушение законодательства Российской Федерации в области персональных данных. Также данным кодексом предусмотрена ст. 19.7, согласно которой состав правонарушения представляет собой непредставление или несвоевременное представление сведений, представление которых предусмотрено законом и необходимо для осуществления этим органом его законной деятельности, а равно представление таких сведений в неполном объеме или искаженном виде. В этом случае протокол об административном правонарушении составляет должностное лицо органов исполнительной власти в лице сотрудника полиции.

Определив понятие «персональных данных» можно выделить принципы, по которым происходит их обработка: законность целей и способов обработки персональных данных; соответствие целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных; соответствие объема и характера обрабатываемых персональных данных, достоверности персональных данных и их достаточности для целей обработки, а также недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных; недопустимости объединения созданных для несовместимых между собой целей без данных информационных систем персональных данных. Принципы характеризуют понятие «персональных данных» и позволяют «обеспечивать защиту прав и свобод человека и гражданина при обработке его персональных данных, в том числе и защиты прав на неприкосновенность частной жизни, личную и семейную тайну»[5].

Согласно судебной практике, некоторые суды также признавали персональными данными информацию о смерти физического лица (постановление суда

Поволжского округа от 25 сентября 2014 г. по делу № А49-005/2014), номер мобильного телефона (апелляционное определение Алтайского краевого суда от 1 октября 2013 г. по делу № 33-9241/2015), фотографии физического лица (апелляционное определение Свердловского областного суда от 9 апреля 2015 г. по делу № 33-5232/2015).

Ни в одном нормативно-правовом акте из изученных не отражен полный перечень данных, которые мы можем отнести к персональным данным. В разных случаях информация рассматривается и как персональные данные, и как просто информация. Поэтому важно определить критерии, по которым можно понять, что информация является персональными данными. В п. 1 ст. 3 Федерального закона № 152-ФЗ указано, что персональными данными является информация, по которой можно сделать вывод о принадлежности данной информации к определенному субъекту правоотношений. Но в п. 9 той же статьи, присутствует такое понятие как «обезличивание личных сведений», которое характеризуется совершенными действиями с личной информацией, после которых невозможно будет установить, к какому лицу относится эта информация.

Законодателю для точного определения, относится ли информация к персональным данным или нет, для каждого государственного органа следует уточнить понятие персональных данных, их критерии, а также указать перечень информации, которая для данных органов является персональными данными. Также следует отделить понятие персональных данных, конкретизирующую информацию, с помощью которой можно идентифицировать человека, и персональных изображений как персональных данных.

Таким образом, персональные данные – это любая информация о конкретном человеке, которая отождествлена или может быть отождествлена с ним и может указать на данного человека.

Главным требованием закона является беспрекословное соблюдение конфиденциальности при обработке любых персональных данных, позволяющее идентифицировать лицо, которому принадлежат эти данные. Федеральный закон «О персональных данных» предусматривает, что обработка персональных данных и иные фактические операции с ним (получение, хранение, создание, использование) допускается только с согласия субъекта персональных данных.

Не секрет, что правонарушения против жизни и здоровья человека, собственности, государственной власти сегодня совершаются с использованием компьютерных технологий. В связи с этим выявление и профилактика правонарушений являются ключевыми задачами для правоохранительных органов в Российской Федерации. Министерство внутренних дел Российской Федерации рекомендует гражданам проявлять бдительность и ответственность в случаях использования своих персональных данных, как в сети «Интернет», так и в других ресурсах. Во-вторых, необходимо осуществить контроль над пребыванием в сети пользователей, не готовых к отражению угроз, связанных с безопасностью их персональных данных. К таким категориям относятся дети, пожилые люди и лица, которые не имеют навыков использования персональных данных в информационном пространстве. Данным субъектом важно разъяснить, что такое персональные данные, как мошенники могут использовать их в неправомерных действиях.

Поэтому, такая деятельность со стороны социальных служб и участковых уполномоченных полиции является важной составляющей профилактической работы. Так как, для получения, например, государственной услуги необходима регистрация на официальном сайте «Госуслуг РФ», то законодательством стоит предусмотреть альтернативный способ предоставлять государственные услуги пожилым людям ввиду отнесения данной группы населения к группе риска в потере персональных данных и, следовательно, более уязвимыми для информационных мошенников. В-третьих, существует ряд формальных рекомендаций, выполняя которые можно обезопасить себя от потери персональных данных (использовать антивирусное лицензионное программное обеспечение, воздержаться от покупок в малоизвестных и подозрительных интернет-сайтах и др.).

Согласно комментариям к Федеральному закону от 27 июля 2006 г. «О персональных данных» в ст. 1 указано, что обрабатывать персональные данные могут федеральные органы государственной власти, федеральные органы субъектов Российской Федерации, а также федеральные органы власти и иные органы местного самоуправления и юридические или физические лица. В данном случае под федеральными органами власти понимаются органы власти, осуществляющие властные полномочия на федеральном уровне, к которым относятся органы внутренних дел в составе исполнительной власти.

Согласно ст. 13 Федерального закона от 7 февраля 2011 г. № 3-ФЗ «О полиции» полиция имеет право в связи с находящимися в производстве административными правонарушениями запрашивать и получать безвозмездно по мотивированному запросу уполномоченных должностных лиц полиции необходимую информацию, в том числе и персональные данные граждан, знакомиться с ними, использовать их.

Также полиция наделена правом формирования и ведения банков данных о гражданах согласно ст. 17 Федерального закона «О полиции». Правоохранительные органы в лице полиции имеют право не только собирать, обрабатывать и использовать эти персональные данные, но и на основе этих данных получать иную информацию, которая конкретно не является персональными данными, но содержит сведения о персональных данных. В связи с этим органы внутренних дел также обязаны охранять и защищать полученную новую информацию.

П. 6 ст. 6 закона «О персональных данных» говорит о необходимости обработки персональных данных в случае защиты жизни и здоровья или иных жизненно важных интересов субъекта персональных данных, если не удастся подписать согласие на обработку персональных данных. А в законе «О полиции» ст. 1 ведущим положением является назначение полиции для защиты жизни, здоровья, прав и свобод граждан. Следовательно, одной из задач деятельности полиции является защита персональных данных граждан.

Так как правоохранительные органы несут ответственность за сохранность информации, находящуюся в базе данных, а сотрудники ОВД лично несут дисциплинарную ответственность за нарушение хранения персональных данных, следует выделить два направления деятельности полиции в сфере защиты персональных данных граждан:

- контроль за сохранением персональных данных субъектов правоотношений;

– сбор персональных данных с целью организации правопорядка на территории государства.

Профилактика, в деятельности сотрудников полиции направлена на устранение правонарушений согласно ст.ст. 13.11 и 19.7 КоАП РФ. Централизованное информирование граждан о совершаемых административных правонарушениях с использованием персональных данных помогает снизить процент совершаемых преступлений в данной области путем воздействия на сознание людей. Формирование и ведение централизованных учетов, баз данных розыскной, криминалистической, оперативно-справочной, дактилоскопической, статистической и иной персональной информации, формирование архивных фондов, осуществление учета и хранения персональных данных правонарушителей помогает при производстве дел об административных правонарушениях.

Библиографический список

1. Конституция Российской Федерации (принята всенародным голосованием 12 декабря 1993 г.) (с учетом поправок, внесенных Законами Российской Федерации о поправках к Конституции Российской Федерации от 30.12.2008 г. № 6-ФКЗ, от 30.12.2008 г. № 7-ФКЗ, от 05.02.2014 г. № 2-ФКЗ, от 21.07.2014 г. № 11-ФКЗ) // СПС «Гарант-Сервис». – URL: <https://base.garant.ru/10103000>. (дата обращения 01.07.2020).

2. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» // СПС «КонсультантПлюс». – URL: http://www.consultant.ru/document/cons_doc_LAW_61801.

3. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера» // СПС «Гарант-Сервис». – URL: <http://base.garant.ru/10200083>.

Абдуразакова Л. Э.¹,

*курсант института подготовки сотрудников
для органов предварительного расследования
Московского университета МВД России имени В.Я. Кикотя,
рядовой полиции*

Гончар В. В.²,

*заместитель начальника кафедры информационной безопасности
учебно-научного комплекса информационных технологий
Московского университета МВД России имени В.Я. Кикотя,
кандидат юридических наук, полковник полиции*

СОВЕРШЕНСТВОВАНИЕ ПРОТИВОДЕЙСТВИЯ ТЕРРОРИСТИЧЕСКИМ И ЭКСТРЕМИСТСКИМ КИБЕРПРЕСТУПЛЕНИЯМ

Киберпреступность – значимая проблема как для всей мировой экономики, так и для каждой компании в отдельности. По объему потенциального ущерба, аналитики Всемирного экономического форума ставят киберпреступность на седьмое место в списке основных глобальных рисков: она опережает техногенные экологические катастрофы и распространение инфекционных заболеваний.

Противодействие терроризму и экстремизму в интернет-пространстве, сохранность персональных данных – одни из главных проблем настоящего и ближайшего будущего. В 2018 г. только от самых громких утечек пострадало более полумиллиарда учетных записей. Среди таких случаев – компрометации клиентской базы американской сети отелей Starwood, фитнес-приложения производителя спортивной одежды Under Armour, социальной сети Facebook. Современные инструменты для защиты информационных систем быстрее и надежнее обнаруживают вредоносные программы, поэтому злоумышленники все чаще пытаются обмануть не технологии, а пользователей.

Социальная инженерия стала основным методом дистанционного хищения денег у частных лиц. Только в России 80 % атак на клиентов банков совершается с её помощью: в большинстве таких случаев (79 %) жертвы сами переводят злоумышленникам деньги, поддавшись на уловки вроде фальшивых объявлений о продаже. От «телефонных минирований» наносится значительный ущерб интересам общества и государства, парализуется деятельность многих государственных органов.

Против различных компаний киберпреступники применяют усложненные механики атак. Во-первых, хакеры постоянно используют новые версии вредоносных программ, пусть даже с небольшими модификациями. У одного только опасного и очень распространенного трояна Emotet ежедневно находят от 300 новых образцов. Во-вторых, киберпреступники ищут не прямые пути в инфраструктуру организации. Для этого они прибегают к атакам на «цепочку по-

¹ © Абдуразакова Л. Э., 2020.

² © Гончар В. В., 2020.

ставок»: вместо того чтобы подбираться к хорошо защищенной жертве, они находят ее уязвимых партнеров и подрядчиков, заражают их сети, а через них – свою основную цель. Число таких атак за последние годы значительно выросло и, вероятнее всего, будет расти в нынешнем году. В-третьих, преступные группировки объединяют разработки, чтобы системы жертв заражались несколькими вирусами одновременно. Некоторые злоумышленники превратили распространение таких «пакетов» в основной источник дохода.

Одним из ключевых международных актов в области кибербезопасности за последние годы стал европейский Общий регламент по защите данных (GDPR). С мая 2018 г. все компании, работающие с персональной информацией жителей Евросоюза, обязаны соблюдать единые стандарты при сборе и обработке сведений о пользователях. Среди этих нормативов есть ужесточенные требования к прозрачности действий организаций: об утечках данных теперь следует сообщать не позднее чем через 72 часа после обнаружении инцидента. Обычно из-за рисков для репутации и стоимости акций компании замалчивают инциденты, а если и предадут их огласке, то только после полного расследования и устранении всех уязвимостей.

В результате об утечках становится известно спустя недели и даже месяцы после их обнаружения. Новый регламент вынуждает компании сразу оповещать о проблемах – иначе их ждёт штраф до 4 % от глобального оборота. К примеру, в январе 2019 г. французские власти взыскали с компании Google 50 млн. евро за несоблюдение GDPR. За первые восемь месяцев действия нового регламента профильные регуляторы в ЕС получили более 59 тыс. сообщений об утечках. Однако эта цифра не доказывает, что преступники стали чаще воровать данные.

Поток информации об утечках в прошлом году, нынешнем и, вероятнее всего, в последующие годы – следствие активности не киберпреступников, а компаний и законодателей, которые стали внимательнее относиться к проблемам кибербезопасности. В России в минувшем году также было принято несколько законов, которые показывают намерения государства задать единые стандарты для кибербезопасности в ключевых отраслях.

В начале 2018 г. в силу вступил закон «О безопасности критической информации инфраструктуры». В нем обозначено, какие госучреждения и компании должны считать свои сети критическими и как они должны себя защищать, в том числе от террористических угроз. Кроме того, документ обязывает ответственные организации отчитываться об инцидентах уполномоченному ведомству и проходить оценку безопасности.

В мае 2018 г. Банк России внес изменения в положение «О требованиях к обеспечению защиты информации». В документе регулятор прописал требования к кибербезопасности для всех финансовых организаций. В частности, банки должны будут использовать для транзакций только сертифицированное ПО, каждый год проводить анализ защищенности и информировать Центробанк об инцидентах. Второй документ особенно примечателен тем, что он нацелен на защиту организаций от атак с сугубо финансовой мотивацией. Если соблюдать новые правила, злоумышленникам будет труднее красть деньги у банков и получать их от пользователей и компаний через мошеннические транзакции.

Заметным трендом в кибербезопасности как для организаций, так и для поставщиков услуг стало привлечение внешних ресурсов. Для адекватной защиты и реагирования на угрозы компаниям нужны квалифицированные специалисты и значительные денежные вложения. Специалистам, в свою очередь, важно постоянно наблюдать за новым ВПО и векторами атак, а это невозможно без стабильного потока инцидентов.

Требования к комплаенсу также стимулируют потребность бизнеса во внешних экспертах. Новые законодательные инициативы демонстрируют, что государства усиливают надзор за соблюдением норм кибербезопасности. Это означает, что организации будут нуждаться в специалистах по отраслевым стандартам. Наконец, экспертов по кибербезопасности приглашают, чтобы помочь сотрудникам повысить компьютерную грамотность. За последние года обучающие курсы и эмуляция атак стали полноценной услугой у многих вендоров.

Самим фирмам, специализирующимся на кибербезопасности, тоже требуется помощь в реагировании на угрозы. Злоумышленники очень быстро развивают свои методы и инструменты. Как утверждает разработчик антивирусов G DATA Software, новый файл с вредоносным кодом появляется в сети каждые четыре секунды. Чтобы успевать обрабатывать огромные массивы данных, экспертам необходимо частично автоматизировать анализ ВПО. Для этого они привлекают искусственный интеллект и строят платформы для обмена информацией о киберугрозах.

За последние полтора года мы увидели, что правительства и частные компании стали ответственнее подходить к вопросам кибербезопасности. Власти по всему миру начинают строже контролировать то, как организации защищают свои инфраструктуры. Это отражено и в GDPR, и в российских документах вроде закона о критической инфраструктуре и требований ЦБ РФ к защите информации. Бизнес, в свою очередь, показывает самостоятельное развитие цифровой культуры. Все больше компаний понимают необходимость защиты от хакеров и привлекают для этого внешних экспертов. Кроме того, организации учат сотрудников, не разбирающихся в кибербезопасности, базовым правилам компьютерной гигиены.

Киберпреступники все больше полагаются на социальную инженерию, поэтому в ближайшие годы киберграмотность сотрудников многих организаций подвергнется многократным проверкам. Кроме того, злоумышленники начали объединять усилия, поэтому государству и бизнесу предстоит сотрудничать еще теснее для обеспечения безопасности своих инфраструктур и персональных данных пользователей, в том числе для успешного противодействия современному терроризму и экстремизму. Все более актуальным становится вопрос совершенствования государственно-частного партнерства в данной сфере.

Библиографический список

1. Bissell, K. Ninth Annual Coast of Cybercrime Study / K. Bissell, R.M. Lassale, P. Dal Cin // Accenture. – URL: <https://www.accenture.com/us-en/insights/security/cost-cybercrime-study>.

2. The Global Risks Report 2019 // World Economic Forum. – URL: http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf
3. The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC // CNIL. – URL: <https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc>
4. Международное исследование EY в области информационной безопасности 2018-2019 // Earnest and Young Global Ltd. – URL: https://www.ey.com/ru_ru/giss
5. Malware trends 2017// G DATE Software. – URL: <https://www.gdatasoftware.com/blog/2017/04/29666-malware-trends-2017>.
6. Marriott Announces Starwood Guest Reservation Database Security Incident// Marriott International. – URL: <https://news.marriott.com/news/2018/11/30/marriott-announces-starwood-guest-reservation-database-security-incident>.
7. Under Armour Notifies MyFitnessPal Users of Data Security Issue// Under Armour, Inc. – URL: <https://about.underarmour.com/investor-relations/news-events-presentations/corporate-news/id/12866>.
8. Security Update//Facebook Newsroom // Facebook.com. – URL: <https://about.fb.com/news/2018/09/security-update/>

Ахмедов Д. Р.¹,

*курсант института подготовки сотрудников
для органов предварительного расследования
Московского университета МВД России
имени В.Я. Кикотя, рядовой полиции*

Гончар В. В.²,

*заместитель начальника кафедры информационной безопасности
учебно-научного комплекса информационных технологий
Московского университета МВД России имени В.Я. Кикотя,
кандидат юридических наук, полковник полиции*

ОСОБЕННОСТИ ПРАВОВОГО ВОЗДЕЙСТВИЯ НА ТЕРРОРИСТИЧЕСКИЕ ПРОЯВЛЕНИЯ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

В настоящее время тема развития информационно-телекоммуникационных сетей, в частности расследования и раскрытия преступлений в этой среде наиболее актуальна, поскольку в наше время каждый человек хотя бы раз пользовался сетью «Интернет», как следствие и информационно-телекоммуникационными сетями. Интернет в наши дни считается важнейшей и неотъемлемой частью жизни общества и в этой связи преступность также не стоит на месте, она прогрессирует наравне с развитием информационных сетей[2].

В современном глобальном сообществе, когда открыты границы, в свободном доступе информация, в обществе стали видоизменяться и виды преступления, средства их совершения. Раскрытие и расследование наиболее опасных и резонансных преступлений становится все сложнее, так как организаторы данного преступления могут находиться вне пределов территориальной юрисдикции национальных границ того государства, где совершается то или иное преступление. К данным видам преступлений относится терроризм.

В настоящее время во всем глобальном сообществе происходит активная цифровизация всех сфер общественной жизнедеятельности, что неминуемо привело к тому, что деструктивные формы социальной жизни, а именно преступления, также начали осваивать новую сферу развиваемых отношений. Как следствие, в последнее время мы все чаще видим и слышим о различных видах преступлений, совершаемых в виртуальной среде, но затрагиваемых наш мир в материальных и духовных отношениях.

Прогрессивное развитие виртуальной социальной индустрии привело к тому, что и радикально настроенная часть населения также стала использовать данные технологии в своих преступных целях. Средствами распространения террористических проявлений, деструктивно развивающих общественные отношения, стали такие социальные сети как «Вконтакте»; «Инстаграмм»; «Фейсбук», «Телеграмм».

¹ © Ахмедов Д. Р., 2020.

² © Гончар В. В., 2020.

К сожалению, на первых порах развития преступных форм активности не оказались регламентированы отечественным законодательством. В результате чего законодатель, проанализировав сложившуюся негативную ситуацию, принял ряд мер экстренного юридического характера. Были разработаны текущие локальные акты, законы, в том числе доктрины и стратегии, которые установили юридические барьеры для расширения и развития виртуальных преступных сообществ. После чего в дело вступила судебная практика, наглядно реагирующая на текущие отрицательные свойства общественной жизнедеятельности и ее проявление в виртуальном пространстве.

В настоящее время судебная практика Российской Федерации уже имеет достаточный опыт привлечения к уголовной ответственности лиц, совершивших преступные деяния террористической направленности против основ конституционного строя и безопасности национального государства в глобальной виртуальной сети «Интернет».

Также необходимо отметить, что за рассматриваемые противоправные социально негативные проявления деструктивного характера, которые совершаются группой лиц, в той или иной степени ограничиваются и нарушаются законные права и свободы человека и гражданина, либо создаются угрозы причинения подобного вреда[3]. Поэтому за подобного рода преступления должна наступить уголовная ответственность, и лицо, совершившее данное уголовное преступление должно претерпевать определенные неблагоприятные последствия личностного характера для него.

Статьи УК РФ также определяют наказание за подобную противоправную деятельность. В диспозиции ст.ст. 205–205.5 УК РФ[1] содержатся нормы права, предусматривающие уголовную ответственность за преступления против общественной безопасности и общественного порядка.

Так или иначе, террористическая деятельность наносит разрушительный социально-экономический ущерб и препятствует развитию общественно-политических отношений созидательного характера, не только для Российской Федерации, но и, в глобальном масштабе, для всех членов мирового сообщества. Так как те угрозы и последствия, которые проявляются после деятельности деструктивного характера террористическими сообществами, в своей юридической сути, носят разрушительный характер и в социально-идеологической среде, препятствуя мирозозидательным взаимоотношениям в человеческом социуме, развивая отношения правового нигилизма между членами сообщества.

Необходимо отметить, что преступления террористической направленности носят достаточно серьезный характер общественной опасности для каждого гражданина любого государства, общества, как в целом, так и в частности[4]. Подобные противоправные деяния обычно совершаются в местах массового скопления людей и материальных ресурсов[5]. Тем самым, по сути, преступники стремятся причинить максимальный ущерб и создать общественный резонанс своим преступным поступком, запугать, создать негативный отрицательный фон к правоохранительной системе государства, которое якобы не в силах противостоять и предупреждать совершение данных противоправных проявлений.

Однако, нельзя также забывать, что терроризм активно интегрировался и в политическую среду, приобретя криминально-политические качества с целью дестабилизации общественно-политической обстановки не только в пределах национальных границ государства, но и региона, а может быть, и мира в целом. Голливудские красочные сюжетные художественные фильмы наглядно демонстрируют возможность разноуровневого проявления данного вида социально негативного проявления. К сожалению, также необходимо констатировать, что террористы тоже усилили свою противоправную деятельность. Причем формы их проявления, также как и сферы реализации преступных намерений в общественной среде, различны. Сегодня мы можем наблюдать отдельные формы проявления терроризма в политике, религии, экономике, идеологии, культуре. На это, в частности, подробно указывает ныне существующая общественно-политическая и социально-экономическая ситуация на Ближнем Востоке, где, к сожалению, отдельные государства мира спонсируют данное направление финансовыми активами, материальными ресурсами и вооружением, в обмен на будущую политическую лояльность в лице нового руководства государства, либо в получении открытого доступа к культурным и природным богатствам страны, ее расхищению.

Подводя итог вышесказанному, хочу отметить, что преступления террористической направленности являются на сегодняшний день общемировой проблемой. В этой связи, в качестве уголовно-правовой прерогативы, необходимо и в дальнейшем разрабатывать более эффективные методы и средства юридического свойства, которые будут регламентировать общественные отношения в сфере противодействия террористическим проявлениям. Важно также иметь в виду то, что своевременное предупреждение и пресечение подобных преступных посягательств на стадиях их разработки и подготовки имеют наиболее серьезное значение, ведь так или иначе террористическая деятельность создает прямую угрозу конституционному строю, а также национальному суверенитету государства и личной безопасности граждан. Необходимо принимать совместные соглашения, конвенции, иные акты, основной целью и задачей которых будет являться обеспечение защиты основных прав и свобод граждан, безопасность государств от террористических посягательств.

Именно совместная работа государств над этим вопросом поможет осуществить должную защиту от подобных противоправных деяний и на должном уровне поддерживать безопасность стран от преступных действий террористического характера. Поэтому необходимо учитывать все эти положения. Руководствуясь данными критериями, государство и общество сможет обеспечить необходимую защиту и безопасность от преступных посягательств террористической направленности.

Библиографический список

1. Уголовный кодекс Российской Федерации от 13.06.1996 г. № 63-ФЗ (ред. от 31.07.2020 г.) // Собр. законодательства Рос. Федерации. – 17.06.1996 г. – № 25, ст. 2954.

2. Цыганкова, Я. В. К вопросу о противодействии пропаганде религиозных преступлений в сфере информационно-телекоммуникационных сетей / Я. В. Цыганкова, А. А. Дорошин, Д. Р. Ахмедов // *Colloquium-journal*. – 2019. – № 18-7 (42). – С. 60–62.

3. Иванова, Ю. А., Экстремизм и терроризм в окружающей среде: проблема юридической регламентации / Ю. А. Иванова, Д. Р. Ахмедов, К. И. Озеров // *Вестник экономической безопасности*. – № 2. – С. 62–65.

4. Ахмедов, Р. М. Взаимодействие министерства внутренних дел российской федерации с религиозными объединениями в сфере противодействия религиозному терроризму и экстремизму. // *Российская полиция: три века служения отечеству. Материалы юбилейной международной научной конференции, посвященной 300-летию российской полиции* / под ред. Н. С. Нижник. – СПб.: Санкт-Петербургский университет МВД России, 2018. – С. 1380–1383.

5. Гончар, В. В. Отдельные направления совершенствования расследования киберпреступлений // *Противодействие терроризму и экстремизму в информационных сетях : сборник материалов Всероссийской научно-практической конференции*. – М. : Московский университет МВД России имени В.Я. Кикотя, 2019. С. 13–16.

Баргаринов А. Р.¹,

адъюнкт факультета подготовки

научно-педагогических и научных кадров

Московского университета МВД России имени В.Я. Кикотя

Тишутина И. В.²,

профессор кафедры криминалистики

Московского университета МВД России имени В.Я. Кикотя,

доктор юридических наук, доцент

О НЕКОТОРЫХ ВОПРОСАХ ОРГАНИЗАЦИИ РАССЛЕДОВАНИЯ ТРАНСНАЦИОНАЛЬНЫХ ПРЕСТУПЛЕНИЙ ЭКСТРЕМИСТСКОГО ХАРАКТЕРА В РЕСПУБЛИКЕ КАЗАХСТАН

Эффективность организации раскрытия и расследования экстремизма и его наиболее опасной формы проявления – терроризма – в информационных системах во многом предопределяется своевременным поступлением оперативной информации о соответствующих фактах и грамотными действиями оперативных работников по ее закреплению.

Современные информационные технологии, которые прочно вошли в повседневную жизнь, довольно активно используются преступной средой в разных направлениях противоправной деятельности, и транснациональный экстремизм в этом отношении не исключение. Постоянная модернизация таких технологий усложняет работу правоохранительных органов по выявлению, раскрытию и расследованию преступлений, совершаемых с их использованием.

Глобальные перемены в общественной и государственной жизни всегда неминуемо влекут и изменения в преступной среде. Практически все преступные посягательства так или иначе связаны с использованием возможностей современных компьютерных технологий и глобальных информационных сетей, предоставляющих возможности удаленного доступа и общения в отсутствие непосредственного контакта.[1] Сегодня совершенно очевидно, что повышение эффективности деятельности правоохранительных органов на данном направлении напрямую зависит от освоения ими возможностей цифровизации и их грамотного применения для целей предупреждения, выявления и расследования преступлений.[2].

В настоящее время большая часть преступлений экстремистской направленности, прописанных в Уголовном кодексе Республики Казахстан, совершается с использованием сети «Интернет» и предоставляемых ею возможностей: ст. 174 «Возбуждение социальной, национальной, родовой, расовой, сословной или религиозной розни»; ст. 179 «Пропаганда или публичные призывы к захвату или удержанию власти, а равно захват или удержание власти либо насильственное изменение конституционного строя Республики Казахстан»; ст. 182 «Создание, руководство экстремистской группой или участие в ее деятельности»; ст. 256

¹ © Баргаринов А. Р., 2020.

² © Тишутина И. В., 2020.

«Пропаганда терроризма или публичные призывы к совершению акта терроризма»; ст. 257 «Создание, руководство террористической группой и участие в ее деятельности»; ст. 258 «Финансирование террористической или экстремистской деятельности и иное пособничество терроризму либо экстремизму»; ст. 259 «Вербовка или подготовка либо вооружение лиц в целях организации террористической либо экстремистской деятельности»; ст. 404 «Создание, руководство и участие в деятельности незаконных общественных и других объединений»; ст. 405 «Организация и участие в деятельности общественного или религиозного объединения либо иной организации после решения суда о запрете их деятельности или ликвидации в связи с осуществлением ими экстремизма или терроризма».

Анализ практики показывает, что экстремистские и террористические организации используют в своих целях как открытые, так и защищенные веб-сайты и чат-группы ограниченного доступа в Интернете. Так, весной 2017 г. в г. Павлодаре Ф., 1988 г.р., являясь приверженцем нетрадиционного для Казахстана религиозного течения салафизм, в целях возбуждения религиозной вражды и розни, умышленно предоставил Б. информацию о том, как стать подписчиком в Интернете бот-канала «Новости Исламского государства», распространяющего материалы экстремистского характера. Б., став подписчиком бот-канала, получил материал под названием «Пути к победе», который, согласно заключению эксперта от 9 июня 2017 г. № 1087, содержит признаки возбуждения религиозной вражды и розни.

Таким образом, осуществляется пропаганда экстремизма и призывы к совершению террористических актов, вербовка новых членов в состав запрещенных организаций и т. п. Практически неограниченный доступ граждан к сети «Интернет» позволяет таким организациям и их сторонникам рассматривать всю аудиторию как потенциальных клиентов. Форумы, группы, чат-боты ограниченного доступа становятся для завербованных местом общения, «просвещения», обучения, получения заданий и отчета о «проделанной работе». В целях ограждения пользователей сети «Интернет», социальных сетей от влияния пропаганды экстремизма и терроризма осуществляется постоянный мониторинг информационного пространства. По данным Комитета национальной безопасности (КНБ) РК, в 2018 г. было заблокировано более 620 тыс. материалов, содержащих пропаганду терроризма и экстремизма. Ежегодно в Казахстане блокируется 400–600 сайтов за пропаганду идей радикализма и терроризма.[3]

Так, житель г. Щучинска, 28-летний М., на своей странице в социальной сети «ВКонтакте» опубликовал аудиофайлы, запрещенные к распространению в Казахстане, а также направлял их в личных сообщениях другим пользователям соцсети.[4] Б. на своей странице в социальной сети «Instagram», а также в личной переписке мессенджера «WhatsApp» разместил публикации, комментарии и сообщения, содержащие признаки возбуждения религиозной вражды и розни.

Нередко граждане РК, являясь членами запрещенных экстремистских и террористических организаций и находясь в их составе за рубежом, осуществляют вербовку своих сограждан посредством мессенджеров. Так, в период с июня по ноябрь 2015 г. М., находясь на территории Сирийской арабской республики

(САР), используя различные зарубежные и казахстанские абонентские номера, на систематической основе осуществляла переписки в мессенджерах «Whatsapp» и «Telegram» под аккаунтами «С...У...» с жителями Жезказганского региона с целью склонения абонентов Р., Ш. и др. к радикальной религиозной идеологии. Она отправляла фотографии с огнестрельным оружием в руках, аудиосообщения, восхваляя жизнь в САР и призывая присоединиться к ней.

В ходе проведения оперативно-разыскных мероприятий установлено, что гражданин РК А., 1989 г. р., оказывает помощь гражданину РК Ж., 1971 г. р. (находится в международном розыске за совершение деяний предусмотренных ч. 2 ст. 257 УК РК «Создание, руководство террористической группой и участие в ее деятельности»), путем создания аккаунтов в социальных сетях и интернет-мессенджерах, а также приобретения сим-карт для организации безопасных каналов связи между Ж. и его пособниками в РК.

Возможность удаленного доступа позволяет членам запрещенных организаций, реализовывать преступные планы, находясь за пределами государства. Так, 25 августа 2016 г., в ходе проведения оперативно-разыскных мероприятий, была установлена интернет-страница в социальной сети «ВКонтакте» под логином «Abu-Ibrohim Sadykov-Kazakhstani», где в общем доступе размещены видеоролики, содержащие боевые действия на территории Сирии и Ирака с призывами присоединиться к международной террористической организации «ДАИШ» (далее МТО «ДАИШ»)[5]. Страница принадлежит жителю Карагандинской области С., который находится на территории Сирии, где участвует в деятельности данной организации.

Практика выявления и расследования преступлений экстремистской направленности, совершаемых с помощью информационно-телекоммуникационных систем, актуализирует проблему получения криминалистически значимой информации. Она характеризуется объективными сложностями установления пользователей соответствующего оборудования, особенно с учетом повсеместного открытого доступа к средствам сокрытия идентификационной информации пользователей сети «Интернет» и преобладания серверов и ресурсов, находящихся за пределами действия законодательства Республики Казахстан. Так, в ходе ОРМ получена информация, что гражданин РК К., 1993 г. р., посредством мессенджера «Telegram» контактирует с неустановленным боевиком МТО «ДАИШ»[5]. К. при координации указанного лица осуществляет пособническую деятельность в интересах указанной МТО. Целью указанного боевика является осуществление террористических актов на территории г. Алматы.

Результаты проведенного нами исследования показали, что при подготовке и осуществлении пропаганды и публичной демонстрации нацистской или сходной с ней атрибутики или символики; публичных призывов к осуществлению указанной деятельности или совершению указанных действий, которые в 84 % случаев осуществляются с использованием сети «Интернет», преступники, как правило, проводят мониторинг социальной сети, в которой предполагается размещение соответствующей информации, создание сначала открытых групп, затем при необходимости, переадресация на закрытые; пользователи постепенно с помощью соответствующих психологических приемов воздействия, техноло-

гии нейролингвистического программирования (НЛП) втягиваются в общение, происходит их «дрессировка», манипуляция посредством обесценивания традиционных ценностей и формирования искаженных ориентиров, у них создается ощущение неблагополучия и опасности объективной реальности и это служит базой для последующей реализации непосредственно действий по совершению преступления – призывам к насилию, как на уровне пропаганды, так и с выходом в реальную жизнь и активными действиями по дестабилизации социальной и политической обстановки.

Многие деструктивные движения создаются заблаговременно с расчетом на отсроченный результат. Согласно исследованиям, проведенным в Российской Федерации, самый большой прирост такого рода групп в информационном пространстве в последние годы отмечается именно ультрарадикальных, экстремистских и политизированных деструктивных движений (анархизм, радикальная оппозиция).[6] Похожая ситуация прослеживается и в Республике Казахстан.

Для преодоления таких ситуаций и своевременного мониторинга информационного пространства важны системы искусственного интеллекта, осуществляющие автоматизированный поиск и анализ контента в сети «Интернет», а также латентно-семантический анализ. Технологии искусственного интеллекта, предполагающие в том числе и создание качественной системы сбора, хранения, обработки и анализа больших данных позволяют решать самые сложные задачи. В условиях повсеместной цифровизации деятельность правоохранительных органов невозможна без их использования и практика демонстрирует острую необходимость совершенствования технических возможностей их эффективной обработки для повышения потенциальной полезности этих массивов информации.

Большое внимание было уделено стартап-проектам Казахстана по автоматизации и цифровизации процессов в правоохранительной сфере на форуме «Digital Almaty: цифровое будущее глобальной экономики», прошедшем 31 января 2020 г. в г. Алматы с участием премьер-министров стран ЕАЭС.[7] Форум был посвящен обсуждению путей построения устойчивого развития региона на основе больших данных (Big Data) и искусственного интеллекта. В плане возможностей использования по рассматриваемому в статье направлению следует отметить один из представленных проектов – компании Kazdream Technologies, специализирующейся на разработке решений на основе больших данных и искусственного интеллекта. Компания интегрирует данные сотовых операторов, социальных сетей, государственных баз данных без привязки к персональным данным и составляет аналитику, которую используют в своей работе государственные органы.[8]

Обобщение практики применения возможностей искусственного интеллекта в правоохранительной деятельности различных стран в целях раскрытия и расследования преступлений позволяет выделить ее основные направления:

- использование возможностей компьютерного зрения (Computer Vision) для распознавания и сравнения визуальных образов на фото- и видеоматериалах;
- отслеживание перемещений в режиме онлайн;
- создание фотороботов разыскиваемых лиц;
- диагностика противоречий в показаниях допрашиваемых лиц;

- мониторинг интернет-трафика и выявление подозреваемых и их связей по заданным параметрам в сети Интернет;
- перспективная аналитика – прогнозирование возможных сценариев развития преступной цепочки;
- анализ и обработка больших массивов информации с целью выборки по заданным параметрам;
- распознавание текста и автоматизация процесса документооборота.[9]

Представляется перспективным использование возможностей искусственного интеллекта при выявлении и расследовании преступлений экстремистской направленности, связанных с использованием телекоммуникационных сетей, для их мониторинга и диагностики на предмет выявления как скрытых, зашифрованных, так и открыто размещаемых данных, содержащих признаки или призывы к осуществлению экстремистских действий либо обосновывающие или оправдывающие необходимость их совершения.

Библиографический список

1. Давыдов, В. О. Цифровые следы в расследовании преступлений, совершенных с использованием информационно-телекоммуникационных технологий / В. О. Давыдов, И. В. Тишутина // Материалы международной научно-практической конференции «Современное уголовно-процессуальное право – уроки истории и проблемы дальнейшего реформирования» (15–16 октября 2020 г.) – № 1(2). – Орел: Орловский юридический институт МВД России, 2020. – С. 181.
2. Тишутина, И. В. Использование возможностей искусственного интеллекта в деятельности следователя / И. В. Тишутина // Создание и развитие модели органов предварительного расследования в Российской империи : материалы Всероссийской научно-практической конференции (Москва, 24 сентября 2020 г.) / под общ. ред. Д. Н. Кожухарика. – М. : Московская академия следственного комитета Российской Федерации, 2020. – С. 109.
3. Гусарова, А. Особенности противодействия насильственному экстремизму и терроризму в Казахстане [электронный ресурс] // Центральное бюро аналитической журналистики CABAR.ASIA. – URL: <https://cabar.asia/ru/osobennosti-protivodejstviya-nasilstvennomu-ekstremizmu-i-terrorizmu-v-kazahstane>. (дата обращения: 30.10.2020).
4. Муканов, Б. Жителя Щучинска осудили на 7,6 лет лишения свободы за рассылку аудиофайлов [электронный ресурс] // ТОО «Инфополис». – URL: <https://informburo.kz/novosti/zhitelya-shchuchinska-osudili-na-76-let-lisheniya-svobody-za-rassylku-audiofaylov.html>.
5. Список религиозной литературы и материалов, признанных экстремистскими на территории Республики Казахстан [электронный ресурс] // Управление по делам религий Актюбинской области. – URL: <https://www.gov.kz/memleket/entities/aktobe-din/documents/details/93468?lang=ru>.
6. Выступление Н. Касперской на Международной научно-практической конференции «искусственный интеллект (большие данные) на службе полиции». – М.: Академия управления МВД России, 2019 // <https://a.mvd.pf/Press-sluzhba/Novosti/item/18999231>.

7. В Казахстане планируют создать национальный кластер искусственного интеллекта [электронный ресурс]. // Strategy2050 : обзорно-аналитический портал. – URL: <https://strategy2050.kz/ru/news/v-kazakhstane-planiruyut-sozdat-natsionalnyy-klaster-iskusstvennogo-intellekta>.

8. Тишутина И.В. Использование возможностей искусственного интеллекта в деятельности следователя // Создание и развитие модели органов предварительного расследования в Российской империи : материалы Всероссийской научно-практической конференции (Москва, 24 сентября 2020 г.) / под общ. ред. Д. Н. Кожухарика. – М. : Московская академия Следственного комитета Российской Федерации, 2020. – С. 109–115.

Алдушина К. В.¹,
*курсант института психологии служебной
деятельности органов внутренних дел
Московского университета МВД России
имени В.Я. Кикотя, рядовой полиции*

Прудникова Т. А.²,
*профессор кафедры административного права
Московского университета МВД России
имени В.Я. Кикотя, доктор юридических наук,
подполковник полиции*

БОРЬБА С ЭКСТРЕМИЗМОМ И ТЕРРОРИЗМОМ В РОССИЙСКОЙ ФЕДЕРАЦИИ И ПУТИ ЕЕ СОВЕРШЕНСТВОВАНИЯ

Общественная безопасность и охрана общественного порядка являются основополагающими задачами для государственной власти. Исполнительная власть нацелена на профилактику и непосредственное противодействие деяниям, ставящим под угрозу особо охраняемую ценность – человеческую жизнь. Особую опасность представляют собой такие негативные явления как экстремизм и терроризм.

Экстремизм и терроризм представляет угрозу национальным интересам и национальной безопасности любого государства. В связи с этим устранение террористической угрозы и пресечение распространения экстремизма рассматривается как одно из приоритетных направлений обеспечения безопасности в политике Российской Федерации.

Терроризм – это крайняя форма экстремизма, которая реализуется через совершение террористических актов неправительственными организациями для изменения основ конституционного строя путем совершения поджогов, захвата заложников и т. п. Полное определение как экстремизма, так и терроризма дано в законе «О противодействии терроризму» и законе «О противодействии экстремизму», там же прописаны основные мероприятия и направления совершенствования профилактики и борьбы с терроризмом и экстремизмом, основные направления описаны и в «Стратегии национальной безопасности».

Борьбой с терроризмом и экстремизмом занимается большинство государственных органов исполнительной власти, в том числе МВД России, ФСБ России, Росгвардия, но их полномочия разграничены ст. 151 УПК РФ «Подследственность». Большинство дел, связанных с терроризмом или экстремизмом, относятся либо к общей подследственности, либо к подследственности федеральных органов безопасности. Главным подразделением ФСБ России, которое занимается противодействием терроризму и экстремизму занимается вторая служба ФСБ России управления по борьбе с терроризмом и защитой Конституционного строя.[2]

¹ © Алдушина К. В., 2020.

² © Прудникова Т. А., 2020.

Терроризм достаточно давнее явление. Появление первых террористических организаций прослеживается с 19 века, когда было сформировано тайное революционное общество «Земля и воля», одним из подразделений которого была организация «Черный передел» и можно сказать, что уже тогда они совершали террористические акты покушаясь на жизнь Александра Второго.

Основными мотивами терроризма для лиц, которые причастны к террористической деятельности, являются меркантильные основы, идеологическая возможность самореализации, сотоварищество. Наибольшую опасность национальной безопасности Российской Федерации, ее культуре, социально-политическому устройству несут организации, принадлежащие к направлениям исламского радикального фундаментализма (устанавливающим свое влияние не только в традиционно мусульманских регионах, но и на всей территории страны) и новым религиозным движениям деструктивного характера. Религиозный фактор зачастую используется в качестве идеологической и организационной основ при реализации практических интересов политических субъектов. Агрессивными и общественно опасными представляются так называемые «эмиссары» – те, кто проповедует неверные, радикальные формы ислама. Впервые данная организация была замечена в Чечне. Ее структура выглядела так: самой низшей были боевые полевые группы, численностью от 50 до 100 человек, во главе каждой боевой группы стоял амир, выше полевого амира стоял главный амир, который поддерживался духовным наставником. Вся эта организация делилась на боевые и резервные группы. Боевые группы составляли примерно 500 человек и от нее уже развивались ответвления: отряды, амиры. Резерв составляли те, кто вступил или собирается вступить в незаконно вооруженные формирования, они проходили стабильную подготовку, обеспечивая тем самым постоянную смену кадров.

Террористической деятельностью занимаются люди, которые либо имеют социально адаптивный тип личности, либо дезадаптивный. Социально адаптивный тип составляют люди, именуемые вышеупомянутым термином «амиры», это командиры отрядов, которые устойчивы и способны повести массы за собой, а дезадаптивный – легко внушаемые, доверчивые и доступные к вербовке. Основными целями они ставят перед собой создание халифатов. Халифат – это форма государственного устройства, при котором все нормативно-правовые споры решались посредством Шариата. Шариат – это свод духовных правил, который прописан в Коране, трактате или записках Мухаммеда. В соответствии с этим шариатом, различные течения ислама, такие как сунниты, шииты, алавиты, трактуют свод правил по-разному.

Террористов принято называть приверженцами крайней религиозной или экстремистской формы. В профессиональной среде не принято употреблять термин «террорист», принято их называть «лица причастные к террористической деятельности».

Чеченский политический деятель, лидер движения 1990-х годов, бывший советский генерал, боевой летчик Джохар Дудаев, захватил власть в Чечне, и объединил все бандитские группировки, главной целью которых была борьба с органами государственной исполнительной власти. Джохар Дудаев представлял большую угрозу, было множество попыток прервать его деятельность. Ликвиди-

ровать Дудаева удалось посредством телефонного звонка. По спутниковому телефону был выявлен охват его местоположения, далее было принято решение запустить взрывные устройства, несмотря на опасность задеть взрывом других лиц. По прошествии некоторого времени в Чеченской республике появился Аслан Масхадов, который сосредоточил власть в своих руках. Но Аслан Масхадов был слаб и не настойчив и власть в период его правления перешла к группировкам, отрядам (Северный отряд, Восточный отряд).

К 2005 г. их структура стала меняться, они стали действовать малыми группами, уже не было больших кочующих 500 человек, их численность упала до 10–15 человек и лишь изредка возрастала ввиду объединения для совершения крупных актов. Претерпели изменения и их принципы, они стали более мобильными, их действия происходили с опорой на население с целью ослабления федеральных сил. Они вели террористическую деятельность путем партизанской войны (захват заложников за пределами конфликтов). В 2006 г. Аслана Масхадова, последнего представителя этой группировки, ликвидировали.

Терроризм очень противоречив и нетерпим. Представители международных террористических организаций (МТО) междоусобно ведут военные действия. К примеру, группировка «Талибан», которая действует на территории Северного Афганистана вот уже более 20 лет, остатки «Игил» ведут открытые боевые столкновения, «Алькаида», которая из своего круга ликвидировала структурные подразделения «Игил». Международные группировки находятся за пределами Российской Федерации, благодаря зачисткам специальных служб.

Переход терроризма от незаконно вооруженных формирований к терроризму в информационном пространстве произошел в 2010 г., их основу составляла пропагандистская деятельность, или информационный террор. На данный момент современному терроризму тяжело противостоять. Расформированы бандитские группы и всю опасность представляют собой завербованные «спящие ячейки», которые направлены на одиночный джихад, т. е. действия по одному-два человека, без контроля «эмира».[1]

В современном мире большую опасность представляет собой Интернет, а конкретнее Darknet, «Темная сеть». В пространстве «Темной сети» существуют сайты, на которых после авторизации человек проходит комплекс подготовки боевика: как собрать СВУ, как скрываться от слежки и т. п.

Существуют гласные и негласные способы противодействия терроризму. Гласные методы включают в себя, во-первых, профилактическую работу в мечетях с представителями восточных народов, которые проповедуют ислам. Необходимо проводить профилактическую работу, заключающуюся в правильном толковании ислама. Это делается с целью исключения принятия призывов народных течений. Во-вторых, обеспечение информационной безопасности, т. е. недопущение в открытый доступ, Интернет информации о негативном исламе. В-третьих, это проведение боевых мероприятий и освещение в СМИ, чтобы граждане понимали серьезность и жесткость методов борьбы с террористами, а также для предупреждения вступления в террористические группировки. В-четвертых, освещение уголовных дел, для того чтобы остановить популяризацию терроризма.

Борьба с экстремизмом и терроризмом – залог здорового развития общества и государства в целом.

Библиографический список

1. Власов, В. И. Экстремизм, терроризм, сепаратизм: политико-правовое осмысление в условиях глобализации. – М.: РАГС, 2009. – 43 с.
2. Бутков, П. П. Терроризм и проблема безопасности в современном мире / П. П. Бутков, А. И. Зайцев. – СПб.: Издательство Политехнического университета, 2015. – 336 с.

Дуваа А. А.¹,

*слушатель факультета подготовки специалистов
в области информационной безопасности 962 учебной группы
Московского университета МВД России имени В.Я. Кикотя,
младший лейтенант полиции;*

Овчинский А. С.²,

*профессор кафедры информационной безопасности
учебно-научного комплекса информационных технологий,
доктор технических наук*

ИСПОЛЬЗОВАНИЕ БОЛЬШИХ ДАННЫХ В ВЫЯВЛЕНИИ ТЕРРОРИСТИЧЕСКИХ УГРОЗ

Использование больших данных можно считать как достижением человечества, так и его проблемой. В последние годы террористические акты бросили вызов глобальной безопасности. Однако новые технологии искусственного интеллекта, внедряемые государствами, вносят свой вклад в борьбу с терроризмом, в том числе быстрое развитие технологий машинного обучения позволяет применять массовое наблюдение в более крупных масштабах и анализировать большие объемы данных.

В наши дни правительства многих стран по всему миру расширили использование автоматизированной разведки для сбора и оценки данных в целях обеспечения национальной безопасности. Программа PRISM, осуществляемая Агентством национальной безопасности США (АНБ), стала одним из самых известных примеров крупномасштабных операций по прослушиванию телефонных разговоров после утечки информации в 2013 г. Тем не менее, существует множество других программ, которые используются правительствами других стран, в том числе Великобритании, Германии, Швеции, Франции и Нидерландов. Их цель – обнаруживать подозрительное поведение людей в большой группе граждан[1].

Раскрытие информации, совершенное Эдвардом Сноуденом, показало, что АНБ прослушивало переговоры миллионов американских граждан и собрало обширные архивы записей телефонных разговоров и данных электронной почты. Этот метод наблюдения, который включал в себя прослушивание телефонных разговоров или слежку в социальных сетях граждан, возмутил многих американцев, которые считали его нарушением конфиденциальности своей личной жизни. Однако использование данной тактики слежки и прослушивания было обосновано и оправдано тем, что сбор данных ограничивался метаданными (т. е. данными о данных), а не фактическими данными (содержанием разговоров и писем), тем самым вмешательство в личную жизнь граждан было минимальным.

Быстрое совершенствование информационных и коммуникационных технологий облегчает сбор и анализ увеличивающихся объемов данных за более ко-

¹ © Дуваа А.А., 2020

² © Овчинский А.С., 2020

роткие периоды времени, что делает слежку в Интернете работоспособной и привлекательной альтернативой целенаправленному перехвату информации. В последние годы улучшение вычислительной мощности привело к повышению производительности алгоритмов машинного обучения.

С использованием больших наборов данных машинное обучение может распознавать объекты на изображениях, например, обнаруживать рак груди[2]; слушать речевые команды и отвечать на них, как это делают Siri от Apple или Google Assistant; и победить чемпиона мира в игре Go (Google AlphaGo)[3]. Повышение производительности алгоритмов машинного обучения для решения сложных проблем изменило баланс проблемы конфиденциальности и безопасности в отношении слежки в Интернете, что потребовало переоценки отношения эффективности к вмешательству используемых методов.

Машинное обучение – отрасль искусственного интеллекта, являющаяся одной из самых быстрорастущих областей информационных технологий. Этот термин относится к автоматическому обнаружению закономерностей и повторений в больших наборах данных с помощью различных методов «обучения». Алгоритмы машинного обучения заполняются наборами искусственных данных, содержащими определенные шаблоны, которые могут быть обнаружены в наборах реальных данных. Применительно к массовому наблюдению обучающие наборы состоят из личных данных или характеристик человека (имя, год рождения, содержание электронных писем, телефонных звонков и т. д.) и набора меток, указывающих, считают ли спецслужбы этого человека угрозой. Затем обученный алгоритм применяется к немаркированному набору данных с теми же функциями, и он вычисляет людей, представляющих собой угрозу обществу, на основании того, что он узнал. Точность этих алгоритмов зависит от характеристик набора данных и количества данных, которые используются для обучения.

Применение алгоритмов машинного обучения для работы полиции становится все более распространенным явлением. Одним из примеров является признание определенных районов как горячих точек для преступности. Математик, полицейский инспектор Испанского национального полицейского корпуса и докторант Гранадского университета Мигель Камачо-Колладос и преподаватель инженерии данных и знаний в Школе компьютерных наук и информатики Кардиффского университета Федерико Либераторе разработали систему принятия решений, которая предлагает, когда и где следует разворачивать полицейские патрули, на основе наборов данных, которые фиксируют время и место совершения преступлений в прошлом. Эти алгоритмы используются для определения того, где и когда могут быть совершены преступления, но не определяют, кто будет совершать преступления[4].

Данные, доступные для применения контртеррористических мер с помощью алгоритмов машинного обучения, отличаются от данных, которые используются в полицейской деятельности. Террористические акты, особенно те, которые совершаются одиночками, не связанными с какой-либо организацией, очень разнообразны по своим мотивам, планированию и исполнению. Цифровые следы потенциальных террористов могут значительно различаться, что приводит к отдельным точкам в данных обучения. Это усложняет обучение алгоритмов ма-

шинного обучения, поскольку уникальность многих атак увеличивает вероятность неправильного обучения и, следовательно, неточных алгоритмов. Распространенный подход к решению проблемы нерегулярных точек данных – увеличение размера обучающего набора данных. Поскольку большее количество обучающих данных, естественно, подразумевает более высокую вероятность достижения более надежных и точных алгоритмов, нерегулярность точек данных может быть исправлена таким образом. В случае локализованного прогнозирования преступности этот метод может дать результат, при этом набор данных о преступности, используемый для обучения алгоритма, просто увеличивается до размера, который дает достаточно точные результаты. Однако, в отличие от предсказания обычных преступлений, наборы данных, относящиеся к потенциальным террористическим актам, не могут быть так легко расширены. Это связано с тем, что маркировка наборов данных требует, чтобы потенциальных террористов уже идентифицировали как угрозу. Хотя Министерство внутренней безопасности США за последнее десятилетие составило обширный список для наблюдения, составленные им списки оказались весьма неточными, содержащими большое количество ложных срабатываний, т. е. людей, ошибочно обозначенных как угрозы[5].

Поскольку террористические атаки различаются по своим мотивам, планированию и осуществлению, цифровые следы, оставленные террористами во время подготовки атак, различаются в зависимости от импульса их действий. Например, религиозных или политических убеждений или проблем с психическим здоровьем, количество вовлеченных людей и способы их общения, которые могут быть зашифрованы или офлайн[6]. Кроме того, подсказки может быть трудно найти в одном наборе данных, но они могут стать более ясными при объединении данных из разных наборов. Эти характеристики требуют анализа большого количества функций или деталей и дают высокую «размерность» набора предметной области.

В конечном итоге алгоритмы машинного обучения для массового наблюдения должны быть обучены на большом количестве различных наборов данных, чтобы иметь возможность находить связь между ними. Эта проблема машинного обучения для больших данных называется проблемой размерности. Сложность статистического вывода, которая растет с увеличением размера набора данных, снижает точность и производительность алгоритма машинного обучения. Для массового наблюдения это означает, что выбор большего количества деталей для каждого подозреваемого может повысить точность алгоритма, но влечет за собой потребность в гораздо более обширном наборе данных. Следовательно, требуется больше точек данных о террористических атаках, и количество зарегистрированных террористических атак может оказаться слишком маленьким для надлежащего обучения.

Также существуют проблемы обработки данных, которые значительно снижают точность классификации алгоритмов машинного обучения. Применительно к массовому наблюдению это может привести к получению результатов, содержащих высокую степень неопределенности, что приведет к неправильной классификации уровня угрозы как для террористов, так и для невинных граждан.

Если метод выявления потенциальных террористов неточен, это может привести к переоценке или недооценке уровня угрозы. Большое количество наблюдаемых групп подразумевает, что даже высокоточный алгоритм может привести к большому количеству неверных оценок, для которых потребуется наблюдение человека, проверка с использованием различных методов.

В качестве наглядного примера: алгоритм с относительно высокой точностью 99,9%, примененный к набору данных о населении в 10 миллионов человек, предложит неточные оценки 10 000 человек. Увеличение популяции или снижение алгоритмической точности увеличивает потребность в более тщательном надзоре. Эта проблема становится еще более существенной, если учесть, что математические оценки общей производительности и, что более важно, точности алгоритмов машинного обучения, еще не разработаны. Чтобы поймать значительную часть террористов, правоохранительные органы ложно идентифицируют десятки тысяч граждан.

Одной из распространенных стратегий анализа сети является объединение коммуникаций через метаданные. Когда в алгоритм вводятся данные об отправителе, получателе (получателях), времени суток, продолжительности звонка и частоте соединений, могут быть использованы различные типы статистических методов сетевого анализа, которые в сочетании с теорией социальной психологии могут раскрыть роль индивидуумов внутри группы с разумным запасом погрешности. Правильным способом запуска процесса «больших данных» является доступ к большим объемам массовых коммуникаций и попытка выявить «темные сети», которые имеют общие характеристики, не разделяемые большинством пользователей телекоммуникаций.

Алгоритмы машинного обучения могут выводить более конфиденциальную информацию из полученных метаданных, что позволяет глубже заглянуть в личную жизнь людей.

Например, используя данные банковской карты, содержащие время, место и диапазон цен совершенных покупок, можно успешно идентифицировать владельцев анонимных банковских карт[7].

Алгоритмы машинного обучения, основанные исключительно на метаданных об активности сотовых телефонов (т. е. на том, какие номера вызывались и в какое время) смогли получить личную информацию о владельцах телефонов. Например, владеет ли человек огнестрельным оружием и даже какие у него проблемы со здоровьем.

Кроме того, аналитики использовали анонимный набор данных рейтингов фильмов Netflix для обучения алгоритма, который может определить, какие рейтинги из набора принадлежат одному и тому же пользователю[8].

Эти примеры показывают, что за последнее десятилетие автоматизированные алгоритмы смогли деанонимизировать наборы данных в нескольких приложениях, раскрывая личную информацию. Поскольку ожидается, что со временем алгоритмы станут более продвинутыми, сбор метаданных больше не следует рассматривать как незначительное нарушение конфиденциальности людей, поскольку деанонимизация больших наборов метаданных с большим количеством функций или большего количества записей будет еще быстрее.

При использовании набора данных с достаточным количеством помеченных случаев машинное обучение может помочь правоохранительным органам выявлять локальную преступность, тем самым отвечая на вопрос, где и когда будут совершены преступления. Однако при ответе на вопросы, кто будет совершать преступление, в частности террористическую атаку, характеристики наборов данных увеличиваются, а точки данных становятся более четкими, что приводит к алгоритмам машинного обучения, которые потенциально менее точны. Следовательно, ожидается, что количество ложных срабатываний и ложных отрицаний будет очень большим при использовании этих алгоритмов для обеспечения безопасности государства.

Более того, использование метаданных вместо данных не обязательно уменьшает нарушение конфиденциальности человека. Используя исследования из литературы за последнее десятилетие, которые сосредоточены на деанонимизации наборов данных о телефонных записях, данных банковских карт, местоположениях мобильных телефонов и рейтингах фильмов, необходима тщательная оценка фактической анонимности доступных данных. Кроме того, определение метаданных различается в зависимости от системы, что означает, что метаданные в одной системе считаются данными в других. В связи с этим важно тщательно определить типы разведывательных органов, которым разрешено собирать и передавать информацию.

С ростом производительности и точности алгоритмов машинного обучения эти методы могут помочь правоохранительным органам находить закономерности в правильно подобранных наборах данных, но в то же время они гораздо более навязчивы. Учитывая крайнюю редкость террористических актов и их универсальность в планировании и исполнении, можно предположить, что даже при постоянном прогрессе в машинном обучении обучение алгоритмов массового наблюдения будет проблемой, которую следует тщательно оценивать в ближайшие годы с учетом последствий крупных неточностей.

Библиографический список

1. Биго, Д., Каррера, С., Эрнанц, Н., Жандесбоз, Дж., Паркин, Дж., Рагацци, Ф., и Шеррер, А. Массовая слежка за персональными данными со стороны государств-членов ЕС и его совместимость с законодательством ЕС. (2013)
2. Гадепалли К., Норузи М., Даль Г. Е., Колбергер Т., Бойко А. и Штумпе М.С. Выявление метастазов рака на гигапиксельных изображениях патологии. (2017).
3. Боровец, С. AlphaGo одерживает победу со счетом 4:1 над гроссмейстером го Ли Седолом (2016)
4. Камачо-Колладос, М., и Либераторе, Ф. Система поддержки принятия решений для прогнозирующего патрулирования полиции. (2015)
5. Согоян, К. Небезопасный рейс: сломанные посадочные талоны и неэффективные списки наблюдения за террористами (2008)
6. Сирселуди, член парламента. Как предсказывать непредсказуемое: О раннем обнаружении террористических кампаний. Анализ обороны и безопасности, 21 (4), 369–386, (2005)

7. Де Монтжой, Ю.А., Радаэлли, Л., Сингх, В.К., и Пентланд, А.С. Уникальность в торговом центре: повторная идентификация метаданных кредитных карт. (2015)
8. Нараянан А., Шматиков В. Надежная деанонимизация больших разреженных наборов данных. (2008)

Осипова А. А.¹,

*заместитель командира взвода факультета
подготовки специалистов в области
информационной безопасности
Московского университета МВД России
имени В.Я. Кикотя, сержант полиции;*

Цимбал В. Н.²,

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

ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИИ BIG DATA В ДЕЯТЕЛЬНОСТИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

Проживая в новой эпохе, все больше и больше задумываешься о том, как развивается мир, какие технологии внедряются в нашу жизнь и как они влияют на будущее. Общий объем обрабатываемых в Интернете и иных сетях данных подсчитать очень сложно, но мы можем привести некоторые оценочные сведения. По исследованию IDC (International Data Corporation) в 2006 г. весь объем цифровых данных составлял 0,18 ЗБ, к 2011 г. он должен был увеличиться до 1,8 ЗБ, в 2018 г. этот показатель составил 33 ЗБ [1, с. 399], а к 2025 г. это будут уже 175 ЗБ [2, с. 77]; фондовая биржа в Нью-Йорке в день генерирует порядка терабайта информации; в проекте Internet Archive хранится более 2 ПБ данных; эксперименты на Большом адронном коллайдере могут формировать около 1 ПБ данных в секунду [3, с. 143].

В последние годы в сфере аналитики все чаще употребляется термин «Big Data», как и в медицине, финансах, интернет-компаниях и других отраслях. Наше государство наряду с другими в последнее время проявляет серьезный интерес к указанным технологиям. В рамках данной статьи нами будет рассмотрено, что представляют из себя «большие данные», области их применения, а также возможности использования в деятельности органов внутренних дел.

Какого-то однозначного подхода к терминологии понятия Big Data («Большие данные») нет, имеются разнообразные мнения на этот счет: согласно докладу Генерального секретаря ООН – это «...накопление и анализ значительно возросшего объема информационных ресурсов, который превышает возможности их хранения и анализа с использованием созданных ранее аппаратных и программных средств» [4, с. 10]; В. С. Овчинский и Е. С. Ларина приходят к выводу: «...это в первую очередь сырье для различного рода поведенческих технологий, ориентированных на группы достаточно большой размерности, таких как покупатели тех или иных товаров, избиратели, поклонники того или иного бренда, лица, ориентированные на те или иные банковские продукты и т. п.» [5, с. 65];

¹ © Осипова А. А., 2020.

² © Цимбал В. Н., 2020..

в другом источнике В. С. Овчинский предлагает другое по своему содержанию определение «...сбор, хранение, оцифровка и предоставление в удобном для пользователя виде в любой точке всей совокупности сведений о тех или иных событиях, процессах, явлениях и т. п.» [6, с. 21]; П. Д. Иванов и В. Ж. Вампилова формулируют следующее понятие «...серия подходов, инструментов и методов обработки структурированных и неструктурированных данных огромных объемов и значительного разнообразия» [7]; достаточно интересным и емким является определение сформулированное Oracle Corporation: «...разнообразные данные, которые поступают с постоянно растущей скоростью и объем которых постоянно растет... Три основных свойства больших данных – разнообразие, высокая скорость поступления и большой объем»[8].

Мы же постараемся сформулировать собственное видение данного термина, однако применительно к рассматриваемой в работе тематике. Под «Большими данными» понимается объемное количество разрозненных данных, которые по заданным пользователем характеристикам могут быть обработаны, систематизированы и получен искомым результат. В качестве примера можно привести любую информацию из Интернета (в соцсетях, интернет-магазинах, где используется программы лояльности, фото- и видеохостингах и т. п.), от разнообразных считывающих устройств, объектов здравоохранения, корпоративной информации и иного.

Каждый шаг, который человек делает в Интернете, – это «электронный след», т. е. данные, фиксируемые в цифровом формате и хранящиеся на различных носителях цифровой информации. Эти данные настолько огромны, что традиционное программное обеспечение для их обработки не справляется. Big Data основывается на трех основных характеристиках:

1. Volume (объем) – это количество информации. Большие данные обрабатываются в очень больших объемах. Они являются неструктурированными или могут быть неизвестного происхождения, могут занимать от нескольких десятков терабайт до сотен петабайт.

2. Variety (разнообразие) – большие данные относятся к многочисленным типам данных. Традиционные типы данных были структурированы и аккуратно вписаны в реляционную базу данных. Однако с ростом поступающей информации их все больше относят к неструктурированной, так как они зачастую нечетко сформулированы или требуют дополнительной предварительной обработки (например, аудио, видео или текст).

3. Velocity (скорость) – это скорость, с которой данные принимаются и обрабатываются. Их необходимо обрабатывать так, чтобы какие-то решения на основе этих данных принимались почти в реальном времени. То есть, с точки зрения человека, недолго, иногда долю секунды (например, в поиске), иногда несколько секунд (например, пока пользователь осматривается по сайту) на то, чтобы система подумала, что надо сформировать.

Также к характеристикам больших данных относят: value (ценность), veracity (достоверность) и variability (изменчивость).

Данную технологию следует назвать универсальной, поскольку ее использование пригодится в любой сфере деятельности, например:

1) предиктивная аналитика или диагностическое обслуживание (используемая для поиска потенциального преступника или для мониторинга состояния оборудования с целью выявления и предотвращения сбоев);

2) оптимизация продаж (разработка, снижение стоимости и оптимизация продукции);

3) банковская деятельность (оценка платежеспособностей, улучшение клиентского сервиса);

4) машинное обучение (обучение нейронных сетей);

5) стимулирование инноваций (с помощью изучения взаимозависимости, определения новых способов использования знаний) и многое др.

Благодаря этим обширным способностям больших данных, их возможно применять и в деятельности органов внутренних дел. Одной из главных проблем является установление личности преступников до и/или после того, как они начнут противоправные действия. К примеру, используя информацию, полученную из больших данных потенциально возможно предотвращать тяжкие и особо тяжкие преступления или значительно снизить процент преступности. Однако использование больших данных в деятельности правоохранительных органов является насущной проблемой, не имеющей простых, тривиальных или готовых решений. Обозначим сферы деятельности ОВД, где эффективно было бы применение больших данных:

- оперативно-разыскная деятельность;
- административно-правовая деятельность;
- предварительное следствие и дознание;
- экспертно-криминалистическая деятельность;
- деятельность по обеспечению информационной безопасности.

Объем информации, который получает сотрудник ОВД в ходе выполнения своих должностных обязанностей, постоянен и возрастает геометрически без фильтрации и в виде сплошного потока. Ведь найти преступника среди миллионов людей очень сложно: требуется установление личности с помощью отпечатков; показаний очевидцев и свидетелей; записей камер видеонаблюдения; установление транспортного средства, использованного при совершении деяния; установление соучастников или других подозреваемых, которые могут быть причастны по системе взаимосвязей; выявление местоположения или маршрутов передвижений в определенные периоды времени. На любую необходимую информацию для расследования и раскрытия преступлений или правонарушения нужно время. Например, если это прослушивание телефонных переговоров или просмотр камер видеонаблюдения, то информация обо всех разговорах и действиях фигуранта за значительный промежуток времени. Или это может быть получение данных о движении денежных средств по счетам или по действиям в Интернете, то это большой объем информации обо всех операциях за определенный период времени, а сами периоды могут быть от нескольких дней до нескольких месяцев или лет. Если речь идет о получении компьютерной информации или о получении информации из технических каналов связи, то это работа с обширной информацией из этого источника.

Вся перечисленная неотфильтрованная (несистематизированная, неупорядоченная и т. п.) информация и относится к Big Data, которые позволят правильно поставить конкретные вопросы, установить определенные критерии отбора, использовать специализированное программное обеспечение, то анализ, распознавание и получение искомой информации получится быстрый, эффективный, а процесс раскрытия и расследования преступления или правонарушения сократится в разы. А по завершении расследований эти данные следует рассортировать по показателям, совершенствуя разработку и выстраивая «дерево решений», где у каждой ветви имеется свой определенный вес (или же использовать Machine Learning, то есть машинное обучение для более оперативной работы с имеющейся информацией). Тогда при работе над последующими преступлениями сотрудник из задаваемых критериев отбора при помощи подобной технологии смог бы в кратчайшие сроки находить искомое.

Несмотря на все положительные моменты внедрения технологии больших данных в правоохранительные органы, есть и обратная сторона:

1. Действующие сотрудники не смогут воспользоваться данной технологией без дополнительного обучения, а лучше всего – это привлечение профильных специалистов, которые разбираются в технологии и смогут эффективно ее эксплуатировать. Сейчас в системе МВД России есть четыре учебных заведения, готовящих технических специалистов: Московский, Санкт-Петербургский и Краснодарский университеты, а также Воронежский институт.

2. Использование рассматриваемой технологии невозможно без соответствующего программного и технического оборудования. Ведь вся информация больших данных очень объемна, и ее надо где-то хранить, обрабатывать, анализировать и т. п.

3. Большие объемы затрат на внедрение технологии. Согласно прогнозу уже упоминаемой нами ранее аналитической компании IDC 2016 г. объем мирового рынка программного обеспечения, оборудования и сервисов в бизнес-аналитике и работе с Big Data составил 130,1 млрд. долларов. Большая часть расходов пришлась на банковский сектор (13,1 % или 17 млрд. долларов), дискретное (11,9 %), непрерывное производство (8,4 %), а также денежные вливания от государственных органов составили 7,6%[9].

4. Неточность получаемой при анализе больших данных информации. Даже совершенствуя такую технологию для определения (предсказания) возможных правонарушений или потенциальных преступников, алгоритмы будут не всегда выдавать точный ответ, а на полученную информацию (которая может являться недостоверной) сотрудники будут отвлекаться, проверяя ее аутентичность.

5. Коррупционная и/или иная преступная составляющая, которая может повлиять на результат анализа.

6. Сложность интеграции технологии Big Data в уже существующие и применяемые в ОВД программно-технические решения.

На сегодняшний день на рынке больших данных существует немалое количество программных решений (с точки зрения конечного пользователя): Apache Spark (Hadoop, Storm, Cassandra) (США), Lumify (США), Elastic (США), Oracle Data Mining (США), Mail.Ru Cloud Solutions (Россия) и иные.

Нельзя сказать, что из-за такого количества недостатков нельзя пользоваться технологией Big Data в деятельности ОВД. Однако в данный промежуток времени, как нам кажется, это невозможно из-за указанных минусов. В свою же очередь, положительные моменты применения подобной технологии очень заманчивы: это и автоматизация анализа большого объема информации, и прогнозирование тех или иных ситуаций (действий, поступков), и оперативная классификация сведений и др. Предположим, что данный перспективный ресурс в дальнейшем будет полноценно внедрен в работу правоохранительных органов, что позволит снизить количество преступлений и успешно раскрывать уже совершенные на территории нашей страны.

Библиографический список

1. Кляус, О. А. Применение технологий Big Data в современных условиях / О. А. Кляус, П. Т. Кляус // Стратегия устойчивого развития в антикризисном управлении экономическими системами : материалы VI Международной научно-практической конференции. – Донецк, 2020. – С. 395–406.
2. Дейтел, П. Python. Искусственный интеллект, большие данные и облачные вычисления / П. Дейтел, Х. Дейтел. – СПб.: Питер, 2020. – 864 с.: ил. – (Серия «Для профессионалов»).
3. Клеменков, П. А. Большие данные: современные подходы к хранению и обработке / П. А. Клеменков, С. Д. Кузнецов // Труды Института системного программирования РАН. – Ч. 23. – 2012. – С. 143–158.
4. Доклад Генерального секретаря ООН «Использование информационно-коммуникационных технологий для инклюзивного социально-экономического развития. Семнадцатая сессия. – Женева, 12-16 мая 2014 года. – 26 с.
5. Овчинский, В. С. Искусственный интеллект. Большие данные. Преступность / В. С. Овчинский, Е. С. Ларина. – М.: Книжный мир, 2018. – 188 с. – (Коллекция Изборского клуба).
6. Овчинский, В. С. Криминология цифрового мира : учебник для магистратуры / В. С. Овчинский. – М. : Норма ; ИНФРА-М, 2018. – 352 с.
7. Иванов, П. Д. Технологии Big Data и их применение на современном промышленном предприятии / П. Д. Иванов, В. Ж. Вампилова // Инженерный журнал : наука и инновации. – № 8 (32). – 2014 [электронный ресурс].
8. Что такое Big Data – большие данные // Oracle Россия и СНГ. – URL: <https://www.oracle.com/ru/big-data/what-is-big-data.html> (дата обращения: 05.12.2020).
9. Большие данные (Big Data) мировой рынок [электронный ресурс] // TAdviser (Государство. Бизнес. ИТ). – URL: [http://tadviser.ru/index.php/Статья: Большие_данные_\(Big_Data\)_мировой_рынок](http://tadviser.ru/index.php/Статья:Большие_данные_(Big_Data)_мировой_рынок) (дата обращения: 07.12.2020).

Плохих Е. М.¹,

*слушатель факультета подготовки специалистов
в области информационной безопасности
Московского университета МВД России
имени В.Я. Кикотя, младший лейтенант полиции;*

Овчинский А. С.²,

*профессор кафедры информационной
безопасности учебно-научного комплекса
информационных технологий Московского
университета МВД России имени В.Я. Кикотя,
доктор технических наук, профессор*

НАПРАВЛЕНИЯ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОГО ПРОТИВОДЕЙСТВИЯ ТЕРРОРИЗМУ

За последние несколько лет террористические атаки поставили под вопрос глобальную безопасность. Несмотря на то, что международные сообщества и государства по всему миру пытаются положить этому конец, криминальные группы все еще находят выход. Однако новые технологии искусственного интеллекта вносят свой вклад в борьбу с терроризмом.

Согласно Федеральному закону «О противодействии терроризму» понятие «терроризм» трактуется как «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».[4]

Использование аналитики для выявления финансирования терроризма, моделей и потенциальных горячих точек. Сфера аналитики мошенничества — хорошо изученная область с возможностью обнаружения различных типов мошеннических транзакций, неестественной финансовой деятельности, системных подозрительных транзакций и отмывания денег.[3] При расширении до анализа отмывания денег, полученных преступным путем, в разных регионах, аномалии и закономерности могут быть обнаружены в глобальных подпольных финансовых системах, которые являются проводниками финансирования терроризма. Инструменты интеллектуального анализа, анализа и визуализации данных позволяют собирать, связывать, отслеживать, анализировать и распространять разведывательную информацию и сведения о террористической деятельности. Помимо возможностей прогнозирования, интегрированные бесшовные системы могут предоставлять уведомления для предупреждающих действий.

Направления борьбы с терроризмом с помощью аналитики:

— выявление операций по отмыванию денег, используемых для финансирования терроризма;

¹ © Плохих Е. М., 2020.

² © Овчинский А. С., 2020.

- отслеживание террористических организаций / подозреваемых;
- выявление активных мест террористической деятельности в целях эффективного противодействия терроризму;
- связь террористических атак с геополитическими тенденциями и денежными путями;
- выявление потенциальных восстаний и спонсируемой террористами деятельности;
- прогнозирование потенциальных террористических действий на основе всего вышеперечисленного.

Программно-аналитические методы. Интеллектуальный анализ данных, анализ настроений, интеллектуальный анализ текста, методы машинного обучения и предиктивный анализ – вот некоторые из методологий, используемых для выявления терроризма и борьбы с ним. Международное агентство DARPA рассекретило информацию о поисковой системе Memex по сайтам Невидимой сети (Deep Web). Поисковик разработан для нужд спецслужб. Например, подразделение минобороны использует этот софт для отслеживания информации о торговле людьми.

Невидимая сеть – это сайты Tor и запароленные форумы и сайты, требующие регистрации. Есть еще различные базы данных (юридические, судебные, адресные и т.д.), которые не хранят документы в статичном виде, а выдают их после заполнения формы[2] и серверы, которые выдают информацию с каких-либо сенсоров. Это огромный массив сведений, недоступный обычным поисковикам вроде Google и Bing. Правоохранительным органам крайне важно иметь доступ к этой информации.

Программа Memex выдает мгновенные результаты поиска для определенных областей и задач, таких как закономерности преступности в масштабах региона или определенные связи с автомобилем, используемым для террористической деятельности.

DARPA пишет, что обычные поисковики не устраивают их еще и с технологической точки зрения, потому что выдают информацию слишком примитивно – в виде ссылок. Нужны продвинутые возможности – например, составление списков с конкретными фамилиями, отслеживание изменения информации по определенным запросам, поиск закономерностей в собранных данных.

Для создания поисковика DARPA сотрудничало с 17 исследовательскими группами из частных компаний и университетов, чтобы разработать способы извлечения, анализа и организации информации, полученной из Скрытой сети.

Естественно, система Memex не доступна для обычной публики и о ней известно очень мало. Есть только сведения о ее применении различными агентствами. Очевидно, что подобные инструменты есть и в разведслужбах.

По мере того, как террористы и террористические организации вступают в новую эру с помощью технологий, передачи информации в Интернете и сбора средств от кибератак, страны всего мира также используют искусственный интеллект для борьбы с экстремизмом. Некоторые из популярных инструментов,

используемых в этом процессе, – это распознавание лиц, искусственная нейронная сеть и анализ социальных сетей. Вот несколько примеров применения.

Машинное обучение. Прогнозирование и анализ больших данных с использованием машинного обучения и структуры прогнозирования можно интегрировать с ГИС-системой для определения точного местоположения подозрительных попыток, перехода границы каждого региона. Машинное обучение может считывать аудио и видео каждого кадра, сегментировать в соответствующую область хранения данных и уведомлять о таких кадрах при попадании в данную область. Экспресс аналитика как часть машинного обучения может не только прогнозировать атаку, но также может реагировать на атаки в режиме реального времени. Платформа искусственного интеллекта может немедленно вызвать тревогу или уведомить соответствующее должностное лицо о необходимости принять меры в случае необходимости.

Интеллектуальная система управления транспортом позволяет отслеживать передвижения террористов. Интеллектуальная система управления транспортом включает сигнал тревоги и уведомляет должностных лиц, если подозрительный автомобиль движется в поле зрения камер данной системы. Технология также отправляет оповещение при обнаружении автомобиля с поддельным номерным знаком.

Платформы социальных сетей вышли на первый план в технологическую эпоху. Однако дезинформация становится угрозой национальной безопасности. Компания Facebook недавно объявила, что платформа использует искусственный интеллект для поиска и удаления контента, связанного с терроризмом, из социальных сетей. Facebook использует технологию распознавания изображений для выявления и предотвращения распространения фотографий и видео известных террористов на другие учетные записи. Компания также предложила использовать алгоритмы машинного обучения для поиска шаблонов террористической пропаганды, чтобы их можно было быстро удалить из профилей других пользователей. Эти усилия по борьбе с терроризмом будут распространены на другие платформы, принадлежащие Facebook, включая WhatsApp и Instagram. Также Facebook сотрудничает с другими технологическими компаниями, включая Twitter.

Сценарии использования. Проект «Вычислительный анализ террористических групп» – отличный пример того, как аналитические методы могут быть использованы для борьбы с терроризмом. Модель, разработанная исследователями из Университета Мэриленда, известная как «Система вероятностей времени», помогает прогнозировать террористические атаки, совершаемые конкретной террористической организацией. Система использовала алгоритмы для анализа извлеченных данных по 770 переменным за 20 лет деятельности террористических организаций, которые ежемесячно обновляются для компьютерного анализа. Это помогло понять факторы, определяющие частоту атак, тип террористических атак, используемых в различных геополитических ситуациях, тенденции в представлении террористической деятельности и другие критерии. Алгоритмы также использовались для определения условий, которые могут привести к атакам.

Департамент полиции Лос-Анджелеса и Лондонская столичная полиция используют сложные системы анализа данных, «предназначенные для выявления и связывания соответствующих разведывательных данных, чтобы помочь сдерживать террористические атаки и реагировать на них».

Окупаемость инвестиций от использования аналитики для противодействия терроризму не может быть определена количественно.

Хотя системы ГИС используются для противодействия терроризму, существует множество способов использовать возможности аналитики для выработки тактических стратегических решений по борьбе с терроризмом и обеспечению общественной безопасности.

Борьба с терроризмом с помощью видеонаблюдения и предиктивной аналитики. После теракта 11 сентября 2001 г. повышенная безопасность авиаперелетов вызвала затруднения для большинства пассажиров. Крушение российского самолета Metrojet над Синаем в Египте 31 октября 2015 г. показывает, что наблюдение в аэропорту все еще необходимо усилить. Возможно, худший компромисс усиленного наблюдения – это постепенная утрата человеком разумных ожиданий конфиденциальности. Это вызывает серьезные вопросы в демократических странах, но в конечном итоге усиление наблюдения – меньшее зло в войне с терроризмом. Видеонаблюдение (обычно с помощью замкнутого телевидения и IP-камеры) и мониторинг коммуникаций (особенно по телефонии и Интернету), несомненно, заслуживают большего внимания.

Роль аналитики больших данных и Интернета вещей (IoT). Здесь вступает в игру анализ больших данных и Интернета вещей.[1] Последние достижения в области видеонаблюдения включают усовершенствованные механические, оптические и электронные устройства. Камеры видеонаблюдения с высоким разрешением позволяют повышать уровень детализации и получать более четкие изображения, что очень важно для целей идентификации. Количество видеокамер, микрофонов и других датчиков для целей наблюдения растет с невероятной скоростью и обычно генерирует взрывоопасный объем данных. С растущей интеграцией между государственными и частными сетями видеонаблюдения, включая недавнюю разработку видео в частных автомобилях и нательного видео, видеонаблюдение выводит его на новый уровень.

Важнейшим элементом в этой области является разработка программного обеспечения для анализа видеоконтента (VCA). Обработывая терабайты данных, собираемых камерами, новые алгоритмы анализа изображений улучшают задачи идентификации, особенно человеческих лиц (системы распознавания лиц). Эти новые аналитические технологии видеонаблюдения быстро развиваются, включая отслеживание нескольких человек и динамический анализ изображений, что означает, например, способность программного обеспечения использовать 3D-методы для идентификации каждого человека в движущейся толпе.

Эта область все еще находится в зачаточном состоянии, но быстро развивается. В результате большие данные, генерируемые устройствами мониторинга по всему миру, становятся источником прогнозной аналитики. Новые алгоритмы анализа изображений улучшают задачи идентификации, особенно человеческих лиц (системы распознавания лиц).

Предиктивная аналитика фиксирует отношения между независимыми (или независимыми) переменными и прогнозируемыми переменными из прошлых событий, чтобы создать шаблоны данных для прогнозирования неизвестных результатов. Прогностический анализ, применяемый к извлеченным данным наблюдений, может предсказывать поведение человека на основе анализа нескольких моделей, аналогичных прошлым событиям. Все чаще разрабатывается новое программное обеспечение для моделирования для полностью автоматизированной семантической маркировки записей отслеживания на основе множественного обнаружения присутствия человека и аномальной активности.

Разрабатываются и другие модели для автоматической сортировки видео и сообщений с целью выявления агрессивного поведения, особенно в общественных местах. Приток извлеченных данных в этом отношении и постоянная разработка новых алгоритмов для их обработки будет обеспечивать предиктивный анализ с исключительными инструментами для составления возможных сценариев насилия. Это открывает новые возможности для наблюдения, в частности для предписанного анализа, во избежание угроз.

Крупные компании по видеонаблюдению все чаще работают с компаниями-разработчиками программного обеспечения для анализа видеоконтента в целях прогнозирования. Последние разработки в области робототехники, в частности, в отношении улучшенного цифрового зрения и способности машин распознавать окружающую среду с помощью нескольких датчиков изображения и учиться на ошибках, означают, что искусственный интеллект постепенно заменит людей с такими задачами, как видеонаблюдение и др. общение. Такая работа трудна и малоэффективна для человека, так как люди склонны к перенапряжению глаз и утомлению при просмотре записей с камер в течение длительного времени.

Таким образом, можно сделать вывод, что развитие средств и способов борьбы с терроризмом с помощью аналитических методов не стоит на месте. Взаимодействие заинтересованных в борьбе с террором и экстремизмом коммерческих компаний, производящих продукты в сфере аналитики, в тандеме с органами госбезопасности всех стран может привести к разрешению многих проблем борьбы с терроризмом, а также установлению всех заинтересованных в порождении и продвижении бесчеловечных поступков в отношении граждан.

Библиографический список:

1. Samuel, M G. How to fight terrorism with video surveillance and predictive analytics [электронный ресурс] // Icrunch Data, LLC. – URL: <https://icrunchdata.com/blog/352/how-to-fight-terrorism-with-video-surveillance-and-predictive-analytics>.
2. Predictive Policing to Combat Terrorism [электронный ресурс] // Predictive Analytics. – URL: <https://www.predictiveanalytics.co.ke/blog/predictive-analytics/predictive-policing-to-combat-terrorism>.
3. Deogawanka, S. The fight against terrorism – analytics application [электронный ресурс]. // Analytics India Magazine – URL : <https://analyticsindiamag.com/fight-terrorism-analytics-application>.
4. Федеральный закон «О противодействии терроризму» от 6 марта 2006 г. № 35-ФЗ (ред. от 31.12.2014 г.) // Российская газета. – № 48. – 2006. – 10 мар.

Курбатова М.С.¹,

*курсант факультета подготовки специалистов
в области информационной безопасности*

*Московского университета МВД России имени В.Я. Кикотя,
рядовой полиции*

Клочкова Е. Н.²,

*доцент кафедры специальных информационных технологий
учебно-научного комплекса информационных технологий*

*Московского университета МВД России имени В.Я. Кикотя,
полковник полиции*

КИБЕРТЕРРОРИЗМ КАК УГРОЗА СОВРЕМЕННОМУ ИНФОРМАЦИОННОМУ ОБЩЕСТВУ

В настоящее время идет стремительное развитие информационных технологий, которое упрощает жизнь человека. Однако существуют и негативные последствия, а именно увеличение преступных посягательств с использованием глобальной информационно-телекоммуникационной сети «Интернет». В этой связи появляются новые понятия, ранее не использовавшиеся в лексиконе. Одним из таких понятий является кибертерроризм.

Термин «кибертерроризм», или «компьютерный терроризм», впервые прозвучал в восьмидесятые годы прошлого столетия, но и в настоящее время до конца не определены границы данного понятия. В законодательстве Российской Федерации оно до сих пор не закреплено, в этой связи говорить об однозначности трактовки исследуемого термина не приходится. Очень часто в средствах массовой информации, говоря о кибертерроризме, подразумевают любое преступление, совершенное в сети «Интернет». На наш взгляд, такая трактовка некорректна.

Существует два основных определения кибертерроризма. Ряд исследователей считают, что под кибертерроризмом следует понимать преступные посягательства в киберпространстве, в результате чего возникает угроза безопасности личности, обществу и государству [1]. Целью кибертерроризма в этом случае является повышение напряженности в обществе, а также нагнетание страха с целью возможности воздействия при принятии решений в политических, экономических и социальных сферах жизни. Способами такого воздействия могут являться угрозы причинения вреда здоровью, воздействия на материальные объекты информационно-телекоммуникационных сетей, искажение правдивой информации с целью введения в заблуждение людей, хищение личных данных пользователей с целью последующего шантажа и получения денежного вознаграждения.

По мнению других исследователей, понятие «кибертерроризм» является схожим с понятием «терроризм», однако атаки осуществляются на компьютерную систему и сеть, в результате чего нарушается работа важнейших инфра-

¹ © Курбатова М. С. 2020.

² © Клочкова Е. Н., 2020.

структурных объектов, таких как, например больницы, банки, электростанции, создавая тем самым опасность для жизни и здоровья людей, а также возможность наступления иных тяжких последствий. Особенностью кибертерроризма является и то, что преступники не используют взрывные устройства, не захватывают заложников, а все противоправные действия совершают с помощью компьютерных вирусов, специализированного программного обеспечения, а также различного вида атак на сервера (DoS-атаки, DDoS-атаки). Данное описание исследуемого понятия является более ограниченным по своему содержанию.

Информатизация общества, с одной стороны, привела к упрощению доступа обывателей к информации различного рода, но с другой стороны, преступники также стали активно пользоваться возможностями сети «Интернет» для общения и вовлечения новых людей в свои ряды, используя в своих целях популярные социальные сети, такие как ВКонтакте. Более того, террористические организации создают свои сайты, а осуществляют общение через мессенджеры, которые поддерживают шифрование данных. Сложность в обнаружении таких лиц заключается и в том, что чаще всего деятельность осуществляется через «Darknet» [2], т. е. так называемую «темную» часть Интернета, которая по объему значительно больше привычной сети «Интернет». Доступ в «Darknet» осуществляется с использованием специализированного браузера Tor. Для соединения между пользователями применяется «луковая» маршрутизация с использованием туннельного шифрования. Исходная информация шифруется несколько раз и передается через несколько сетевых узлов, причем минимальное количество таких узлов не должно быть менее трех. Далее при передаче сообщения маршрутизатор удаляет необходимое шифрование, чтобы определить следующий маршрутизатор, на который будет передана информация. Аналогичные действия происходят и на последующих узлах. Таким образом, осуществляется возможность скрыть IP-адреса серверов, на которых расположены сайты, а также информация об источнике, пункте назначения и содержанием сообщения является недоступной. По этой причине данная часть сети обладает высокой степенью анонимности, что усложняет поиски террористов.

Привлечение в свои ряды ИТ-специалистов, способных организовать атаку в киберпространстве, также является одной из основных задач, стоящих перед террористическими организациями. Причем, для совершения противоправных действий террористам не обязательно иметь хорошее техническое обеспечение. К примеру, с помощью обычных методов общения в любой социальной сети имеется возможность узнать нужную информацию о лице и проанализировать ее. Вербовкой новых лиц в террористические организации занимаются достаточно хорошие психологи, знающие все необходимые механизмы пропаганды и вовлечения. В этой связи, даже взрослому и достаточно образованному человеку сложно противостоять такому воздействию и манипуляции, а молодому специалисту тем более. Говоря о таких специалистах необходимо отметить, что зачастую они являются талантливыми людьми, которые могут достаточно легко подвергаться негативному влиянию, при этом в силу своего возраста не имеют достаточного жизненного опыта, чтобы распознать угрозу от общения.

Совершать акты террора в компьютерной сфере способны многие террористические организации, в том числе и запрещенная в Российской Федерации террористическая организация ИГИЛ [3]. Данные атаки способствуют дестабилизации обстановки на Ближнем Востоке, приводят к возникновению кризисных ситуаций в отношениях между различными странами. Мы можем говорить о появлении принципиально нового вида терроризма – кибертерроризма. При этом необходимо различать хакеров и кибертеррористов. Отличительной особенностью последних являются действия, способные причинить тяжкие последствия, такие как гибель людей, разрушения. Преступления совершаются по идеологическим, политическим, религиозным мотивам, с целью выдвижения каких-либо требований. Хакеры же преследуют в своих действиях чаще всего материальную выгоду, но не разрушения или выполнение своих требований [4].

Признаком кибертерроризма может стать его открытость, так как террористы стремятся к тому, чтобы как можно больше людей узнало об их противоправных действиях, пытаясь максимизировать ущерб от своей деятельности, стараясь заставить паниковать как можно больше людей.

В заключение хотелось бы отметить, что законодательное закрепление понятия «кибертерроризм» позволит разрешить некоторые спорные вопросы в данной области. Информационная сфера в настоящее время является наиболее уязвимой, и в будущем количество преступлений будет только возрастать, то закрепление понятия кибертерроризм в нормативных документах позволит выделить исследуемое противоправное действие из других преступлений, относящихся к компьютерным. В настоящее же время данный термин применяется достаточно широко, и для несведущих людей обозначает практически любое преступление, совершенное в сети «Интернет».

Библиографический список

1. Васенин, В. А. Информационная безопасность и компьютерный терроризм // Научные и методологические проблемы информационной безопасности (сборник статей) / под ред. В. П. Шерстюка. – М.: МЦНМО, 2004. – С. 67–84. – URL: http://www.iisi.msu.ru/UserFiles/File/publications/sherstyuk_ed.pdf (дата обращения: 06.12.2020);
2. Поликарпов, Е. С. Компьютерная разведка : учебное пособие / сост. Е. С. Поликарпов. – Краснодар: Краснодарский университет МВД России, 2018. – 263 с.
3. ИГИЛ занимается кибертерроризмом – спецпред президента России [электронный ресурс] / Сетевое издание www.tvzvezda.ru. – URL: https://tvzvezda.ru/news/vstrane_i_mire/content/201605270125-g3cp.htm (дата обращения: 05.12.2020).
4. Кибертерроризм [электронный ресурс]. // АМ-Медиа. – URL: <https://www.anti-malware.ru/threats/cyberterrorism> (дата обращения: 06.12.2020).

Попова С. Н.¹,

*курсант факультета подготовки специалистов
в области информационной безопасности
Московского университета МВД России
имени В.Я. Кикотя, рядовой полиции*

Цимбал В. Н.²,

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

ПРИМЕНЕНИЕ СИСТЕМ БИОМЕТРИЧЕСКОЙ ИДЕНТИФИКАЦИИ В ПРОТИВОДЕЙСТВИИ ТЕРРОРИЗМУ

С каждым годом общество все больше и больше погружается в информатизацию процессов. Примерами служат подача электронных заявлений через государственный портал, использование электронных подписей, банковские онлайн-операции и т. д. С появлением данных процедур остро встал и вопрос удостоверения личности граждан, в частности, с помощью биометрических систем идентификации.

Под биометрией понимается автоматическое распознавание индивидов, основанное на их поведенческих и биологических характеристиках [1].

Под биометрической характеристикой понимается биологическая и поведенческая характеристика индивида, которая может быть использована в качестве отличительных повторяющихся биометрических признаков для биометрического распознавания [2].

Биометрическая идентификация использует природные свойства пользователя – отпечаток пальца, голос, структура сетчатки глаза, особенности строения лица и др. В отличие от других методов идентификации (основанных на факторах знания какой-либо информации или владения каким-либо идентифицирующим предметом) не возникает проблемы сохранности идентификационной информации, так как каждый человек уникален. Также данный идентификатор невозможно передать посторонним лицам.

Стремительное развитие технологий позволяет широко пользоваться ими во всех сферах жизнедеятельности человека. Информационные технологии направлены на облегчение, увеличение уровня удобства различных процедур, совершаемых человеком, в сочетании с высоким уровнем защиты личной информации, что считается важным фактором безопасного взаимодействия населения с организациями.

В данной статье рассмотрены основные виды биометрических систем идентификации, их принципы работы, преимущества и недостатки, их применение

¹ © Попова С.Н., 2020.

² © Цимбал В.Н., 2020.

в ОВД. Также приведены проблемы их внедрения, как с технической, так и с нормативно-правовой точки зрения.

Биометрические системы идентификации – это системы, которые требуют предъявления уникальных физических или поведенческих характеристик человека в различных целях. Они бывают разные, исходя от того, под какой природный идентификатор разработаны.

Методы биометрической идентификации принято делить на два класса[10]:

1. Статические методы основаны на физиологических характеристиках человека, присутствующих с ним на протяжении всей его жизни. К статической биометрической идентификации относятся идентификация по отпечаткам пальцев, по радужной оболочке глаза, по сетчатке глаза, по геометрии руки и лица, по термограмме лица, по ДНК, по рисунку вен, по акустическим характеристикам уха.

2. Динамические методы основаны на поведенческих характеристиках людей, на подсознательных движениях в процессе воспроизведения или повторения какого-либо обыденного действия. К динамической биометрической идентификации относятся идентификация по голосу, по рукописному почерку, по клавиатурному почерку, по особенностям походки человека.

Также существуют определенные критерии для биометрических параметров:

- всеобщность (универсальность): данный признак должен присутствовать у всех людей без исключения;
- уникальность: не существует абсолютно двух одинаковых людей с одинаковыми физическими и поведенческими параметрами;
- постоянство: для корректной аутентификации необходимо постоянство во времени;
- измеримость: возможность измерить признак каким-либо устройством для дальнейшего занесения в базу данных;
- приемлемость: общество не должно быть против сбора и измерения биометрического параметра [3, с. 268];
- эффективное функционирование: они должны быть точными, быстрыми в обработке и надежными как на начальном, так и на последующих этапах технологического процесса;
- уязвимость к возможным действиям в обход – потенциально злоумышленники могут получить санкционированный доступ с помощью различных приспособлений и устройств-«обманок»; для противодействия этому необходимо принимать и постоянно совершенствовать жесткие контрмеры [4, с. 8].

Усиленной версией биометрической идентификации является мультимодальная (комбинированная), под которой понимается использование нескольких биометрических идентификаторов [5, с. 175]. Она считается более надежной в силу того, что будет сложнее подделать несколько человеческих характеристик, нежели один.

Выделим системы биометрической идентификации, являющиеся наиболее популярными, а также обозначим в некоторых технологиях процент их использования в России [6, с. 88].

1. Отпечатки пальцев рук (29 %) – метод основан на определении структуры линий, которые находятся на подушечках пальцев (папиллярных узорах).

2. Рисунок вен на пальцах/руках (17,3 %) – инфракрасные лучи проходят через поверхность кожи, где они поглощаются венозной кровью. Специальная камера фиксирует изображение, оцифровывает данные, а затем либо сохраняет их, либо использует для подтверждения личности.

3. Радужная оболочка глаза (0,3 %), которая состоит из толстых нитевидных мышц, формирующих зрачок человека. Специальные инструменты определяют именно эти уникальные складки.

4. Сетчатка глаза – в случае данного метода сканируются капиллярные сосуды внутри глаза с помощью камер ближнего инфракрасного диапазона. Получившееся изображение обрабатывается для улучшения его качества, а затем преобразовывается в цифровой шаблон для последующей сверки для распознавания пользователя.

5. Лицо (50 %) – данный метод позволяет измерять геометрию лица человека, которая включает в себя множество параметров, например, расстояние между глазами, расположение бровей, длина рта и т. д. После сбора данные преобразуются в системе в зашифрованный код, который называется подписью (сигнатурой) лица.

6. Голос (4 %) – специализированные инструменты фиксируют тон, тембр, темп речи и пр., который также неповторим для каждого человека.

7. ДНК – метод обладает абсолютной точностью. Также он единственный, который может отслеживать родственные связи, что особо ценно при работе с пропавшими без вести, определении жертв катастроф, аварий. Материал, содержащий последовательности коротких tandemных повторов, может собираться из волос, слюны, потожировых выделений, крови и т. д. С их помощью можно однозначно подтвердить личность, сравнивая их с другими tandemными повторами в базе данных; и иные методы [7, с. 183–184].

Нормативной составляющей использования биометрических систем в нашей стране являются следующие акты.

1. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

2. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

3. Постановление Правительства Российской Федерации от 6 июля 2008 г. № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных».

4. ГОСТ Р ИСО/МЭК 19784-1-2007 Автоматическая идентификация. Идентификация биометрическая. Биометрический программный интерфейс. Часть 1. Спецификация биометрического программного интерфейса.

5. ГОСТ Р ИСО/МЭК 19794-2-2013 Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 2. Данные изображения отпечатка пальца – контрольные точки.

6. ГОСТ Р ИСО/МЭК 19794-5-2013 Информационные технологии (ИТ). Биометрия. Форматы обмена биометрическими данными. Часть 5. Данные изображения лица.

7. ГОСТ Р ИСО/МЭК 19795-1-2007 Автоматическая идентификация. Идентификация биометрическая. Эксплуатационные испытания и протоколы испытаний в биометрии. Часть 1. Принципы и структура и другие.

Все ранее перечисленные методы имеют широкую область применения и распространены в различных сферах:

- правоохранительная сфера: выявление преступников, подозреваемых;
- военная отрасль: идентификация противника и/или союзника, а также лица, допущенного к чему-либо (солдат, командир);
- финансовый сектор: идентификация и мониторинг пользователей банковского обслуживания, страхования;
- государственный сектор: системы электронных документов, содержащие биометрические данные (электронные паспорта и удостоверения, водительские права и т. п.);
- пограничный и миграционный контроль: идентификация путешественников, мигрантов, пассажиров;
- здравоохранение и социальное обеспечение: идентификация пациентов и медицинских работников, получателей социальной помощи;
- продажи: идентификация и мониторинг потребителей и покупателей, обнаружение нарушителей.

Возможно выделить существенные плюсы систем биометрической идентификации:

- 1) высокий уровень защиты от подделки (подмены, обмана);
- 2) наличие идентификатора при человеке постоянно;
- 3) простота доступа к защищаемой системе, иными словами – удобство использования подобных систем.

Но, несмотря на положительные стороны, внедрение подобных систем в повсеместный оборот имеет достаточное количество проблем и недостатков:

- дополнительные требования к оборудованию (защита от механического воздействия, влаги, несанкционированного доступа и т. д.);
- высокая стоимость оборудования;
- некомпетентность и/или незнание применяемых технических решений со стороны пользователя (в некоторых случаях);
- недоверие со стороны граждан (различные конспирологические теории);
- вероятность того, что биометрические данные могут быть сфальсифицированы;
- публичность биометрических данных. Особенно в нынешнее время, когда очень популярны социальные сети. Можно найти фото, видео- и аудиозаписи многих людей, что в свою очередь ставит под сомнение надежность систем биометрической идентификации.

Биометрическая идентификация нашла широкое применение и в правоохранительной сфере. Ее значение для правоохранительных органов велико – с по-

мощью внедрения биометрии многие задачи стали легче решаемы. В ОВД биометрия применяется для обеспечения общественной безопасности и общественного порядка, раскрытия и расследования преступлений и в системах защиты. Для обеспечения общественной безопасности в местах массового скопления людей (аэропорты, метрополитен, стадионы и др.) устанавливаются специальные аппараты, способные идентифицировать человека по геометрии лица, по походке. Такие системы позволяют предотвратить теракты или же заметить преступников, находящихся в розыске.

В современном мире применение биометрической идентификации является одним из важных аспектов эффективной борьбы с преступлениями против основ конституционного строя и безопасности государства, прав и интересов человека и гражданина, общественных и коммерческих структур. Также широкое применение биометрические технологии позволяет противостоять терроризму, организованной и трансграничной преступности, торговле наркотическими веществами, незаконной миграции, работоторговле.

Перспективными возможностями применения биометрических технологий в борьбе с терроризмом являются следующие:

- идентификация лиц, которые подозреваются в совершении преступлений, по биометрическим данным (путем создания банка биометрических данных преступников рассматриваемой направленности, которые будут содержать следующие биометрические характеристики: ДНК, голос, отпечатки пальцев рук и иное);
- применение современных программных решений для анализа полученной информации и оперативного ответа на запросы сотрудников;
- совершенствование законодательства с целью упрощения доступа сотрудников правоохранительных органов к информации, которая имеется в распоряжении организаций различных форм собственности, индивидуальных предпринимателей и т. п. (информация с камер видеонаблюдения, систем контроля и управления доступа и иного);
- упрощение возможности доступа к различным банкам данных, биометрическим системам государственных органов (например, Единая биометрическая система, Единая система идентификации и аутентификации (ФГИС ЕСИА)[9]);
- международный обмен биометрическими данными: доступ к базам данных, обмен опытом, обучение сотрудников.

Биометрические системы безопасности разнообразны в силу наличия у человека множества уникальных физических и поведенческих признаков. Современные технологии позволяют с высокой точностью и оперативностью идентифицировать человека. Данное направление становится актуальнее и востребованнее год за годом за счет быстрого цифрового развития.

Необходимо отметить, что биометрические технологии стоят и на вооружении органов внутренних дел, оказывая посильную помощь при раскрытии преступлений и предоставлении своевременной помощи гражданам. Их использование облегчает деятельность служащих и помогает эффективно справляться с поставленными задачами [8, с. 293].

Библиографический список

1. ГОСТ ISO/IEC 19794-1-2015 Информационные технологии (ИТ). Биометрия. Форматы обмена биометрическими данными. Часть 1. Структура.
2. ГОСТ Р 54412-2019 (ISO/IEC TR 24741:2018) Информационные технологии (ИТ). Биометрия. Общие положения и примеры применения.
3. Иванов, Г. Н. Управление доступом к сети и услугам связи с использованием биометрических методов идентификации / Г. Н. Иванов, А. И. Парамонов, П. И. Смирнов // Информационные технологии и системы : управление, экономика, транспорт, право. – 2019. – № 2 (34). – С. 266–270.
4. Сборник практических рекомендаций ООН по ответственному использованию биометрических данных и обмену ими в рамках борьбы с терроризмом [электронный ресурс]. – 83 с. – Режим доступа: официальный сайт ООН. URL: <https://www.un.org/sc/ctc/wp-content/uploads/2019/04/V1808431-Biometrics-Manual-RUSSIAN.pdf>.
5. Сесин, Е. М. Системы идентификации личности, основанные на интеграции нескольких биометрических характеристик человека / Е. М. Сесин, В. М. Белов // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2012. – № 1–2 (25). – С. 175–179.
6. Пчеловодова, Н. Российский биометрический рынок в 2019–2022 гг. // Системы безопасности. – 2019. – № 2 (146). – С. 88–91.
7. Шумилин, В. П. Применение биометрического метода распознавания лица в правоохранительных органах / В. П. Шумилин, С. Л. Паньков // Научный вестник Орловского института МВД России имени В.В. Лукьянова. – 2019. – № 4 (81). – С. 182–186.
8. Бойко, А. А. Обзор биометрических систем безопасности. Применение биометрических систем контроля доступа в деятельности сотрудников органов внутренних дел / А. А. Бойко, Ю. С. Милевская // Вестник Московского университета МВД России. – 2017. – № 5. – С. 291–293.
9. Единая биометрическая система [электронный ресурс] // Официальный сайт Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации. – URL: <https://digital.gov.ru/ru/activity/directions/802>. (дата обращения: 07.12.2020).

Рудакова Н. К.¹,

*слушатель факультета подготовки специалистов
в области информационной безопасности*

*Московского университета МВД России имени В.Я. Кикотя,
младший лейтенант полиции*

Клочкова Е. Н.²,

*доцент кафедры специальных информационных технологий
учебно-научного комплекса информационных технологий*

*Московского университета МВД России имени В.Я. Кикотя,
полковник полиции*

ВОПРОСЫ ПРОТИВОДЕЙСТВИЯ РАСПРОСТРАНЕНИЮ ЭКСТРЕМИСТСКОЙ ДЕЯТЕЛЬНОСТИ В СЕТИ «ИНТЕРНЕТ»

В Российском законодательстве наравне с иными существует правовая норма, благодаря которой экстремистская деятельность стала уголовно наказуемым деянием. Ст. 282 УК РФ предусматривает уголовную ответственность за возбуждение ненависти либо вражды, а равно унижение человеческого достоинства. Среди преступлений против основ конституционного строя и безопасности государства экстремизм является одним из самых опасных преступных деяний.

Групповой молодежный экстремизм – противоправная деятельность организованной группы физических лиц в возрасте от 14 до 25 лет, объединенных по принципу расовой, национальной, религиозной, политической, социальной или иной ненависти либо вражды. В политическом аспекте экстремизм выступает против сложившихся общественных структур и институтов, пытаясь подорвать их стабильность, как правило, силовыми методами. Для этого экстремистские организации организуют беспорядки, акции гражданского неповиновения, террористические акции, используют методы партизанской войны. При этом они придают исключительно большое значение общественному резонансу, вызываемому их действиями.

Основная цель экстремизма – навязывание определенных убеждений населению и привлечение как можно большего числа единомышленников в свои организации. В наши дни информационное пространство сети «Интернет» широко используют для вербовки новых членов различные экстремистские и террористические организации, радикально настроенные группировки, при этом основной целью данной работы становится претворение в жизнь идеологии экстремистской направленности.

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

¹ © Рудакова Н. К., 2020.

² © Клочкова Е. Н., 2020.

Распространение молодежного экстремизма в сети «Интернет» становится все более острой проблемой для «мирных» граждан, так как увеличивается количество преступлений, поднимается уровень насилия, при этом сам экстремизм становится все более жестоким и профессиональным. Данный вид экстремизма можно определить как информационный экстремизм.

На текущий момент, несмотря на все предпринимаемые меры, в сети «Интернет» ведется активная деятельность по вербовке последователей, готовых осуществлять экстремистскую деятельность. Причем основным контингентом такой деятельности становится молодежь. Вербовка осуществляется по трем направлениям. Одно из них связано с тем, что в сети создаются сайты экстремистских организаций, посетители, которых в дальнейшем, если они заинтересовались, могут вовлекаться в незаконную деятельность. Это фактически начальная стадия вербовки, когда из всех посетителей сайта, отбираются те, которых в дальнейшем возможно будет заинтересовать идеями экстремизма. Другим вариантом становятся социальные сети, различные форумы, в которых кураторы ведут более активную работу по вербовке последователей, они не ждут пока к ним придут, а сами иницируют обсуждение тем экстремистской направленности и тут же распространяют материалы. Последним направлением, наиболее опасным, на наш взгляд, является использование интернет-сообществ, общение в чатах. Опасность такого общения связана, прежде всего, с его скрытностью от посторонних, т. е. участниками сообществ становятся не просто случайные пользователи сети, а те, кто уже заинтересовался экстремистской деятельностью и в дальнейшем может стать полноценным членом экстремистской группировки, от обсуждения перейти к конкретным действиям.

Необходимо отметить, что если раньше представители экстремистских религиозно-политических движений и групп общались при встречах с десятками последователей, то сейчас, используя интернет-ресурсы, они получили возможность вступать в дискуссии, отстаивать свою идеологию и убеждения перед аудиторией, численность которой может достигать сотни тысяч человек. При этом данные ресурсы негативно воздействуют на молодежное сознание и не контролируются государством и обществом.

Таким образом, отдельные проявления экстремизма, сопряженные с использованием вредоносной информации, представляют реальную угрозу информационной безопасности не только общества, но и государства. Экстремистская деятельность в сети «Интернет» – проблема общегосударственного значения и угроза национальной безопасности страны. Практически во всех странах мира ведется интенсивная борьба против информационного экстремизма, именно поэтому данный вопрос является весьма актуальным и основополагающим.

В данных условиях интернет-посредники могли бы рассмотреть возможность разработки условий предоставления услуг в социальных сетях на основе консультаций с тем, чтобы обеспечить правовую и соразмерную основу для действий, особенно в отношении правительств или других третьих сторон, направленных на отслеживание, раскрытие или обмен информацией о молодых пользователях, а также на удаление контента, направленного на подстрекательство к радикализации в сторону экстремизма.

В свою очередь пользователи Интернета могли бы рассмотреть возможность:

1) активизировать усилия организаций гражданского общества по использованию социальных сетей для стимулирования формулирования и распространения мирных сообщений, альтернативных и контрнарративов, которые бросают вызов экстремистской пропаганде и разжиганию ненависти;

2) поощрять организации гражданского общества в качестве сторонников расширения прав и возможностей для борьбы с нарративами и создания сообществ, основанных на мирных ценностях и антиэкстремизме;

3) поддерживать сети онлайн и офлайн, наряду с родительским влиянием, и инвестировать в социальную структуру, которая может умерить чувство отчуждения среди молодежи;

4) поощрять грамотность, способствующую ненасильственному урегулированию конфликтов и формированию культуры мира;

5) информировать пользователей Интернета об этичном поведении в Сети, проблемах конфиденциальности и рисках, связанных с раскрытием персональных данных и другой потенциально конфиденциальной информации (через социальные сети), а также о том, как распознавать и отмечать незаконный контент/деятельность и экстремистские злоупотребления в социальных сетях.

Развитие компьютерных технологий и электронных средств массовой информации повлекло формирование единого мирового информационного пространства, которое открыло новые возможности противостоящим сторонам. Если раньше в группах экстремистской направленности применялись только техники психологического воздействия, то в настоящее время совместное использование возможностей специфики психологии человека и информационной среды дают ошеломляющий эффект.

При этом в противодействии экстремизму еще более активную роль должна играть полиция. Результативность ее работы в этом направлении зависит от правильной организации деятельности служб и подразделений, непосредственно принимающих в этом участие. Однако здесь существуют определенные сложности, связанные с квалификацией преступлений и иных правонарушений экстремистской направленности, а также с определением целевой направленности выступлений и информационных материалов.

Высокая общественная опасность правонарушений экстремистской направленности, возможность вовлечения в их совершение большого числа участников, динамизм их возникновения и развития определяют особые требования к деятельности сотрудников органов внутренних дел по их пресечению.

В заключение отметим, что противодействие экстремизму будет эффективно только при соблюдении ряда условий: обеспечение устойчивого экономического, социального, политического и культурного развития страны; правовое регулирование деятельности политических партий и организаций; решительное и своевременное противодействие незаконной деятельности экстремистских организаций; постоянный учет особенностей деятельности.

Библиографический список

1. Федеральный закон от 25 июля 2002 г. № 114-ФЗ «О противодействии экстремистской деятельности» // СПС «Гарант-Сервис» URL: <http://base.garant.ru/12127578> (режим доступа: ограниченный).
2. Указ Президента Российской Федерации от 26.07.2011 № 988 «О Межведомственной комиссии по противодействию экстремизму в Российской Федерации». // СПС «КонсультантПлюс». – URL: http://www.consultant.ru/document/cons_doc_LAW_117677. Режим доступа: ограниченный (по времени).
3. Resolution adopted by the General Assembly on 12 February 2016 on Secretary-General's Plan of Action to Prevent Violent Extremism (70/254) [электронный ресурс]. // Организация Объединенных Наций (ООН) [официальный сайт]. – URL: http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/70/254.

Тараканова Т. Э.¹,

*слушатель факультета подготовки специалистов
в области информационной безопасности
Московского университета МВД России имени В.Я. Кикотя,
младший лейтенант полиции;*

Борзунов К. К.²,

*доцент кафедры информационной безопасности
учебно-научного комплекса информационных технологий
Московского университета МВД России имени В.Я. Кикотя,
кандидат технических наук, старший научный сотрудник*

АЛГОРИТМЫ МОДЕЛИРОВАНИЯ ТЕРРОРИСТИЧЕСКОЙ АКТИВНОСТИ

Террористические атаки происходят во всех частях мира. Приоритетной задачей каждого государства стало искоренение терроризма в своей стране. Математическое моделирование – это процесс, который используется для построения модели с помощью исторических данных для прогнозирования будущего поведения. В процессе прогностического моделирования мы используем методы статистического и машинного обучения.

На современном этапе происходят внушительные изменения терроризма как социально-политического явления.

Использование моделирования поможет дать ответ на следующие вопросы:

- Когда террористы с наибольшей вероятностью нападут в следующий раз?
- Будут ли они использовать химическое, биологическое, радиологическое или ядерное оружие или прибегнут к саботажу или обычным атакам?
- На какие места и объекты они будут нацелены?

Если мы получим ответы на эти вопросы, то это позволит нам предотвратить преступление террористической направленности.

«В самом общем виде под моделированием понимается «исследование социальных явлений и процессов на их моделях, т. е. косвенная проверка, заступающей в познавательном ходу подлинник и позволяющей зарабатывать новое искусство об объекте исследования»[1].

Алгоритм построения модели террористической активности можно представить в виде следующей последовательности действий:

1. Определение целей, постановка задач моделирования и обоснование необходимости обращения к методу.
2. Абстрактная организация модельного курса, в масштабах которого проводится полный анализ терроризма как социального явления.
3. Определение устройства концептуальной модели террористической активности, где изучаются механизмы воздействия и взаимодействия структурообразующих единиц.

¹ © Тараканова Т. Э., 2020.

² © Борзунов К. К., 2020.

4. Проектирование формализованной модели, в процессе которой формируется пространство переменных, собираются данные и отображаются эмпирические объекты в некоторых формальных математических конструкциях.

5. Изучение модели и получение информации на основе анализа.

6. Переход от полученной информации в процессе моделирования к структурированным знаниям о предмете исследования, использование данных знаний в системе абстрактных познаний объекта исследования.

Модели террористических сетей могут быть большими, динамичными и характеризоваться неопределенностью. Последние два свойства, в частности, характерны не только для террористических сетей, но и для «тайных» сетей, где могут иметь место преднамеренные попытки скрыть незаконную деятельность.

Мы попробуем спроектировать математическую модель с использованием объектно-структурного моделирования, для этого рассмотрим систему, благодаря которой будет проводиться исследование и прогнозирование террористической активности.

Нам необходимо обнаружить и спрогнозировать опасные ситуации с точки зрения возможных проявлений терроризма, изучить функционирование экономических систем, политической жизни общества с целью обнаружения сбоев и ситуаций, которые могут способствовать проявлению терроризма. Осуществление моделирования стратегии и тактики вооруженной борьбы. Где осуществлялась закупка боеприпасов и оружия, где террористы планируют нападение и с какой целью?

Эта модель должна отражать отношения между всеми аспектами терроризма и выявлять корни терроризма, его современные тенденции. Должны быть определены ранние индикаторы будущих террористических действий.

Нужно проанализировать поведение отдельного объекта системы, т. е. мы рассматриваем отдельного человека (террориста), который находится в нашей системе определения террористической активности. На данном этапе моделирования мы изучаем индивидуальные особенности человека, что может произойти в жизни человека, чтоб он пошел на насильственное преступление, какой возраст у лиц, совершавших преступление террористической направленности.

Изучив отдельный объект системы, необходимо перейти к определению роли этого объекта в структуре системы, т. е. если имеет место организованная преступная группа, то какую роль играет в этой группе наш объект.

Далее при построении модели важную роль играет выявление латентных связей между объектами системы. Объекты могут находиться в различных состояниях и переходить из одних состояний в другие в результате действия различных факторов, отражающих как внешние воздействия и влияния, так и внутренние побуждения, а также влияния и воздействия со стороны связанных с ними элементов[2]. Создаются модели террористических организаций, которые позволят нам предсказывать то, какие типы действий эти организации и их агенты могут предпринять.

Таким образом, возможно осуществить анализ полученных моделей и определить различные варианты решений, проверку их, определение эффективной тактики противодействия возможным будущим актам терроризма. Количествен-

ная оценка и обоснование решения на основе потенциальных сценариев возможных проявлений терроризма будут способствовать снижению, а в будущем и отсутствию террористической активности.

Модель позволяет глубже пробраться в суть моделируемого явления, а также использовать полученные результаты для прогнозирования. Кроме этого, в таком роде модель способна быстрее обнаружить недостатки показателей, определить, при каких условиях целесообразно их применение[3].

Таким образом, решение задачи предотвращения терроризма требует нетрадиционных подходов. Но определить их можно только тогда, когда мы будем иметь модель терроризма, когда управляющие решения будут испытываться не на людях, а на моделях.

Путем математической обработки можно подтвердить возможность обнаруживать индивидуальные направленности в действии исследуемого объекта и на основе этого прогнозировать будущее направление этого поведения, помочь существенно ограничить террористические формы его проявления.

Конечная цель – предотвратить все возможные акты и проявления терроризма. Однако цель минимизации их тоже очень важна. И мы должны использовать все возможные методы моделирования для прогнозирования и предотвращения терроризма, включая методы искусственного интеллекта, которые на данном этапе применяются не в полном объеме.

Библиографический список

1. Палитай, И. С. Особенности применения метода моделирования в социологическом исследовании терроризма. автореф. дис. ... канд. социол. наук. – Москва, 2019. – 29 с.
2. Борзунов, К. К. Информационная картина преступной среды: лекция // Учебно-методическое обеспечение кафедры информационной безопасности учебно-научного комплекса информационных технологий. – 2016.
3. Овчинский, А. С. и др. Информационные технологии в органах внутренних дел : монография. – М.: Московский университет МВД России, 2010.

Жданов И. С.¹,

*слушатель факультета подготовки специалистов
в области информационной безопасности
Московского университета МВД России имени В.Я. Кикотя,
младший лейтенант полиции;*

Овчинский А. С.²,

*профессор кафедры информационной безопасности
учебно-научного комплекса информационных технологий
Московского университета МВД России имени В.Я. Кикотя,
доктор технических наук, профессор*

ИНИЦИАТИВНАЯ АНАЛИТИКА В ПРЕДУПРЕЖДЕНИИ ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ С ТЕРРОРИСТИЧЕСКИМИ УГРОЗАМИ

Терроризм – один из вариантов тактики политической борьбы с помощью насилия. Суть терроризма – насилие с целью устрашения. Терроризм проявляется в самых разных контекстах и принимает разные формы. Общие черты терроризма [4] – опасность (для жизни, здоровья или имущества); попытка намеренно подорвать демократическое правление, в частности пытаться повлиять на политических деятелей и законодателей; неизбирательный подход с целью запугивания людей.

Террористические акты являются уголовно наказуемыми деяниями, и поэтому на них распространяются правила системы уголовного правосудия. Такие правила системы уголовного правосудия применяются независимо от того, рассматривается ли конкретный инцидент как террористический акт, в отличие от любого другого серьезного преступного деяния.

Терроризм представляет реальную угрозу национальной безопасности страны: похищение людей, взятие заложников, случаи угона самолетов, взрывы бомб, акты насилия в этно-конфессиональных конфликтах, прямые угрозы их реализации и т. д. Поэтому противодействие терроризму в Российской Федерации – это одна из наиболее важных задач обеспечения безопасности на государственном уровне.

«Спящие ячейки» террористических организаций. Одна из основных тактик, используемых ИГИЛ и другими террористическими организациями, – это создание так называемых «спящих ячеек». «Спящая ячейка» – это группа людей, действующих как сторонние представители террористической организации, осуществляющие тайное планирование и подготовку к совершению террористических актов. Слово «спящий» в названии подразумевает скрытность. Они могут долгое время находиться в таком «спящем» («замороженном») состоянии, ожидая команду или призыв к активным действиям со стороны органов управления

¹ © Жданов И.С.,

² © Овчинский А.С., 2020

МТО. Координация осуществляется удаленно с использованием социальных сетей, мессенджеров, IP-телефонии и современных средств связи.

Удаленный характер управления «спящими ячейками» позволяет руководителям террористических организаций проводить синхронные атаки в разных населенных пунктах страны, тем самым усиливая устрашающее воздействие на население. С этой известной ячейкой в большинстве случаев есть информация о существовании друга. Одна из главных задач «спящих ячеек», наряду с планированием и подготовкой террористических актов, – вербовка новых членов террористических организаций, в том числе для руководства зоной боевых действий в Сирии, Ираке и Афганистане. Также их задачи заключаются в получении финансовых ресурсов и отработке навыков совершения преступных группировок, включая грабежи, вымогательство, незаконный оборот наркотиков и т. д.

Вербовочная деятельность террористических организаций. В настоящее время вербовочная деятельность террористических организаций осуществляется:

1. *В Интернете*[5]. В силу своих функций Интернет стал основной площадкой для вербовки террористических организаций. Для приема на работу в основном используются ресурсы социальных сетей (социальные сети, тематические чаты, форумы) и мессенджеры.

2. *Среди молодежи, занимающейся спортом (в спортивных секциях и секциях).* Активисты террористических организаций проявляют интерес к тем, кто занимается спортом, прежде всего, различными видами боевых искусств. Этому способствуют такие факторы, как стремление спортсменов реализовать свои лидерские качества, особый режим тренировок. Изучение биографических данных выехавших в зоны боевых действий граждан государств-участников показывает, что некоторые из них прошли физическую подготовку в различных спортивных учреждениях, а некоторые имеют спортивные достижения. При этом вербовщики террористов часто обещают спортсменам возможность применить свои навыки.

3. *Среди заключенных за преступления террористического характера.* Значительная часть осужденных за преступления террористического характера в государстве-участнике, несмотря на применение к ним мер государственного принуждения и просвещения, остаются активными приверженцами радикального ислама и вынашивают намерение продолжить свою незаконную деятельность после освобождения. Некоторые из них осуществляют вербовку среди осужденных.

4. *Среди трудовых мигрантов.* Национальная изоляция, отсутствие надлежащих материальных и социальных условий, нарушения трудовыми мигрантами миграционного и трудового законодательства, влекущие за собой их социальную дискриминацию и зависимость от своих работодателей, способствуют вербовке мигрантов в ряды террористических организаций. Среда мигрантов стала одним из основных источников вербовки новых членов в террористические организации, в том числе формирования «спящих ячеек». Эмиссары наиболее активны в социальных сетях, таких как ВКонтакте, Одноклассники, Facebook, Instagram, где происходит первоначальное общение с возможными кандидатами. Также вербовщики активно используют для общения мессендже-

ры: Viber, Whats App, Telegram и др. В последнее время вербовочная деятельность эмиссаров международных террористических организаций стала более секретной. В частности, они осторожны при общении в незнакомой аудитории, используют для модемного подключения SIM-карты телефонных операторов, зарегистрированных у третьих лиц, при вводе личных данных предоставляют ложную информацию о себе (имя, возраст, место жительства), общение на вопросы предоставления через VPN или прокси-серверы и т. д.

Противодействие терроризму. Роль правоохранительных органов и спецслужб состоит в том, чтобы в конечном итоге обеспечить безопасность граждан[2]. В отделы правоохранительных органов имеют потоки информации, которые больше, чем когда-либо прежде. Но разобраться в них для проведения расследований и правоприменения может быть чрезвычайно сложно, так же, как и предупредить данные преступные деяния на самых ранних этапах. Перед правоохранительными органами стоит сложная задача – объединить огромные объемы информации в связную историю о преступниках, бандах или даже потенциальных террористических актах.

Как говорилось ранее, терроризм представляет собой постоянную неопровержимую угрозу для общества. Для обеспечения внутренней и международной безопасности правоохранительные органы должны постоянно находиться в режиме повышенной готовности. Это включает в себя тщательный мониторинг потенциально опасных лиц, склонных к совершению террористических актов, включая их каналы связи и способы передвижения. Правоохранительные органы делают большую работу по поддержанию национальной безопасности и используют существующие технологии и инструменты, имеющиеся в их распоряжении. Во многих случаях использование реактивного интеллекта, такого как видеонаблюдение, недостаточно, поскольку он помогает только после того, как произошел инцидент. Но сотрудникам полиции необходимо не только расследовать преступления, но и предупреждать их.

Использование инициативной аналитики в противодействии терроризму при обеспечении безопасности на массовых мероприятиях. Инициативная аналитика предполагает не ждать, когда произойдет преступление, а в инициативном порядке выявлять потенциального преступника[1]. В профилактике преступлений, связанных с терроризмом и экстремизмом, основной задачей является выявление людей, которые способны совершить данные преступные деяния[3]. Выявлять потенциальных преступников мы можем по той информации, по совокупности данных, которые мы имеем об этом лице. В цифровом мире накапливается большой объем информации, из которого можно вычленять определенные данные, с конкретной вероятностью способствующие совершению террористических актов. Правоохранительные органы имеют доступ к огромным объемам данных из электронных писем, видео и файлов чатов, а также из файлов отпечатков пальцев, полицейских записей, водительских прав, реестров автомобилей и других общедоступных баз данных. С помощью этих данных и использования инициативной аналитики сотрудники правоохранительных органов могут выявить тенденции и закономерности у лиц, склонных к совершению преступлений, связанных с терроризмом.

Решение проблем, связанных с безопасностью мероприятий, должно осуществляться с учетом целостного подхода. Помимо сбора разведанных, ключевым моментом в этих усилиях будет упреждающее снижение рисков и обучение персонала мероприятий. Персоналу необходимо поддерживать максимально возможный уровень подготовки, чтобы обеспечить безопасность посетителей в кризисной ситуации.

Организаторы мероприятий должны хорошо осознавать многочисленные угрозы, проблемы и уязвимости, с которыми сталкивается их пространство для проведения мероприятий. Ситуационная осведомленность и поведенческий анализ потенциально подозрительных лиц должны быть непрерывными.

Особое внимание следует уделить: территориям, прилегающим к месту проведения мероприятия; развлекательным зонам; точкам входа/выхода; местам, ведущим к узлам общественного транспорта – такси, автобусам, вестибюлям станций метрополитена.

В этом разделе также стоит упомянуть об интеллектуальных системах видеоаналитики. Они могут быть развернуты для идентификации оружия и взрывчатых веществ, которые находятся на виду или скрыты, прежде чем злоумышленник получит возможность их использовать. Они позволяют постоянно отслеживать видимые и скрытые угрозы, тем самым снижая нагрузку на полицию и позволяя им эффективно реагировать на атаки до того, как они произойдут.

Необходима настройка автоматизированных информационно-поисковых систем и программно-аппаратных комплексов на инициативные аналитические исследования. Создание единой информационно-аналитической системы оперативно-разыскного назначения и попытки включить весь набор поисковых, идентификационных, диагностических и прогностических процедур в определенный программно-технический комплекс уже не имеют большого смысла.

Мониторинг социальных сетей. Также важен мониторинг социальных сетей. Среди публикаций в таких социальных сетях, как Facebook, Twitter, Instagram, необходимо искать потенциальные угрозы, собирая и обмениваясь разведывательными данными, анализом в реальном времени с сотрудниками правоохранительных органов и организаторами мероприятий, сотрудниками мероприятий. Правоохранительные органы должны отслеживать конкретные публикации в открытом доступе.

Например, до начала массового мероприятий нужно начинать поиск лиц, склонных совершить террористический акт.

Очень важно перейти полностью к автоматизированному сервису поисковых процедур получения каких-либо данных из сети «Интернет» или из средств массовой информации. Для этого также применяются методы компьютерной разведки, с помощью которых можно извлекать данные из «закрытых» сегментов сети «Интернет». Это требует общих усилий субъектов правоохранительных структур и служб безопасности.

Опыт обеспечения безопасности чемпионата мира по футболу в 2018 г. в полной мере показал значение инициативных аналитических исследований.

Поэтому требуется качественно улучшить состояние ресурсов оперативно-разыскной информации. Чтобы это сделать, необходимо постоянно перепровер-

рять и уточнять учетные данные, чтобы обеспечить обновление ресурсной оперативно-разыскной информации.

Такие технические средства, как средства биометрической идентификации, средства вычислительной техники и алгоритмы обработки изображений позволяют и помогают в распознавании личностей в режиме реального времени.

Важно выявлять криминально-ориентированных лиц, склонных к совершению террористических актов. Для выявления способствуют инициативная аналитика, которую применяют сотрудники правоохранительных органов, используя базы данных и системы искусственного интеллекта.

Библиографический список

1. Информационные технологии в деятельности органов внутренних дел / под ред. А. С. Овчинского. – М.: Московский университет МВД России, 2012.
2. Профилактика терроризма и экстремизма в молодежной среде / М. А. Кочубей, П. Л. Мареев, А. А. Смирнов, Е. В. Сутормина ; под общ. ред. А. П. Новикова. – СПб.: Русь, 2018. – 96 с.
3. Задачи и возможности инициативной аналитики [электронный ресурс] // StudRef – Студенческие реферативные статьи и материалы. – URL: https://studref.com/309166/pravo/zadachi_vozmozhnosti_initsiativnoy_analitiki.
4. Solaris, J. Terrorism and Events: What Event Planners Needs To Know [Соларис Дж. Терроризм и события: что нужно знать организаторам мероприятий]. // Event Manager. Now Part Of SKIFT (The Intelligence Platform To Run Better Events). – URL: <https://www.eventmanagerblog.com/terrorism-and-events>.
5. Использование Интернета в террористических целях [электронный ресурс] // Управление ООН по наркотикам и преступности. – URL: https://www.unodc.org/documents/terrorism/Publications/Use_of_Internet_for_Terrorist_Purposes/Use_of_the_internet_for_terrorist_purposes_Russian.pdf.

Анфиногенова Н. А.¹,

*курсант факультета подготовки специалистов
в области информационной безопасности
Московского университета МВД России имени В.Я. Кикотя,
рядовой полиции;*

Котов И. Д.²,

*командир отделения факультета подготовки специалистов
в области информационной безопасности
Московского университета МВД России имени В.Я. Кикотя,
младший сержант полиции;*

Пименова О. В.³,

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

ТЕХНОЛОГИЯ РАСПОЗНАВАНИЯ ЛИЦА: ПЕРСПЕКТИВА ПРИМЕНЕНИЯ В ДЕЯТЕЛЬНОСТИ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ

В повседневной деятельности сотрудников правоохранительных органов очень важно быстро и качественно получать, а также анализировать оперативно значимую информацию. Указанные преимущества сотрудникам как оперативных подразделений, так и подразделений, осуществляющих функции по охране общественного порядка, при выполнении служебных обязанностей, может предоставить использование современных специальных технологий. Существующие компьютерные технологии предоставляют возможность за короткие промежутки времени осуществлять обработку огромного объема информации. Высокую эффективность из существующих современных технологий на службе правоохранительных органов показало так называемое интеллектуальное видеонаблюдение (компьютерное зрение), использующее обработку биометрических персональных данных с применением нейронных сетей.

Применение биометрических технологий стало особенно актуальным на сегодняшний день. Системы безопасности, основанные на биометрических данных довольно разнообразны, и задействуют для идентификации человека его биологические признаки.

Активное развитие получила технология распознавания лиц, как наиболее перспективный метод биометрической бесконтактной идентификации человека по лицу. Результаты использования технологии позволяют оперативно осу-

¹ © Анфиногенова Н. А., 2020.

² © Котов И. Д., 2020.

³ © Пименова О. В., 2020.

ществлять идентификацию граждан в рамках мероприятий по охране общественного порядка и борьбе с терроризмом.

При проведении массовых мероприятий в 2019 – 2020 гг. в ходе тестирования систем компьютерного зрения в г. Москве задержано более 150 человек, находившихся в розыске. Внедрение системы интеллектуального видеонаблюдения обеспечило снижение количества преступлений, совершаемых в метро.

Цель данной работы – рассмотрение основных подходов к отслеживанию и распознаванию лиц, а также проблем и недостатков этой технологии.

Система распознавания лиц – комплексная система, позволяющая по расположению лица человека на фото- или видеоизображении осуществить идентификацию личности. Задача распознавания лица на неподвижном изображении в большинстве случаев является первым этапом в работе приложений, реализующих взаимодействие человека с компьютером. Результатом работы приложения должно стать определение наличия лица на произвольном изображении и установление его относительного размера и положения [1]. В большинстве случаев указанная система включает IP-камеру и программный продукт, анализирующий получаемое изображение с использованием сложных математических алгоритмов.

Первоначальная задача при осуществлении распознавания заключается в обеспечении локализации лица на полученном изображении. В процессе ее реализации осуществляется обработка полученного изображения по различным параметрам (яркость и др.). В дальнейшем вычисляются необходимые признаки, а затем выполняется само распознавание путем сравнения вычисленных признаков с имеющимися эталонными значениями.

В настоящее время довольно распространенным методом распознавания лиц является «elastic graph matching» – метод, основанный на «гибком» сравнении графов. Компьютерные приложения (программное обеспечение), разрабатываемые в рамках создания систем распознавания лиц, реализуют представление изображений лиц как графов. В вершинах графа рассчитываются значения признаков, чаще всего используют комплексные значения фильтров Габора. Ребра графа взвешиваются расстояниями между смежными вершинами. Разница между двумя графами рассчитывается при помощи некоторой ценовой функции деформации, учитывающей различие между значениями признаков, вычисленными в вершинах, а также степень деформации ребер графа [2].

Граф изменяется (деформируется) путем смещения каждой из его вершин на определенное расстояние в определенных направлениях относительно исходного местоположения и выбора его положения таким образом, чтобы разница между значениями признаков (откликов фильтров Габора) в вершине изменяемого графа и соответствующей вершине эталонного графа была минимизирована.

Данная операция повторяется для всех вершин графа до достижения наименьшего суммарного различия между признаками деформируемого и эталонного графов. Эта процедура называется «релаксацией» и выполняется для всех эталонных лиц, включенных в базу данных системы. Результатом распознавания системы является эталон с оптимальным значением ценовой функции деформации [2].

Главными недостатками систем, реализующих *elastic graph matching*, является их требовательность к предоставлению высоких вычислительных мощностей и низкая технологичность (при запоминании новых эталонов) и линейная зависимость времени отклика от размеров используемой базы данных лиц.

Иной подход реализует метод построения активных моделей внешнего вида – «Active Appearance Models» или ААМ. Active appearance models представляет статистическую модель изображений, которые путем различных изменений могут быть максимально приближены к реальному изображению.

Активные модели внешнего вида содержат параметры, связанные с формой, и параметры, связанные со статистической моделью пикселей изображения (текстурой). Перед использованием модель обучается на множестве предварительно размеченных изображений. Каждая метка имеет свой номер и определяет характерную точку, которую должна будет находить модель во время адаптации к новому изображению. Из всего множества нормированных точек и определяются основные компоненты. После этого, из пикселей, которые образуются точками формы, формируется матрица, каждый столбец которой содержит значения пикселей соответствующей текстуры.

Данный метод делает возможным моделирование изображения объектов, подверженных деформации. При решении задачи локализации лица на изображении выполняется поиск параметров ААМ (расположение, текстура, форма), которые представляют синтезируемое изображение, наиболее схожее с наблюдаемым. По степени сходства модели подгоняемому изображению определяется наличие на нем лица или его отсутствие.

Существует способ отслеживания, основанный на 3D-моделях. При его использовании отслеживание реализуется в виде жесткой или гибкой подгонки 3D-модели к лицу. Общий подход к отслеживанию с помощью жесткой модели заключается в оценке смещений пикселей от одного кадра к другому. Предполагаемая область движения вычисляется с помощью одного из методов оптимизации (метода наименьших квадратов и др.). Модель объекта используется только для преобразования 2D-векторов движения в 3D-движение модели объекта. Недостаток таких методов заключается в дрейфе, или так называемой «проблеме продолжительного движения». Установлено, что данные алгоритмы с течением времени накапливают ошибки и, в конечном счете, перестают должным образом реализовывать функцию отслеживания лиц [1].

Ряд систем для снижения уровня дрейфа используют ограничения, основанные на следующей модели. Взамен использования типового отслеживания системы сравнивают лицо с 3D-моделью.

Модель содержит 3D-описание лица, а также ряд параметров, необходимых для управления мимикой и изменением модели в соответствии с различными лицами. Для изменения геометрических размеров модели применяются специальные параметры, которые определяют так называемые «динамические» изменения в изображении лица (моргание веками, движения губами и т. д.) и параметры формы. На начальном этапе отслеживания происходит фиксация параметров формы, в последующем отслеживаются параметры действий.

Идентификация личности с использованием данных методов в теории может успешно применяться для выявления разыскиваемых лиц. Но на практике все эти методы имеют одни и те же недостатки. Для распознавания объекта с использованием системы видеонаблюдения в режиме реального времени требуется обеспечить максимальную независимость от форм представления.

Значительно влияет на работу систем распознавания лиц уровень освещенности. Распознавание должно осуществляться безошибочно вне зависимости от количества и яркости источников освещения. К ошибкам распознавания может приводить и положение головы в пространстве. Также при работе систем требуется обеспечить безошибочное распознавание лиц при поворотах головы вверх-вниз или влево-вправо. При необходимости идентификации человека в толпе в идеальном случае потребуется обеспечить инвариантность к поворотам головы на величину до 90°. Одновременно с этим, лицо должно быть безошибочно распознано вне зависимости от фона, который может быть как однородным, так и неоднородным. Должна обеспечиваться возможность идентификации человека с различными выражениями лица: грустным, улыбающимся и нейтральным. Качество полученного изображения лица, его частичное перекрытие влияют на эффективность любого из перечисленных методов.

С учетом изложенного определено, что основным проблемным вопросом при работе систем распознавания и идентификации лиц в режиме реального времени, является необходимость исключения зависимости качества работы системы от так называемых «внешних факторов». Учитывая значительное число существующих алгоритмов распознавания, можно сделать вывод, что до настоящего времени не удалось создать систему, способную эффективно работать вне зависимости от многочисленных ограничений, таких как расстояние до объекта или уровень шумов и освещенности. Эффективность работы систем на практике в значительной степени зависит от негативного воздействия внешних факторов и наличия вычислительных мощностей [4].

Вместе с тем, в настоящее время работа сотрудников органов правопорядка не представляется возможной без использования современных технологий, в том числе биометрических систем распознавания лиц. Эффективность современных подходов, применяемых при предупреждении и раскрытии правонарушений, свидетельствуют о необходимости дальнейшего развития данных технологий.

Библиографический список

1. Тихонова, Т. С. Основные подходы к отслеживанию и распознаванию лица / Т. С. Тихонова, Ю. С. Белов // Электронный журнал : наука, техника и образование. – 2016. – № 2. – С. 111–115.
2. Арсентьев, Д. А. Метод гибкого сравнения на графах как алгоритм распознавания образов / Д. А. Арсентьев, Т. С. Бирюкова // Вестник Московского государственного университета печати. – 2015. – № 6. – С. 74–75.
3. Махмадиева, К. Б. Сравнительный анализ алгоритмов распознавания лиц / К. Б. Мухаммадиева // Современные материалы, техника и технологии. – 2017. – № 7. – С. 58–63.

4. Юрко, И. В. Исследование основных проблем, связанных с распознаванием и идентификацией лиц по видеофиксации и совершенствование работы алгоритмов распознавания лиц по видеофиксации в режиме реального времени / И. В. Юрко, В. Н. Алдобаева // Проблемы современной науки и образования. – 2018. – № 2. – С. 66.

Суворов А. Л.¹,

курсант факультет подготовки специалистов

в области информационной безопасности

Московского университета МВД России имени В.Я. Кикотя,

сержант полиции;

Клочкова Е. Н.²,

доцент кафедры специальных информационных технологий

учебно-научного комплекса информационных технологий

Московского университета МВД России имени В.Я. Кикотя,

полковник полиции

УСТАНОВЛЕНИЕ ЛИЧНОСТИ ПОЛЬЗОВАТЕЛЯ МЕССЕНДЖЕРА TELEGRAM КАК ИНСТРУМЕНТ БОРЬБЫ С ЭКСТРЕМИСТСКОЙ ДЕЯТЕЛЬНОСТЬЮ

Интернет в 21-м веке является монополистом в формировании актуальной информации и новостной повестки дня для общества. Высокая концентрация пользователей в социальных сетях, а также низкие продажи печатных изданий свидетельствуют о том, что рынок средств массовой информации неукоснительно переходит в сетевое пространство.

Любой участник интернет-сообщества обладает возможностью по созданию новостных сюжетов и распространению собственных идей, которые будут охватывать большую аудиторию. При этом цели, которые преследуют пользователи, могут быть совершенно разными, начиная от продвижения каких-то интересных проектов, до криминальных. Свое место в интернет-пространстве заняли и различные экстремистские организации, чему способствует отсутствие цензуры, низкий порог входа в информационную среду, а также высокая скорость распространения и обработки информации отдельными пользователями.

Предупреждение и борьба с экстремистской деятельностью в информационном обществе требует как внимания со стороны правоохранительных органов, так и принятия, реализации конкретных мер по предупреждению распространения экстремистских взглядов. Острота ситуации привела к повышенному вниманию правоохранительных органов к данной проблеме, а также к ужесточению цензуры на основных цифровых площадках, результатом чего стала анонимизация личностей пользователей, которые в своих информационных сообщениях и публикациях пропагандируют оппозиционную идеологию, и их сторонников.

Рассмотрим данную проблему на примере мессенджера Telegram, который занял особое место среди цифровых площадок, позволяющих свободно и анонимно обмениваться информацией любого содержания. Политика функционирования мессенджера Telegram привлекла не только правопорядочных граждан, борющихся за анонимность в сети, но и последователей экстремистской идеоло-

¹ © Суворов А. Л., 2020.

² © Клочкова Е. Н., 2020.

гии, скрывание личности для которых является важнейшим инструментом противоправной деятельности.

В целях противодействия терроризму и экстремизму в апреле 2018 г. Роскомнадзором ограничил доступ к мессенджеру Telegram на территории Российской Федерации. Однако это привело к эффекту, обратному ожидаемому: для идеологов экстремистских взглядов данный поступок стал как бы официальным подтверждением анонимности площадки. Блокировка мессенджера не привела к отказу от его применения на территории страны, так как посредством дедиков, VPN и прокси-серверов, технологий «луковой» и «чесночной» маршрутизации использование продолжалось, только теперь анонимность даже повысилась. В июне 2020 г. ограничения были сняты.

Определение личности пользователя Telegram является одной из задач по противодействию экстремистской деятельности, стоящих перед правоохранительными органами. Даже официальное опубликование данных о такой возможности, без раскрытия содержания методик, имеет профилактическое значение.

Во многих случаях деанонимизация в Telegram может проводиться не только посредством ботов, но и с использованием фишинга и методов социальной инженерии, которые могут применяться для комплексного сбора информации о пользователе-злоумышленнике.

Рассмотрим общий принцип идентификации пользователей. Системе мессенджера для однозначной идентификации пользователя необходим специальный численный идентификатор – id. Данный атрибут не изменяется при замене аккаунтом своего username (имени пользователя). Telegram использует id для распознавания личных аккаунтов, каналов и чатов, как и протоколы остальных социальных сетей. Получение id пользователя обеспечит его идентификацию среди множества использованных имен. Creationdatebot – один из ботов, который позволяет определить id пользователя, а также дату регистрации и предыдущие используемые имена аккаунта.

Telegram, как и любой популярный интернет-ресурс, подвержен индексации - процессу получения сведений о сервисе роботом поисковой машины в базу данных, впоследствии использующуюся для полнотекстового поиска информации на сайте. В проиндексированной части Telegram есть свой поисковик, который позволяет найти не только словосочетания, но и сообщения конкретного автора, т. е. по ключевым словам найти публикации и сообщения пользователя в каналах, которые подверглись индексации.

Для распространения экстремистской идеологии группы могут создавать закрытые чаты. Если сообщество достаточно крупное, то оно может иметь отдельный чат для управления каналом. Наличие чата может иметь важное значение с точки зрения правоохранительных органов для получения информации о личности пользователя, а также деанонимизации каналов. Например, List_member_bot может показать каналы и чаты, администратором которых является конкретный пользователь.

Еще одним распространенным способом установления личности злоумышленника в социальных сетях может стать определение номера мобильного телефона – трудно представить себе человека, который бы не пользовался мобильной

связью. В Telegram, используя Deanonym_bot, можно определить имя, фамилию, номер телефона, страну, город и регион, а также операционную систему пользователя, а сервис «<https://anonymov.net/>», например, может показать номер телефона пользователя по имени аккаунта.

Известный и популярный вид интернет-мошенничества, фишинг, также может способствовать определению личности пользователя.

Например, приведенные ниже ссылки при должном представлении их обывателю, могут заставить пользователя осуществить переход по ним, а как следствие привести к получению информации о пользователе.

1. <https://wa.me/номер-приманка?text=текстсообщения!> – сообщение в WhatsApp.
2. <skype:логин-приманка?call> – звонок в skype.
3. <https://vk.com/call?id=id-приманка> – звонок через Вконтакте.

Другой аспект, на который хотелось бы обратить внимание, связан с тем, что современные социальные сети охватывают огромную аудиторию. При этом они даже имеют свои новостные каналы, как, например, рассматриваемый Telegram. Объемом аудитории заинтересовались не только коммерческие компании, которые начали вести на этих площадках свои каналы, но и преступные сообщества, экстремистские организации.

С точки зрения правоохранительных органов интерес представляют администраторы данных сообществ и каналов. Достаточно большие каналы зачастую имеют собственные одноименные чаты. Для удобства создатель и администраторы визуально помечаются знаком звездочки. Главным и самым очевидным показателем того, что аккаунт администрирует определенный канал, является ссылка на пользователя в его описании. До определенного момента (до 2017 г.) ссылки на приватные каналы в Telegram содержали закодированную информацию о том, кто его создал. Признаком таких ссылок становится отсутствие в начале ссылки аббревиатуры «AAAAA», т.е. LinkCreatorBot при определенных условиях может установить владельца канала.

Если у канала, распространяющего экстремистские взгляды, в описании есть контакт в виде электронной почты, то одним из вариантов попытки установления личности владельца может стать отправка сообщения, имеющего фишинговую ссылку.

Еще один способ деанонимизации заключается в использовании внешних «контактов». Многие Telegram-каналы используют для управления публикациями и новостными сообщениями сторонние боты и сервисы. Как следствие любые внешние ссылки, сервисы и хранилища, используемые пользователем могут, стать причиной раскрытия имени пользователя.

На данный момент, Telegram является одной из самых популярных платформ для распространения экстремистских взглядов и экстремистской деятельности. Перед правоохранительными органами, призванными защищать права и законные интересы граждан Российской Федерации в условиях информационного общества и информационного пространства, стоит задача нейтрализации данных угроз. Для ее решения необходимо, прежде всего, определиться с кем реально осуществляется эта борьба, установить его личность, независимо от того, где реально ведется противоправная деятельность.

Библиографический список

1. Деанонимизация пользователей в телеграмм группах [электронный ресурс]. // Анархический черный крест Беларусь. – URL: <https://abc-belarus.org/?p=12489>. (дата обращения: 01.12.20).
2. Козлов, А. Деанонимизация топовых каналов в Телеграме: правда и вымысел. // Российское информационное агентство federalcity.ru. – URL: <https://federalcity.ru/index.php?newsid=1849>. (дата обращения: 02.12.20).
3. «TELEGRAM» ID: зачем он нужен, и как его узнать [электронный ресурс] // Nastroyvse.ru. – URL: <https://nastroyvse.ru/programs/review/telegram-id-kak-uznat-zachem-nuzhno.html>. (дата обращения: 25.11.20).

Шарова К. М.¹,

*курсант факультета подготовки специалистов
в области информационной безопасности*

*Московского университета МВД России имени В.Я. Кикотя,
рядовой полиции;*

Клочкова Е. Н.²,

*доцент кафедры специальных информационных технологий
учебно-научного комплекса информационных технологий*

*Московского университета МВД России имени В.Я. Кикотя,
полковник полиции*

ОСНОВНЫЕ НАПРАВЛЕНИЯ ПРОТИВОДЕЙСТВИЯ КИБЕРТЕРРОРИЗМУ КАК РАЗНОВИДНОСТИ МЕЖДУНАРОДНОГО ТЕРРОРИЗМА

В настоящее время в связи с распространением и быстрым развитием информационных технологий возникло такое понятие как кибертерроризм. Зачастую он рассматривается как одна из разновидностей терроризма, при этом под ним понимается какая-либо деятельность по нарушению организации информационных систем, которая создает опасность причинения общественно опасных последствий, включая гибель и имущественный ущерб, тем самым создавая условия для различного вида катастроф и аварий техногенного характера, устрашения населения и воздействия на органы власти для выполнения последними условий, выгодных правонарушителям.

Согласно Федеральному закону от 6 марта 2006 г. № 35-ФЗ «О противодействии терроризму» терроризм определяется следующим образом: «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». [1]

Под проявлением компьютерного терроризма понимается политически мотивированная атака на информационные системы, сети и информацию, обрабатываемую в этих системах посредством угроз, принуждения к противоправным действиям, привлечения внимания к личности террориста и его организации. [2]

В современном обществе очень часто идет отождествление понятий компьютерного преступления и кибертерроризма. Важной отличительной особенностью кибертерроризма от иных преступлений, связанных с компьютерной информацией, является то, что сам преступник выносит свои условия на широкую аудиторию. Любое государство является уязвимым перед такой угрозой, причем степень серьезности этой угрозы еще не определена до конца, но точно можно сказать, что данная преступная деятельность не имеет границ, ни в том, на кого направлена атака, ни в том, откуда она может осуществляться.

¹ © Шарова К. М., 2020.

² © Клочкова Е. Н., 2020.

Обнаружение виртуального террориста почти невозможно, что само собой подразумевает и трудности с его нейтрализацией и наказанием. Кибертеррористы, путем взлома различных сайтов, могут получить информацию, которая является секретной, утечка которой может привести к необратимым последствиям. Так, из Интернета можно узнать технологии создания различного вида оружия и взрывных устройств, с сайтов органов власти, имея соответствующие навыки, можно получить доступ к различным видам схем коммуникаций, личным данным и т. д. При взломе различных баз данных в руках у преступников помимо основных персональных данных могут оказаться сведения, владение которыми может нанести ущерб и представлять непосредственную угрозу не только конкретным физическим лицам, но и целым организациям, органам власти. [3]

Отличительной особенностью кибертеррористов является то, что орудием преступления, в первую очередь выступают информационные технологии на их современном этапе развития, различное программное обеспечение, главной задачей использования которых является реализация возможности несанкционированного доступа к компьютерным системам и сетям жертв. К числу такого ПО, например, можно отнести вирусы, программные закладки, осуществляющие копирование, модификацию, уничтожение информации.

Таким образом, актуальность проблемы кибертерроризма очевидна, это, несомненно, социально опасное явление для всего мирового сообщества. Его возможности и охват возрастают с не меньшей скоростью, чем развитие и распространение непосредственно информационных технологий. В таких условиях необходимо определить основные направления противодействия кибертерроризму со стороны мирового сообщества. [4].

В первую очередь, так как кибертерроризм носит международный характер и не знает границ, таким направлением является становление, развитие и укрепление международных отношений в сфере обеспечения информационной безопасности от всевозможных угроз кибертерроризма и его проявлений между государствами, правоохрнительными органами, службами и международными организациями. Обмен знаниями и опытом в борьбе с кибертеррористами и отражении их атак, методами и практиками мониторинга информационных ресурсов, проведения экспертиз мог бы также существенно оказать влияние на положение дел в данной области. При этом необходимо отметить, что немаловажное значение имеет наличие контакта между странами по обмену информацией об угрозах, признаках, фактах совершения компьютерных атак и средствах использования информационных систем в противоправных целях кибертеррористов. Помогло бы принятие международных законов об информационной безопасности и борьбе с кибертерроризмом, разъяснение политики государств и мировых сообществ по борьбе с терроризмом, а также недопустимость двойных стандартов по данному вопросу.

В качестве методов противодействия можно рассматривать повышение эффективности сотрудничества государственных органов и структур, занимающихся вопросами противодействия терроризму и обеспечением информационной безопасности; деятельность по принятию мер предупреждающего характера для зарождения у людей негативного отношения к терроризму в целом, к приме-

нению насильственных средств для осуществления преступных замыслов; привлечение к уголовной ответственности лиц, распространяющих террористические взгляды и идеи, а также самих злоумышленников и иных лиц, причастных к кибертерроризму.

Возраст пользователей Интернета значительно варьируется, сейчас даже ребенок может спокойно включить компьютер и зайти в сеть. Поэтому важно помимо основной защиты устройства с помощью программных средств от несанкционированного доступа и иных противоправных операций, проводить организационные мероприятия непосредственно с легальными пользователями информационных систем, предупреждая тем самым возможность кибератак. В этом могут помочь курсы по компьютерной грамотности, поведению в сети Интернет, о том, какие последствия могут быть от манипуляций кибертеррористов. При приеме на работу, чтобы не допустить утечки важной информации, которая может послужить орудием для компьютерных террористов, важно знать уровень компьютерной грамотности, основ безопасности информационных сетей и систем, и при необходимости предоставить работникам возможность обучения.

Помимо организационных мер на местах, где есть угроза неправомерного воздействия кибертеррористов, следует с целью обеспечения информационной безопасности устройств использовать разнообразные технические средства защиты (программные, аппаратные и программно-аппаратные комплексы); криптографические средства, обеспечивающие шифрование информации и механизмы проверки подлинности; антивирусные мониторы, фильтры, сканеры; средства, обеспечивающие отказоустойчивость и резервное копирование; межсетевые экраны и шлюзы.

В отношении юных пользователей (дома или в школе) часто применяют контент-фильтры для закрытия доступа к нежелательным и сомнительным интернет-ресурсам. Такой же фильтр можно применять и в организациях, где помимо защиты от опасного контента, повысится и работоспособность, если ограничить доступ еще и к развлекательным ресурсам. Еще одна проблема связана со спам-рассылками. Фишинговые письма могут привести к несанкционированному доступу кибертеррористов к системе, когда пользователь просто переходит по незнакомой ссылке. В данном случае защитой может стать только запрет на переход по ссылкам, инструктаж и обучение пользователей, а также выработка внимательного и скептического отношения к рассылкам.

В целом, важно наличие человека или целого отдела, отвечающего за безопасность информационной системы, использующейся в организации для качественного проведения мониторинга систем, для разрешения вопросов, возникающих при использовании коммуникационных сетей, для установки фильтров на нежелательные ресурсы, организация помощи и оперативное принятие решений в экстренных ситуациях, связанных с несанкционированным доступом и возможностью у злоумышленников воспользоваться «слитыми» данными в корыстных, террористических целях.

Для противоборства с кибертерроризмом создаются специальные методы, средства и системы киберобороны (cyberdefence, cyber defense, CD, cyber defense system) как проактивные (proactive cyberdefence), так и активные (active

cyberdefence, ACD). Это превентивные меры, направленные на предупреждение и противодействие возможным вредоносным атакам на компьютеры и компьютерные сети государства или организации, на снижение уровня операционных рисков, а также на минимизацию ущерба и времени восстановления в случае состоявшихся кибератак.

Организация борьбы с кибертерроризмом требует многогранного и комплексного подхода, предпринятия совместных действий и решений. Рост угрозы кибертерроризма требует принятия как технических, так и законодательных мер для борьбы за безопасность при работе с информацией. Соблюдение мер информационной безопасности поможет в противостоянии кибертеррористам, поскольку их методы схожи с применяемыми методами киберпреступников.

Библиографический список

1. Федеральный закон от 6 марта 2006 г. № 35-ФЗ «О противодействии терроризму». // СПС «КонсультантПлюс». – URL: http://www.consultant.ru/document/cons_doc_LAW_58840.
2. Методы, виды террористической деятельности и тенденции развития современного терроризма [электронный ресурс] // Портал органов государственной власти Ярославской области. – URL: https://www.yarregion.ru/Pages/terrorism_vid.aspx (дата обращения: 07.12.2020).
3. Журавель, В. «Противодействие угрозе кибертерроризма» / В. Журавель // Fact Military. – URL: http://factmil.com/publ/soderzhanie/informacionnye_vojny/protivodejstvie_ugroze_kiberterrorizma_2018/107-1-0-1346. (дата обращения: 08.12.2020).
4. Голубев, В. Кибертерроризм как новая форма терроризма [электронный ресурс] / В. Голубев // Центр исследования проблем компьютерной преступности. – URL: http://www.crime-research.ru/library/Gol_tem3.htm. (дата обращения: 07.12.2020).