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 материалов
Всероссийской научно-практической конференции
«Противодействие экстремизму и терроризму
в информационных системах»
3 декабря 2019 г.**

Московский университет МВД России
имени В.Я. Кикотя, 2019

ISBN 978-5-9694-0825-8

Москва
2019

ББК 67.408
П83

Рецензенты:
начальник кафедры информационно-компьютерных технологий в деятельности органов внутренних дел Белгородского юридического института МВД России имени И.Д. Путилина кандидат технических наук, доцент **Прокопенко А. Н.**;
профессор кафедры информационной безопасности Краснодарского университета МВД России доктор технических наук, профессор **Еськов А. В.**

П83 **Противодействие терроризму и экстремизму в информационных системах** : сборник научных трудов Всероссийской научно-практической конференции «Противодействие экстремизму и терроризму в информационных системах» 3 декабря 2019 г. – М. : Московский университет МВД России имени В.Я. Кикотя, 2019. – 58 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 978-5-9694-0825-8

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 3 декабря 2019 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, 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. Предназначены для научных и практических работников, участвующих в борьбе с преступностью.

ББК 67.408

ISBN 978-5-9694-0825-8

Научное электронное издание

Компьютерная верстка *Фомин И. Е.*
3,27 усл. печ. л.
Московский университет МВД России имени В.Я. Кикотя
117997, г. Москва, ул. Академика Волгина, д. 12
http: //www.mosu.mvd.ru, e-mail: support_mosu@mvd.ru

СОДЕРЖАНИЕ

Д. С. Богданов, К. Ю. Бардин
Средства выявления информации экстремистской направленности в сети Интернет 4

А. Г. Большунов
Проблемы расследования и предупреждения преступлений экстремисткой направленности в сети Интернет 7

В. Б. Боровиков, В. В. Боровикова
О некоторых аспектах уголовно-правового противодействия проявлениям экстремистской и террористической деятельности с использованием информационных технологий 9

В. В. Гончар
Отдельные направления совершенствования расследования киберпреступлений 13

Н. Н. Гусев
Статистическая зависимость как элемент борьбы с экстремизмом и терроризмом 17

В. М. Данилкина
Профилактические действия в социальных сетях как мера борьбы с киберпреступностью 23

П. Н. Жукова, Н. В. Золотухина, В. А. Насонова
Предупреждение распространения экстремизма в сети Интернет 26

В. Ю. Иванов, А. В. Пузарин
Роль информационных технологий современного терроризма и экстремизма 32

Ю. С. Лунёв, М. Е. Панкратова, А. А. Толстых
О возможности автоматической классификации текстов экстремистской направленности 37

Д. А. Мозговая
Информационный экстремизм в современных условиях 40

Т. В. Молчанова
Проблемы информационных ресурсов в оценке организованной преступности в сфере экономической деятельности 42

А. И. Мысина
Международно-правовое регулирование противодействия финансированию терроризма с использованием информационных технологий 46

А. С. Овчинский
Приоритетные направления противодействия экстремизму и терроризму 50

А. В. Серезевский
К вопросу о запрете признания экстремистскими материалами текстов Библии, Корана, Танаха (священное писание иудаизма) и Ганджура (буддийский канон) 56

Богданов Дмитрий Сергеевич[1]**,**
преподаватель кафедры информационной безопасности
Краснодарского университета МВД России

Бардин Кирилл Юрьевич[2]**,**
курсант 6116 учебного взвода
Краснодарского университета МВД России

СРЕДСТВА ВЫЯВЛЕНИЯ ИНФОРМАЦИИ ЭКСТРЕМИСТСКОЙ НАПРАВЛЕННОСТИ В СЕТИ ИНТЕРНЕТ

В XXI в. цифровых технологий и сверхмощных вычислительных систем в процессе повседневной деятельности человеку свойственно забывать о банальных вещах, в частности, о своей безопасности. Личная безопасность каждого гражданина и общества в целом, целостность государственного и конституционного строя – это ключевые сферы, обеспечение безопасности которых является приоритетной задачей для правительств каждой страны. Экстремизм – главная угроза безопасности современного общества, а Интернет является крупнейшей площадкой для пропаганды и привлечения новых людей к идеям и взглядам экстремистских организаций. На данный момент главным объектом воздействия организаций экстремистской направленности и их сторонников выступает подрастающее поколение. Дети и подростки, которые непрерывно изучают окружающий мир, в том числе и в сети Интернет, которая бесспорно оказывает большое влияние на их формирование, как граждан и социальных личностей. Само собой, это не говорит о том, что взрослый, уже сформировавшийся гражданин, который живет самостоятельной жизнью, не может быть подвержен воздействию экстремистской пропаганды. Известно, что пропагандой, агитацией и вовлечением других людей занимаются подготовленные люди, которые владеют и умело применяют средства воздействия на человеческое сознание, обладают отточенными навыками практической психологии и знают, как вызвать у человека интерес к экстремистской деятельности и в дальнейшем его поддержать.

Цели экстремизма в сети Интернет выражаются в привлечении на «свою сторону» как можно большего количества людей средствами антиправительственной агитации или поддержанием интересов подрастающей молодежи, объединение их в группы и управление их волей. Жертвы подобной пропаганды даже не понимают, что действуют против своей воли и находятся под влиянием других людей, которых не интересуют средства достижения поставленных целей. Самым ярким примером подобных групп лиц могут выступать «Скинхеды», действующие в 1990-е гг. в России, объединенные одной идеей, пропаганды «белой расы» они помимо этого занимались и другой преступной деятельностью, никак не связанной с их идеей. В данной статье будут рассмотрены актуальные средства выявления информации экстремисткой направленности в сети Интернет, позволяющие своевременно выявлять факты

[1] Богданов Д. С., 2019.
[2] Бардин К. Ю., 2019.

распространения таких материалов с целью их последующего блокирования и ограничения распространения в социальных сетях, всевозможных современных молодежных форумах и прочих ресурсах глобальной сети [1]. В соответствии с Федеральным законом от 25 июля 2002 г. № 114-ФЗ «О противодействии экстремистской деятельности» экстремистские материалы – это предназначенные для обнародования документы либо информация на иных носителях, призывающие к осуществлению экстремистской деятельности либо обосновывающие или оправдывающие необходимость осуществления такой деятельности [3].

Одним из эффективных средств разведки в сети Интернет является специальное программное обеспечение *Maltego*, которое содержит в себе большое количество инструментов для социальной разведки. Данное программное обеспечение предназначено для сбора информации из различных интернет ресурсов, в частности, источником информации являются открытые базы данных [2]. Встроенные в программу алгоритмы интеллектуального анализа данных позволяют выстраивать связи между:

– людьми (группами людей), их контактами (электронная почта, аккаунты в социальных сетях, телефонные номера, адреса);
– компаниями;
– веб-сайтами;
– элементами интернет-инфраструктуры (доменные имена, DNS-записи, IP-адреса, сетевые блоки);
– документами;
– фразами, надписями.

Программа реализована на языке программирования *Java*, что позволяет работать с ней на любой операционной системе, с предустановленным пакетом расширений *Java*.

Эффективным инструментом анализа документарной информации является программное обеспечение «Доктор Ватсон». Данное приложение позволяет обрабатывать и структурировать объемные текстовые массивы, что может оказать неоценимую помощь сотрудникам ОВД в выделении экстремистских материалов из большого объема данных. Программное обеспечение проводит анализ исследуемого текста и затем выстраивает связи, которые сумела распознать в данном массиве встроенная нейросетевая модель. Программа очень легка в использовании и позволяет после проведенного анализа самостоятельно внести изменения, указать связи, которые не распознала программа. После проведенного анализа с учетом внесенных изменений программное обеспечение подготавливает развернутый отчет.

Наряду с программным обеспечением «Доктор Ватсон», функционал которого ограничен анализом текстовых массивов, которые пользователь сам вносит в программу, существуют web-анализаторы, которые автоматизируют сбор информации с различных веб-сайтов для формирования целостного массива документарной информации, который пользователь в последующем подвергает обработке и структурированию. Программное обеспечение позволяет пользователю самостоятельно задавать критерии и источник поиска, кроме того, суще-

ствует возможность экспортировать все собранные данные в *CSV* или текстовый файл, а также поместить в заданный формат базы данных.

За исключением программного обеспечения, к средствам поиска экстремистских материалов в сети Интернет можно отнести специальные Web-ресурсы, предназначенные для профессионального поиска, мониторинга, сбора и анализа информации. Одним из наиболее эффективных приложений подобного рода является сервис *sitesputnik*. Пользователь указывает адреса источников и правила сбора информации, затем приложение очищает все собранные сведения от информации, не относящейся к искомой, и формирует рубрики, которые содержат сведения требуемой тематики. Программное обеспечение также включает в себя функцию мониторинга истории поиска, при повторном поиске информации, приложение будет предоставлять только новые ссылки на ресурсы сети Интернет, которые не встречались раннее.

Еще одним программным решением, которое может быть использовано правоохранительными органами для поиска экстремистских материалов может быть *WebSite-Watcher*. Данное программное обеспечение позволяет проводить мониторинг веб-страниц, включая защищенные паролем, мониторинг форумов, RSS-каналов, новостных групп и локальных файлов. Обладает мощной системой фильтров. Мониторинг ведется автоматически и поставляется в удобном для пользователя виде. Позволяет проводить контроль, по ключевым словам, в случае изменений (появления новых сообщений, изменении структуры web-сайта) и оповещает пользователя в случае изменений одного из наблюдаемых параметров.

На сегодняшний день существует огромное количество сервисов и программных решений, позволяющих пользователю эффективно получать и обрабатывать информацию. Стоит отметить, что немалая доля подобных решений распространяется на бесплатной основе и не требует денежных вложений, что существенно упрощает процедуру добывания требуемой информации. В данной статье были перечислены наиболее популярные средства, которые достаточно эффективно могут быть использованы сотрудниками правоохранительных органов для поиска и последующей обработки информации в открытых источниках с целью выявления материалов экстремистской направленности.

Список литературы

1. Социальная разведка: Используем соцсети для сбора данных [Электронный ресурс] // URL: https://xakep.ru/2015/06/23/social-networks-197 (дата обращения: 20.11.2019).

2. Data at your fingertips [Электронный ресурс] // URL: https://www.maltego.com/transform-hub (дата обращения: 22.11.2019).

3. О противодействии экстремистской деятельности: Федеральный закон от 25 июля 2002 г. № 114-ФЗ [Электронный ресурс] // URL: http://garant.ru.

Большунов Александр Геннадьевич[1]**,**
преподаватель кафедры
специальных информационных технологий УНК ИТ
Московского университета МВД России им. В.Я. Кикотя

ПРОБЛЕМЫ РАССЛЕДОВАНИЯ И ПРЕДУПРЕЖДЕНИЯ ПРЕСТУПЛЕНИЙ ЭКСТРЕМИСТКОЙ НАПРАВЛЕНОСТИ В СЕТИ ИНТЕРНЕТ

На сегодняшний день, несмотря на принимаемые меры с стороны правоохранительных органов, количество преступлений экстремисткой направленности возрастает. Основной проблемой при расследовании этого рода преступлений является среда распространения экстремистских материалов в современном мире, одним из главных источников распространения экстремистских идей является сеть Интернет. В соответствии с положениями Конституции, Российская Федерация является многонациональной страной, народы которой исповедуют различные религии, в свете чего экстремизм во всех его формах и проявлениях становится фактором, угрожающим целостности и единству государства.

Статистика, свидетельствующая о неуклонном росте преступлений экстремистской направленности показывает что, в 2018 г. были зарегистрированы 1 265 преступлений экстремисткой направленности[2], что на 16,8 % меньше, чем в 2017 г. (всего в 2017 г. выявлено 1 521 преступление рассматриваемой направленности)[3]. Несколько меньше преступлений экстремисткой направленности было зарегистрировано в 2016 г. – 1 450 преступлений[4], в 2015 г. – 1 329[5], в 2014 г. – 1 034[6].

Интерес представляет определение проявлений экстремизма (экстремистских проявлений), установленных в Стратегия противодействия экстремизму в Российской Федерации до 2025 г., утвержденной Президентом Российской Федерации «общественно опасные и противоправные деяния, совершаемые по мотивам политической, идеологической, расовой, национальной или религиозной ненависти или вражды, а также деяния, способствующие возникновению

---

[1] © Большунов А. Г., 2019.

[2] Состояние преступности в России за январь – декабрь 2018 года / ФКУ «Главный информационно-аналитический центр» МВД России [Электронный ресурс] // URL: https://media.mvd.ru/files/application/1518099 (дата обращения: 15.10.2019).

[3] Состояние преступности в России за январь – декабрь 2017 года / ФКУ «Главный информационно-аналитический центр» МВД России [Электронный ресурс] // URL: https://media.mvd.ru/files/application/1241295 (дата обращения: 15.10.2019).

[4] Состояние преступности в России за январь – декабрь 2016 года / ФКУ «Главный информационно-аналитический центр» МВД России [Электронный ресурс] // URL: https://xn--b1aew.xn--p1ai/upload/site1/document_news/009/338/947/sb_1612.pdf (дата обращения: 15.10.2019).

[5] Состояние преступности в России за январь – декабрь 2015 года / ФКУ «Главный информационно-аналитический центр» МВД России [Электронный ресурс] // URL: https://xn--b1aew.xn--p1ai/upload/site1/document_file/sb_1512.pdf (дата обращения: 15.10.2019).

[6] Состояние преступности в России за январь – декабрь 2014 года / ФКУ «Главный информационно-аналитический центр» МВД России [Электронный ресурс] // URL: https://xn--b1aew.xn--p1ai/upload/site1/document_file/pxOrdPt4BF.pdf (дата обращения: 15.10.2019).

или обострению межнациональных, межконфессиональных и региональных конфликтов»[1].

Уголовное законодательство устанавливает ответственность за возбуждение ненависти либо вражды, а равно унижение человеческого достоинства (ст. 282 УК РФ), организацию экстремистского сообщества (ст. 282.1 УК РФ), организацию деятельности экстремисткой организации (ст. 282.2 УК РФ), финансирование экстремисткой деятельности (ст. 282.3 УК РФ).

Для правильной квалификации действий, направленных на возбуждение ненависти либо вражды, а также на унижение достоинства совершенных с помощью сети Интернет, необходимо понимать, для достоверного установления такого деяния необходимо наличие следующих признаков:

– первый признак – это информация, которая распространена в сети Интернет и содержит по своему смыслу унижение человека, а так же возбуждающая ненависть по признакам расы, национальности и т. д.;

– второй признак – доступность информации в открытом пространстве сети «Интернет» для других пользователей;

– третий признак относится к субъективной стороне преступления – это цель, унижение человека, а также возбуждение ненависти по признакам расы, национальности и т. д.

Основной средой распространение материалов в сети Интернет являются социальные сети, пользователем которых может стать любой человек, имеющий доступ в интернет. Аккаунты, зарегистрированные в социальных сетях, не позволяют идентифицировать этого пользователя из общей массы пользователей сети Интернет. При регистрации аккаунта возможно введение недостоверных анкетных данных, и при их отсутствии не всегда удается установить личность данного пользователя. Пользователь может объединять других пользователей в группы по интересам для удобства общения и передачи информации определенному сообществу пользователей. Становясь в результате создания таких групп организатором с функциями управления группами и различного рода администрирования, например, управление содержимым своего профиля, наполнением контента своей странички (текстовые документы, фото- или видеоматериалы, ссылки на другие интернет ресурсы). В качестве наиболее популярных социальных сетей можно указать: *Facebook, Twitter*, «ВКонтакте», «Одноклассники», *YouTube, Instagram.*

Активность пользователей можно распределить следующим образом, для получения необходимой информации и ее дальнейшего анализа или экспертизы. Анонимность пользователей с помощью использования браузера *TOR, VPN* – сервисов, или proxy, не позволяют в полной мере проводить разыскные мероприятия. Использование мессенджера *Telegram*, вызывает ряд сложностей при идентификации пользователей и выявлении каналов распространения экстремистских материалов. Хотя с помощью имеющихся баз данных, это представляется возможным, но не всегда.

---

[1] Стратегия противодействия экстремизму в Российской Федерации до 2025 года (утв. Президентом Российской Федерации от 28 ноября 2014 г. № Пр-2753) (документ опубликован не был) [Электронный ресурс] // Система ГАРАНТ. – URL: http://garant.ru (дата обращения: 02.11.2019).

Боровиков Валерий Борисович[1],
профессор кафедры уголовного права
Московского университета МВД России имени В.Я. Кикотя,
заслуженный сотрудник органов внутренних дел Российской Федерации,
кандидат юридических наук, доцент

Боровикова Виктория Валерьевна[2],
доцент кафедры уголовного права
Московского университета МВД России имени В.Я. Кикотя,
кандидат юридических наук, доцент

О НЕКОТОРЫХ АСПЕКТАХ УГОЛОВНО-ПРАВОВОГО ПРОТИВОДЕЙСТВИЯ ПРОЯВЛЕНИЯМ ЭКСТРЕМИСТСКОЙ И ТЕРРОРИСТИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Активное использование информационных технологий – закономерное явление в деятельности экстремистских и террористических объединений в современных условиях развития цивилизации. Дело в том, что они позволяют значительно облегчить совершение преступлений этой направленности (например, применять данные технологии для вербовки участников подобных объединений, подстрекательства к совершению ими преступлений, своевременного оповещения об опасности задержания правоохранительными органами, обеспечения конспиративности функционирования данных незаконных структур и т. д.).

Поэтому уголовно-правовая политика в сфере борьбы с указанными деяниями должна учитывать данные обстоятельства и своевременно на них реагировать на уроне законотворчества и правоприменения[3].

Отражает ли действующее уголовное законодательство Российской Федерации названные выше вызовы современности? В определенной мере можно дать положительный ответ на данный вопрос. В УК РФ сейчас немало норм, где использование информационных технологий выступает в качестве признаков основного и квалифицированного составов преступлений (см., например, п. «д» ч. 2 ст. 110, п. «д» ч. 3 ст. 110.1, ч. 2 ст. 110.2, ч. 2 ст. 128.1, чч. 1 и 3 ст. 137, п. «в» ч. 2 ст. 151.2, ст.ст. 159.3, 159.6, 171.2, ч. 2 ст. 205.2, п. «б» ч. 2 ст. 228.1, п. «б» ч. 2 ст. 258.1, ст.ст. 272–274.1 УК РФ)[4].

---

[1] © Боровиков В. Б., 2019.

[2] © Боровикова В. В., 2019.

[3] Об актуальности данного направления уголовно-правовой политики свидетельствуют такие цифры: в 2018 г. в Российской Федерации были зарегистрированы 174 тыс. преступлений, совершенных с помощью IT-технологий (Петров И. Систематические угрозы // РГ. – 2019. – 6 февр.).

[4] Необходимо отметить, что для обозначения факта использования информационных технологий при совершении преступлений, законодатель использует различную терминологию: «в средствах массовой информации или информационно-телекоммуникационных сетях (включая сеть Интернет)» – ч. 1 ст. 171.2 УК РФ; п. «б» ч.2 ст.228.1 УК РФ; «в средствах массовой информации или информационно-телекоммуникационных сетях» – ч. 3 ст. 137 УК РФ; «с использованием средств массовой информации либо электронных или информационно-телекоммуникационных сетей (включая сеть «Интернет») – ч. 2 ст. 280 УК РФ. Думается, законодателю целесообразно использовать при описании подобных признаков

Определенное отражение использования информационных технологий нашло и в нормах об ответственности за террористическую и экстремистскую деятельность. В гл. 24 УК РФ (Преступления против общественной безопасности) есть ч. 2 ст. 205.2, устанавливающая повышенную ответственность за публичные призывы к осуществлению террористической деятельности, публичное оправдание терроризму, совершенные с использованием средств массовой информации либо электронных или информационно-телекоммуникационных сетей, в т. ч. сети Интернет. В гл. 29 УК РФ (Преступления против основ конституционного строя и безопасности государства) предусмотрена также более строгая ответственность за подобные призывы к осуществлению экстремистской деятельности, совершенные с использованием СМИ либо информационно-телекоммуникационных сетей, в т. ч. сети «Интернет» (ч. 2 ст. 280 УК РФ), а равно за публичные призывы к осуществлению действий, направленных на нарушение территориальной целостности Российской Федерации с использованием подобных информационных технологий (ч. 2 ст. 280.1 УК РФ). Кроме того, ст. 282 УК РФ устанавливает более строгую ответственность за возбуждение ненависти либо вражды, а равно унижение человеческого достоинства, совершенные публично, в т. ч. с использованием средств массовой информации или информационно-телекоммуникационных сетей, включая сеть Интернет.

Представляется, имеются резервы, связанные с отражением названного выше признака состава преступления и в других нормах об ответственности за рассматриваемые формы преступной деятельности.

Так, на наш взгляд, законодатель недооценил общественную опасность угрозы террористического акта с использованием информационных технологий (сейчас такое деяние оценивается на основании ч. 1 ст. 205 УК РФ). В подобных ситуациях, даже если угроза окажется ложной, не только вынужденно должны реагировать соответствующие силовые структуры, привлекая для этого большие силы и средства, но имеет место и мощное воздействие на сознание многих людей, по- разному реагирующих на такие проявления психического насилия. В частности, часть населения может быть подвержена панике, что отражается и на производительности организации труда, распространении всевозможных слухов, отрицательных оценок деятельности органов власти, в т. ч. правоохранительных органов. Обстановка страха среди населения влияет и на поведение представителей преступного мира, которые, учитывая отвлечение сил правоохранительных органов на пресечение деятельности, угрожающего террориста, могут активизировать реализацию своих намерений на совершение различных преступлений.

Следовательно, включение в ст. 205 УК РФ указания на использование информационных технологий при угрозе террористического акта позволило бы более адекватно оценить общественную опасность данного деяния[1].

составов преступлений единообразную терминологию – может быть, в виде – «использования информационных технологий».

[1] Представляется, что законодатель в целях дифференциации ответственности за террористический акт мог бы предусмотреть самостоятельную ответственность за угрозу этого

Аналогичные негативные последствия возникают при заведомо ложном сообщении об акте терроризма (ст. 207 УК РФ). Использование при совершении этого преступления информационных технологий увеличивает деструктивные возможности данного деяния, что и обусловливает целесообразность введения рассматриваемого квалифицирующего признака состава преступления в ст. 207 УК РФ (в случае положительного решения данной ситуации, можно было включить в эту статью, например, ч. 3.1, которая содержала бы повышенную ответственность за заведомо ложное сообщение об акте терроризма с использованием информационных технологий).

Представляется, что определенную модификацию могла претерпеть и редакция ст. 205.1 УК РФ (Содействие террористической деятельности). На наш взгляд, нет каких-либо серьезных возражений после утверждения, что склонение, вербовка или иное вовлечение лица в совершение преступлений террористической направленности (чч.1–2 ст. 205.1 УК РФ) приобретает качественно иной характер, если виновное лицо использует для достижения своих целей информационные технологии (как минимум, появляются возможности по вовлечению в ряды террористов большего числа людей). В этой связи будет уместным дополнить ч. 2 ст. 205.1 УК РФ указанием не только на использование лицом своего служебного положения, но и информационных технологий.

По нашему мнению, использование информационных технологий повышает общественную опасность и деяний, которые могут создать условия для террористической и экстремистской деятельности. Например, это имеет место при незаконном обороте оружия, взрывчатых веществ или взрывных устройств (ст.ст. 222–222.1 УК РФ), в частности, при сбыте этих предметов. Несомненно, передача информации через Интернет с предложением об их продаже расширяет во много раз и число потенциальных покупателей, приобретателей, способствует бесконтрольному распространению оружия, взрывчатых веществ или взрывных устройств в преступной среде. Поэтому и установление повышенной ответственности не выглядит каким-то завышенным требованием, предъявляемым обществом к законодателю. В качестве образца можно взять на вооружение опыт законодателя в отношении регулирования ответственности за сбыт наркотических средств, психотропных веществ или их аналогов. Так, согласно п. «б» ч. 2 ст. 228.1 УК РФ предусмотрена достаточно строгая ответственность (наказание в виде лишения свободы от 5 до 12 лет со штрафом в размере до 500 тыс. рублей или в размере заработной платы или иного дохода осужденного за период до 3 лет либо без такового и с ограничением свободы на срок до 1 года либо без такового) за сбыт указанных выше предметов с использованием средств массовой информации либо электронных или информационно-телекоммуникационных сетей, включая сеть Интернет. Аналогичные по конструкции уголовно-правовые запреты могли бы содержаться в ст.ст. 222–222.1 УК РФ.

преступления, выведя упоминание о ней из ч. 1 ст. 205 УК РФ. Это позволило бы дать более точную юридическую оценку содеянного, так как после внесения изменений в Федеральный закон Российской Федерации от 31 декабря 2017 г. № 501-ФЗ «Об уполномоченных по правам ребенка», цели террористического акта несколько отличаются от целей угрозы его совершения.

В последние годы за рубежом и в нашей стране все большее внимание привлекают массовые беспорядки – преступление против общественной безопасности и общественного порядка, нередко совершаемые из экстремистских побуждений. Анализ содержания уголовно-правовых запретов, предусмотренных ст. 212 УК РФ показывает, что и здесь существует потребность, связанная с необходимостью отразить в диспозициях ряда норм признак использования информационных технологий при совершении этого преступления. В частности, это касается таких форм названного преступления как склонение, вербовка или иное вовлечение лица в совершение действий, предусмотренных в ч. 1 ст. 212 УК РФ (ч. 1.1) и призывы к массовым беспорядкам, предусмотренным ч.1 этой статьи, а равно призывы к насилию над гражданами (ч. 3 ст. 212 УК РФ).

Гончар Владимир Владимирович[1]**,**
заместитель начальника кафедры информационной безопасности УНК ИТ Московского университета МВД России имени В.Я. Кикотя,
кандидат юридических наук

ОТДЕЛЬНЫЕ НАПРАВЛЕНИЯ СОВЕРШЕНСТВОВАНИЯ РАССЛЕДОВАНИЯ КИБЕРПРЕСТУПЛЕНИЙ

Последние годы принимается значительное количество нормативно-правовых актов, регламентирующих общественные отношения в сфере информационных технологий, что обусловлено нарастающей информатизацией различных сфер деятельности государства и общества. 10 октября 2019 г. подписан Указ Президента Российской Федерации № 490 «О развитии искусственного интеллекта в Российской Федерации», утверждена «Национальная стратегия развития искусственного интеллекта на период до 2030 года»[2]. Одновременно фиксируется значительное увеличение количества зарегистрированных преступлений, совершенных в сфере телекоммуникаций и компьютерной информации [1, с. 92].

Так в 2018 г. были зарегистрированы 174 674 подобных преступления (на 92,8 % больше АППГ – 90 587 в 2017 г.). За 9 месяцев 2019 г. зарегистрированы уже 205 116 преступлений (на 69,2 % больше АППГ). Таким образом, за последние три года количество зарегистрированных преступлений рассматриваемой категории увеличилось более чем в два раза. По итогам 9 месяцев 2019 г. раскрываемость составила всего 27,1 %.[3] Исходя из того, что не все раскрытые преступления будут окончены расследованием и не по всем расследованным преступлениям будут вынесены обвинительные приговора, ситуацию в данной сфере можно мягко назвать «тревожной». Низкий уровень раскрываемости данных преступлений отметил 28 февраля 2018 г., Президент Российской Федерации В. В. Путин, выступая на расширенном заседании коллегии МВД России[4].

1 декабря 2016 г. В. В. Путин в послании Федеральному Собранию Российской Федерации определил следующее: «Необходимо укреплять защиту от киберугроз, должна быть значительно повышена устойчивость всех элементов инфраструктуры, финансовой системы, государственного управления. Предлагаю запустить масштабную системную программу развития экономики нового технологического поколения, так называемой цифровой экономики. В ее реализации будем опираться именно на российские компании, научные, исследовательские и инжиниринговые центры страны. **Это вопрос** национальной

---

[1] © Гончар В. В., 2019.

[2] URL: http://www.pravo.gov.ru/laws/ (дата обращения 31.10.2019).

[3] URL: https://xn--b1aew.xn--p1ai/Deljatelnost/statistics (дата обращения: 21.10.2019).

[4] Информация о расширенном заседании коллегии МВД России // URL: http://kremlin.ru/events/president/news/56949 (дата обращения: 28.02.2019).

безопасности и технологической независимости России, в полном смысле этого слова – **нашего будущего** (выделено автором – В. Г.)»[1].

Поставленные Президентом России вопросы не только актуальны, но и достаточно сложны, поскольку существующая ситуация свидетельствует о значительных изъянах в системе защиты населения и государственных институтов от киберугроз [2, с. 131]. Криминально ориентированные лица все более активно осваивают новые технологии и наращивают криминальную активность в виртуальном пространстве, в том числе в его экономическом сегменте. Об этом, в частности, сообщил, Председатель Правления ПАО «Сбербанк России» Г. О. Греф по данным которого «98,5 % преступлений, совершенных в финансовой сфере, это киберпреступления, а оставшиеся 1,5 % это традиционные способы совершения подобных преступлений…».[2]

Анализируя варианты противодействия и преодоления данной ситуации, необходимо отметить, что это должны быть не фрагментарные усилия по реагированию на отдельные виды киберугроз (атаки на банк, аэропорт, отдельные информационные ресурсы и т. п.), а самостоятельное направление государственной политики, основанное на Указе Президента Российской Федерации от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации», в п. 18 которой указано: «Состояние информационной безопасности в области науки, технологий и образования характеризуется недостаточной эффективностью научных исследований, направленных на создание перспективных информационных технологий, низким уровнем внедрения отечественных разработок ***и недостаточным кадровым обеспечением в области информационной безопасности*** (выделено автором – В. Г.), а также низкой осведомленностью граждан в вопросах обеспечения личной информационной безопасности. При этом ***мероприятия*** (выделено автором – В. Г.) по обеспечению безопасности информационной инфраструктуры, включая ее целостность, доступность и устойчивое функционирование, с использованием отечественных информационных технологий и отечественной продукции зачастую ***не имеют комплексной основы*** (выделено автором – В. Г.).

Следовательно, основой государственной политики в области информационной безопасности должна стать «обновленная» деятельность по обучению и воспитанию соответствующих кадров, которые бы обеспечили «прорывные» результаты в области информационной безопасности России.

Данный подход предусматривает необходимость существенных изменений как в структуре, так и в организации учебного процесса в образовательных учреждениях (особенно в вузах), организующих подготовку, переподготовку и повышение квалификации специалистов в области информационной безопас-

---

[1] URL: https://infoforum.ru/conference/conference/program/cid/32 (дата обращения: 28.02.2019).

[2] Пресс-конференция «Сбербанк делится знаниями: образовательные проекты Банка», проходившая в Информационном агентстве России ТАСС, 25 января 2017 г. // URL: https://xn--l1aeji.xn--b1aew.xn--p1ai/Press-sluzhba/Novosti/item/9330529 (дата обращения: 28.02.2019).

ности. К данной категории специалистов, наряду со специалистами технических профилей безусловно относятся сотрудники правоохранительных органов (сотрудники оперативных подразделений, дознаватели, следователи, прокуроры, судьи) [2, с. 19].

По нашему мнению, достаточно быстрый и положительный результат может дать взаимодействие вузов с организациями, имеющими определенные достижения в области обеспечения собственной информационной безопасности. Одними из ключевых субъектов в данной сфере деятельности, безусловно являются «ПАО Сбербанк России», «Лаборатория Касперского», *GIB, Positive Technologies, BI.ZONE* и некоторые другие организации.

Вместе с тем, анализ практики расследования уголовных дел о преступлениях данной категории свидетельствует о низкой раскрываемости, обусловленной сложностью сбора доказательств причастности конкретных лиц к их совершению, которая выражена в проведении следственных действий в других регионах, в изъятии телефонных соединений, и сведений из банков. Считаем, что для совершенствования расследования данной категории преступлений целесообразно:

– поручать производство по уголовным делам данной категории следователям, имеющим значительный опыт расследования преступлений в сфере информационных технологий;

– обсуждать материалы доследственных проверок в следственном управлении соответствующего субъекта, уделять особое внимание полноте и качеству собранного материала, проведению необходимых исследований, результатам ОРМ по изобличению лиц, совершивших данные преступления, установлению имущества, на которое может быть наложен арест, организовывать результативное взаимодействие с оперативными подразделениями;

– исключить факты незаконного и необоснованного возбуждения уголовных дел указанной категории, незамедлительно отменять подобные постановления;

– исключить необоснованное принятие следователями решений о приостановлении предварительного следствия без выполнения всех необходимых следственных действий, производство которых возможно в отсутствие подозреваемого или обвиняемого. При установлении таких фактов безотлагательно отменять соответствующие постановления, давать следователю письменные указания о производстве конкретных следственных и процессуальных действий, направленных на установление всех обстоятельств, подлежащих доказыванию, и привлечение виновных к уголовной ответственности;

– в целях соблюдения требований ст. 6.1 УПК РФ и недопущения необоснованного продления процессуальных сроков по делам о преступлениях указанной категории, следует обеспечить в ходе расследования проведение активных следственных действий, особенно на первоначальном этапе расследования, своевременно назначать компьютерные, дактилоскопические, технико-криминалистические экспертизы;

– при необходимости проведения портретных судебных экспертиз следует своевременно изымать в кредитных учреждениях видеоматериалы с изображением лиц, совершивших преступление;

– детально проводить допросы пострадавших, выяснять детали произошедшего;

– в кратчайшие сроки направлять запросы в адрес операторов социальных сетей, сотовой связи, интернет-провайдеров;

– при выполнении требований ч. 1 ст. 164.1 УПК РФ, проводить обучение следователей об особенностях изъятия образов электронных носителей информации, с фиксацией соответствующей «хэш-суммы» в протоколе следственного действия;

– для изъятия и осмотра электронных носителей информации привлекать в качестве специалистов «компьютерных» экспертов ЭКЦ соответствующего субъекта и специалистов организаций, специализирующихся на обеспечении информационной безопасности;

– обратить особое внимание на установление и устранение обстоятельств, способствовавших совершению указанных преступлений, исключив формальный подход к выполнению данных полномочий следователя;

– реализовать комплекс мероприятий, направленных на возмещение причиненного ущерба.

В заключении следует отметить, что выполнение данных рекомендаций, существенно повысит качество процессуальной деятельности следователей по расследованию преступлений в сфере информационных технологий, позволит повысить раскрываемость, обеспечить достаточный уровень безопасности внедряемых технологий [3, с. 93].

Список литературы

1. Савенкова Д. Д. Актуальные вопросы развития института юридической ответственности в сфере обеспечения информационной безопасности в условиях цифровизации // Проблемы права. – 2019. – № 1.

2. Гончар В. В. Совершенствование государственной политики по противодействию преступлениям в сфере информационных технологий // Вестник экономической безопасности. – 2017. – № 3.

3. Гончар В. В. Досудебное соглашение о сотрудничестве: проблемы и перспективы / В. В. Гончар, М. В. Мешков // Закон и право. – 2011.

Гусев Николай Николаевич[1]**,**
начальник кабинета специальных дисциплин
кафедры информационной безопасности
Краснодарского университета МВД России

СТАТИСТИЧЕСКАЯ ЗАВИСИМОСТЬ КАК ЭЛЕМЕНТ БОРЬБЫ С ЭКСТРЕМИЗМОМ И ТЕРРОРИЗМОМ

В настоящее время многие ученые ориентированы на борьбу с терроризмом и экстремизмом [1]. Пишутся научные статьи, проводятся десятки конференций, где каждый спикер пытается предложить свой метод решения проблемы [2]. В эпоху информатизации, когда терроризм и экстремизм может проявиться в любое время в любом субъекте страны, необходимо постоянно анализировать ситуацию. Данное исследование направлено на выявление наиболее радикальных субъектов и связи между ними, а также оценки взаимосвязи экстремизма и терроризма между собой.

Для достижения цели работы на портале правовой статистики Генеральной прокуратуры Российской Федерации был изучен ежегодный отчет 85 субъектов Российской Федерации в области регистрации преступлений террористического характера и экстремистской направленности. Материалы для данного портала предоставляют информационные центры министерства внутренних дел, главного управления внутренних дел, управления внутренних дел субъектов Российской Федерации. Отчет «Сведения о состоянии преступности и результатах расследования преступлений», утвержден приказом Росстата от 13 октября 2009 г. № 222. В настоящей работе изучены сведения за отчетный период с 2011 по 2018 гг. [3].

Шаг 1. Отбор информации связанной с преступлениями террористического характера и экстремистской направленности по каждому из 85 субъектов Российской Федерации.

Информация отбиралась по следующим категориям:

1. Зарегистрировано преступлений террористического характера – отражает количество преступлений террористической направленности, которые были зарегистрированы правоохранительными органами в течение отчетного периода. Преступления террористической направленности относятся к преступлениям против общественной безопасности. Преступления против общественной безопасности представляют собой предусмотренные уголовным законодательством общественно опасные деяния (действия и бездействия), причиняющие существенный вред общественным отношениям, обеспечивающие состояние общественного спокойствия, нормальное функционирование социальных институтов, безопасность личных, общественных и государственных интересов.

Виды преступлений террористической направленности:

а) террористический акт;

б) вовлечение в совершение преступлений террористического характера или иное содействие их совершению;

---

[1] © Гусев Н. Н., 2019.

в) публичные призывы к осуществлению террористической деятельности или публичное оправдание терроризма;

г) захват заложников;

д) заведомо ложное сообщение об акте терроризма;

е) организация незаконного вооруженного формирования или участие в нем.

2. Выявлено лиц, совершивших преступления террористического характера – отражает количество человек, зарегистрированных правоохранительными органами как совершившие преступление террористической направленности, в течение отчетного периода.

3. Не раскрыто преступлений террористического характера – отражает количество преступлений террористической направленности в отчетном периоде, производство по уголовным делам, о которых приостановлено по пп. 1–3 ч. 1 ст. 208 УПК РФ.

4. Зарегистрировано преступлений экстремистской направленности – отражает количество преступлений экстремистской направленности, которые были зарегистрированы правоохранительными органами в течение отчетного периода. Преступлением экстремистской направленности считается преступное деяние, если оно является проявлением экстремизма, а именно:

а) деятельность общественных и религиозных объединений, либо иных организаций, либо средств массовой информации, либо физических лиц по планированию, организации, подготовке и совершению действий, направленных на:

– насильственное изменение основ конституционного строя и нарушение целостности России;

– подрыв безопасности России;

– захват или присвоение властных полномочий;

– создание незаконных вооруженных формирований;

– осуществление террористической деятельности;

– возбуждение расовой, национальной, или религиозной розни, а также социальной розни, связанной с насилием или призывами к насилию;

– унижение национального достоинства;

– осуществление массовых беспорядков, хулиганских действий и актов вандализма по мотивам идеологической, политической, расовой, национальной или религиозной ненависти либо вражды, а равно по мотивам ненависти либо вражды в отношении какой-либо социальной группы;

– пропаганду исключительности, превосходства либо неполноценности граждан по признаку их отношения к религии, социальной, расовой, национальной, религиозной или языковой принадлежности;

б) пропаганда и публичное демонстрирование нацисткой атрибутики (символики) либо атрибутики (символики), сходных с нацисткой атрибутикой или символикой до степени смешения;

в) публичные призывы к осуществлению указанной деятельности или совершению указанных действий;

г) финансирование указанной деятельности либо иное содействие ее осуществлению или совершению указанных действий, в том числе путем предо-

ставления для осуществления указанной деятельности финансовых средств, недвижимости, учебной, полиграфической и материально-технической базы, телефонной, факсимильной и иных видов связи, информационных услуг, иных материально-технических средств.

5. Выявлено лиц, совершивших преступления экстремистской направленности – отражает количество человек, зарегистрированных правоохранительными органами как совершившие преступление экстремистской направленности, в течение отчетного периода.

6. Не раскрыто преступлений экстремистской направленности – отражает количество преступлений экстремистской направленности в отчетном периоде, производство по уголовным делам, о которых приостановлено по пп. 1, 2, 3 ч. 1 ст. 208 УПК РФ [1].

Шаг 2. Выборка субъектов, попадавших топ-10 по количеству зарегистрированных преступлений террористического характера или экстремистской направленности. Составление сводных таблиц.

Шаг 3. Анализ сводных таблиц. Выборка наиболее опасных регионов Российской Федерации. Вычисление коэффициента корреляции между ними.

Шаг 4. Определение зависимости между количеством зарегистрированных преступлений и количеством выявленных лиц, совершивших данные преступления или количеством нераскрытых преступлений.

Шаг 5. Проверка зависимости между преступлениями террористического характера и экстремистской направленности в регионах.

Отбор информации связанной с преступлениями террористического характера и экстремистской направленности по каждому из 85 субъектов Российской Федерации

В результате выборки информации связанной с преступлениями террористического характера по каждому из 85 субъектов Российской Федерации, сформирована сводная таблица (*рис. 1*).

Субъекты РФ	2011		2012		2013		2014		2015		2016		2017		2018	
	кол-во	место	кол-во	место	кол-во	место	кол-во	место	кол-во	место	кол-во	место	кол-во	место	кол-во	место
Астраханская область	2	8	1	15	3	13	4	21	9	17	20	15	27	13	44	8
Волгоградская область	0	28	1	15	5	8	6	17	9	17	21	14	26	14	33	13
Вологодская область	0	28	3	10	3	13	1	42	1	63	6	40	2	63	4	49
Кабардино-Балкарская республика	48	4	67	3	93	2	157	2	110	3	139	3	143	3	91	4
Карачаево-Черкесская республика	19	5	30	5	16	5	41	5	69	4	90	5	57	6	43	9
Краснодарский край	1	14	4	9	1	21	14	10	19	10	30	11	20	16	15	24
Красноярский край	2	8	1	15	3	13	5	19	14	11	12	25	13	25	21	17
Московская область	0	28	2	12	4	10	2	33	1	63	6	40	17	19	30	14
Нижегородская область	0	28	1	15	5	8	9	11	5	26	9	34	4	50	11	28
Пермский край	0	28	1	15	0	32	0	55	5	26	4	49	5	40	45	6
Республика Адыгея	4	7	0	33	0	32	0	55	6	23	10	29	18	18	10	32
Республика Башкортостан	1	14	0	33	4	10	24	8	13	12	32	10	43	8	20	19
Республика Дагестан	220	1	295	1	365	1	472	1	679	1	966	1	531	1	447	1
Республика Ингушетия	67	3	38	4	34	4	64	4	54	5	105	4	67	5	54	5
Республика Северная Осетия-Алания	2	8	0	33	1	21	7	14	10	14	35	9	51	7	23	15
Республика Татарстан	2	8	6	8	10	6	32	6	43	6	45	8	37	10	45	6
Ростовская область	0	28	3	10	0	32	2	33	11	13	22	12	28	12	21	17
Свердловская область	2	8	0	33	1	21	4	21	6	23	16	18	31	11	14	25
Ставропольский край	2	8	8	7	4	10	21	9	38	7	50	7	41	9	41	11
Тюменская область	1	14	1	15	0	32	4	21	22	9	20	15	11	30	12	27
Чеченская республика	218	2	127	2	66	3	121	3	208	2	187	2	256	2	141	2
г. Москва	11	6	13	6	9	7	25	7	36	8	67	6	96	4	105	3
г. Санкт-Петербург	0	28	2	12	2	16	2	33	7	20	13	22	16	21	42	10

Рис. 1. Сводная таблица 23 субъектов Российской Федерации, попадавших с 2011 по 2018 гг. в топ-10 по количеству зарегистрированных преступлений террористического характера

Согласно *рис. 1*, зарегистрированных преступлений террористического характера, в их число можно отнести:

1. Кабардино-Балкарская республика.
2. Карачаево-Черкесская республика.
3. Республика Дагестан.
4. Республика Ингушетия.
5. Республика Северная Осетия – Алания.
6. Республика Татарстан.
7. Ставропольский край.
8. Чеченская республика.
9. Город федерального значения Москва.

В результате выборки информации связанной с преступлениями экстремистской направленности по каждому из 85 субъектов Российской Федерации, сформирована сводная таблица (*рис. 2*).

Субъекты РФ	2011		2012		2013		2014		2015		2016		2017		2018	
	кол-во	место	кол-во	место	кол-во	место	кол-во	место	кол-во	место	кол-во	место	кол-во	место	кол-во	место
Алтайский край	5	41	7	35	21	11	25	10	29	8	26	15	45	7	18	19
Архангельская область	4	47	18	8	15	18	22	12	31	7	25	19	26	17	17	23
Вологодская область	14	7	14	15	17	16	15	20	29	8	19	29	14	38	12	33
Иркутская область	4	47	22	5	12	26	7	50	1	82	3	73	1	78	4	70
Кабардино-Балкарская республика	17	6	16	9	22	9	12	26	22	15	33	10	24	21	40	6
Кемеровская область-Кузбасс	10	19	6	40	14	19	11	31	27	12	35	9	14	38	23	14
Кировская область	11	16	16	9	11	29	26	9	33	6	39	7	30	13	18	19
Краснодарский край	14	7	15	11	20	12	37	5	29	8	20	27	25	19	18	19
Красноярский край	2	62	6	40	12	26	14	24	24	13	56	5	56	5	14	29
Курская область	12	12	12	20	24	6	30	8	20	19	21	26	18	29	25	12
Московская область	39	2	44	2	45	2	36	6	60	4	62	3	62	3	34	7
Нижегородская область	25	4	22	5	23	8	11	31	8	51	15	36	17	32	17	23
Новосибирская область	11	16	24	4	16	17	9	41	14	32	9	48	18	29	20	18
Пермский край	1	66	1	65	8	41	10	34	1	82	26	15	39	8	48	3
Приморский край	9	21	8	29	2	66	12	26	29	8	26	15	22	24	23	14
Республика Башкортостан	27	3	30	3	22	9	16	17	10	41	18	31	17	32	12	33
Республика Дагестан	5	41	14	15	24	6	50	3	82	2	70	2	87	1	75	1
Республика Татарстан	14	7	21	7	45	2	52	2	68	3	38	8	47	6	34	7
Ростовская область	8	24	15	11	11	29	9	41	13	34	17	32	22	24	32	9
Самарская область	6	31	6	40	11	29	16	17	17	25	23	22	23	22	45	4
Саратовская область	7	28	2	58	4	59	9	41	20	19	7	60	12	46	29	10
Свердловская область	11	16	15	11	30	4	44	4	46	5	57	4	62	3	41	5
Челябинская область	18	5	14	15	28	5	32	7	23	14	28	12	35	10	17	23
г. Москва	76	1	51	1	51	1	62	1	112	1	97	1	78	2	62	2
г. Санкт-Петербург	14	7	9	28	8	41	10	34	19	22	25	19	33	11	12	33

Рис. 2. Сводная таблица 25 субъектов Российской Федерации, попадавших с 2011 по 2018 гг. в топ-10 по количеству зарегистрированных преступлений экстремистской направленности

Согласно *рис. 2*, зарегистрированных преступлений экстремистской направленности, в их число можно отнести:

1. Кабардино-Балкарская республика.
2. Кировская область.
3. Краснодарский край.
4. Московская область.
5. Республика Дагестан.
6. Республика Татарстан.
7. Свердловская область.
8. Город федерального значения Москва.

Проанализировав выборки, можно сделать вывод: преступления террористического характера чаще всего совершаются в субъектах, население которых, как утверждается в работе [4], проповедует ислам. В выборке с преступлениями экстремистского направления таких субъектов меньшинство.

Для более детального изучения связей между данными субъектами в своей правовой категории, был высчитан коэффициент корреляции между ними. Таким образом в сфере преступлений террористического характера (*рис. 3*):

– Республика Татарстан, Республика Дагестан, Ставропольский край, Карачаево-Черкесская республика имеют величину коэффициента корреляции близкую к единице, что означает очень высокую связь между субъектами;

– Кабардино-Балкарская Республика, Республика Дагестан, Республика Татарстан, Республика Ингушетия, Ставропольский край имеют высокую величину коэффициента корреляции, что означает высокую связь между субъектами.

Остальные имеют среднюю и низкую связь.

	Кабардино-Балкарская республика	Карачаево-Черкесская республика	Республика Дагестан	Республика Ингушетия	Республика Татарстан	Ставропольский край	Чеченская республика
Карачаево-Черкесская республика	0,633						
Республика Дагестан	0,668	0,955					
Республика Ингушетия	0,475	0,734	0,726				
Республика Татарстан	0,705	0,828	0,788	0,502			
Ставропольский край	0,737	0,968	0,914	0,692	0,954		
Чеченская республика	0,124	0,488	0,287	0,535	0,31	0,549	
г. Москва	0,414	0,542	0,442	0,394	0,77	0,853	0,421

Рис. 3. Коэффициент корреляции преступлений террористического характера

В сфере преступлений экстремистской направленности (*рис. 4*):

– Республика Дагестан и Свердловская область имеют величину коэффициента корреляции близкую к единице, что означает очень высокую связь между субъектами;

– Краснодарский край, Республика Татарстан, Свердловская Область, Республика Дагестан, город Москва, Московская область, Кировская область имеют высокую величину коэффициента корреляции, что означает высокую связь между субъектами.

Остальные имеют среднюю и низкую связь.

	Кабардино-Балкарская республика	Кировская область	Московская область	Республика Дагестан	Республика Татарстан	Свердловская область	г. Москва
Кировская область	0,253						
Московская область	0,159	0,743					
Республика Дагестан	0,56	0,783	0,542				
Республика Татарстан	0,008	0,589	0,449	0,685			
Свердловская область	0,438	0,838	0,619	0,919	0,679		
г. Москва	0,21	0,754	0,712	0,576	0,472	0,494	
Краснодарский край	-0,31	0,514	0,125	0,486	0,81	0,562	0,247

Рис. 4. Коэффициент корреляции преступлений экстремистской направленности

Для определения взаимосвязи между преступлениями террористического характера и преступлениями экстремистского направления, так же проведены корреляционные расчеты:

1. Кабардино-Балкарская республика – 0,73 – взаимосвязь высокая.
2. Карачаево-Черкесская республика – 0,244 – взаимосвязь низкая.
3. Республика Дагестан – 0,712 – взаимосвязь высокая.
4. Республика Ингушетия – (−0,326) – взаимосвязь низкая.
5. Республика Северная Осетия-Алания – 0,83 – взаимосвязь высокая.
6. Республика Татарстан – 0,628 – взаимосвязь средняя.
7. Ставропольский край – 0,789 – взаимосвязь высокая.
8. Чеченская республика – 0,226 – взаимосвязь низкая.
9. Город федерального значения Москва – 0,232 – взаимосвязь низкая.
10. Кировская область – 0,596 – взаимосвязь средняя.
11. Краснодарский край – 0,39 – взаимосвязь низкая.
12. Московская область – (−0,132) – взаимосвязь низкая.
13. Свердловская область – 0,793 – взаимосвязь высокая.

Также необходимо отметить, что высокая связь: между зарегистрированными преступлениями и количеством выявленных лиц, совершивших преступление; между зарегистрированными преступлениями и количеством нераскрытых преступлений. Что говорит о профессионализме правоохранительных органов.

Таким образом, можно сделать вывод, что взаимосвязь между субъектами и между преступлениями в рамках одного субъекта действительно существует. Необходимо проводить более детальный анализ между субъектами, показавшими высокую и очень высокую связь между собой, выявлять и устранять общие причины роста преступности. Анализировать взаимосвязь разных видов преступности в рамках одного субъекта и пресекать все возможные проявления экстремизма и терроризма.

Список литературы

1. Арас Д. Терроризм вчера, сегодня и навеки / Д. Арас. – Баку : SADA, 2003. – 87 с.
2. Белозеров В. С. География терроризма: полномасштабный анализ террористической деятельности / В. С. Белозеров, И. П. Супрунчук. – Ставрополь : Изд-во СКФУ, 2012. – 48 с.
3. Портал правовой статистики // URL: http://crimestat.ru (дата обращения: 02.12.2019).
4. Алов А. А. Мусульманские этносы России / А. А. Алов, Н. Г. Владимиров. – М. : Институт Наследия, 1996. – 122 с. – ISBN 978-5-86443-024.

Данилкина Виталия Михайловна[1]***,***
доцент кафедры криминалистики
Московского университета имени В.Я. Кикотя,
кандидат юридических наук

ПРОФИЛАКТИЧЕСКИЕ ДЕЙСТВИЯ В СОЦИАЛЬНЫХ СЕТЯХ КАК МЕРА БОРЬБЫ С КИБЕРПРЕСТУПНОСТЬЮ

С развитием научно-технического прогресса информационные технологии стали неотъемлемой частью нашей повседневной жизни. Исходя из этого, продолжает быть актуальной деятельность по разработке современных криминалистических и уголовно-процессуальных средств и методов работы правоохранительных органов, способствующих расследованию и предотвращению преступлений в информационной сфере.

За последнее десятилетие происходит глобальное оцифровывание мира, а уровень правовой грамотности населения отстает. Возникла острая необходимость в ускорении и повышении эффективности общественных процессов в сфере информационных технологий. Как следствие, по оценкам Интерпола[2] и Европейской полиции, стремительно растет киберпреступность.

Пока еще количество «киберпреступлений» относительно общего количества преступлений имеет низкий удельный вес. Следственный департамент МВД России отмечает, что количество зарегистрированных «киберпреступлений» за 2018 г. составило 105 645[3], что составляет всего 4,9 % от общего числа преступлений. Однако ежегодно количество указанных преступлений неуклонно растет.

Стала наблюдаться острая нехватка криминалистических методов и средств для проведения профилактических действий в киберпространстве. Необходимы инновационные криминалистические разработки с целью предотвращения «киберпреступлений».

Наиболее востребованной информационной платформой особенно среди молодежи является социальная сеть. Анализ информации, размещенной в социальных сетях «Интернет», может способствовать плодотворному расследованию и эффективному проведению профилактических работ. Так, например, одним из инновационных направлений могут быть криминалистические разработки средств и методов проведения мониторинга веб-страниц с целью выявления и пресечения преступного поведения или призыва к нему. Информация, содержащаяся на веб-страницах социальных сетей, является важным объективным источником информации о личности. Фиксация факта общения в сети, наличия лиц в «друзьях», общие фотографии могут быть использованы для до-

---

[1] © Данилкина В. М., 2019.

[2] Официальный сайт Интерпола: Раздел статистика // Interpol. – URL: https://www.interpol.int (дата обращения: 13.09.2019).

[3] Аналитический обзор «Правоприменительной практики расследования преступлений, совершенных в сфере информационно-коммуникационных технологий, по итогам 2018 года // Следственный департамент МВД России. – М., 2018.

казывания мотива преступления, присутствие личной заинтересованности в ходе расследования и других обстоятельств, а также могут быть положены в основу принятия решения о производстве следственных действий (обыска, допроса, контроля и записи телефонных и иных переговоров).

Компания «Яндекс» запустила сервис для поиска людей в социальных сетях по адресу: *yandex.ru/people*. На сегодняшний день поиск можно осуществить по 16 социальным сетям: «Вконтакте», «Одноклассники», *Facebook*, *Beon*. Его можно осуществлять как по имени, фамилии, так и по никнейму, псевдониму.

Узнать, какие записи человек совершал за последнее время на *Facebook*, *Instagram* и других социальных сетях, можно с помощью *Social Searcher*.

Для того, чтобы узнать, что пользователь посетил веб-страничку в *Twitter* в конкретное время, в социальной сети есть специальный оператор для расширенного поиска – *from:@tim_cook until:2019-10-17*, а с помощью оператора *near:* можно узнать, что пишут люди в конкретном городе или в точке с определенной широтой и долготой: *near:56.35,47.03*.

В большинстве случаев пользователь мало информации выкладывает о себе в глобальную сеть, но этого бывает достаточно, чтобы получить совокупность данных о лице. Правоохранительные органы периодически предупреждают граждан посредством правовой справки, чтоб они не стали жертвой информационного преступника. Сотрудники полиция предупреждают о том, чтоб пользователи не выкладывали в сеть персонифицированную информацию, к которым можно отнести паспортные данные, данные банковских карт.

Интернет-ресурсы позволяют получить нам необходимые и имеющие значение сведения о человеке по фотографиям. Так, обладая фотографией, возможно найти, где в Интернете размещена данная (или очень похожая) фотография. Для этого нужно добавить фотографию лица человека в поиск картинок в *Google*. На сайте[1] при использовании фотографии можно осуществить поиск любого человека в социальной сети «Вконтакте». Например, с помощью поискового инструмента *Yomapic* можно увидеть снимки, которые были сделаны в указанном месте. Также в качестве эффективной профилактической меры, использующей современные информационные технологии, может рассматриваться работа с видеоизображениями. Так, на примере г. Москвы, можно просмотреть на сайте доступные в реальном времени веб-камеры, напрямую передающие все происходящее в сеть.

Таким образом, можно сказать, что целесообразность использования в расследовании преступлений сведений, размещенных на ресурсах социальных сетей сети Интернет, и проведения профилактических работ, обуславливается тем, что такого рода информации может существенно облегчить выбор направлений поисковой деятельности, а также планирование проведения оперативно-розыскных мероприятий и следственных действий; поиск информации на открытых информационных ресурсах быстрее, а иногда и эффективнее, чем при добывании ее с помощью негласных мероприятий; в условиях дефицита времени такие источники являются средством быстрого получения необходимой ин-

[1] FindClone [Электронный ресурс] // URL: https://findclone.ru.

формации. Социальные сети как инструмент в расследовании удобны своей доступностью, скоростью извлечения и объемом информации, которая может быть получена.

В настоящее время представляется целесообразным и важным разработать методические рекомендации для сотрудников правоохранительных органов, разъясняющие современные возможности, средства и методы работы с информацией в сети «Интернет».

Преступность в киберпространстве имеет высокую степень латентности. Правоохранительным органом трудно бороться с киберпреступниками, которых становится все больше, а способы совершения преступлений сложнее. Для эффективной борьбы с преступлениями в информационной сфере правоохранительным органам необходима современная техническая база, должное финансовое и материальное обеспечение, квалифицированные и подготовленные кадры, а также разработка соответствующих криминалистических мероприятий.

Список литературы

1. Предварительное следствие в органах внутренних дел : учебное пособие / А. А. Орлова, В. В. Гончар, В. И. Батюк [и др.] : под ред. М. В. Мешкова. – М. : Щит-М, 2007.

2. Смирнов И. В. Не надо разбрасываться своими персональными данными [Электронный ресурс] // URL: http://www.it-weekly.ru/it-news/security/135841.html.

3. Гончар В. В. Уголовно-процессуальная деятельность в стадии возбуждения уголовного дела: проблемы правового регулирования / В. В. Гончар, М. В. Мешков // Мировой судья. – 2015. – № 4.

4. Официальный сайт Интерпола: Раздел статистика // Interpol. – URL: https://www.interpol.int (дата обращения: 13.09.2019).

5. Состояние преступности за 2018 г. // Официальный сайт МВД России. – URL: http://www.мвд.рф (дата обращения: 24.09.2019).

6. Аналитический обзор «Правоприменительной практики расследования преступлений, совершенных в сфере информационно-коммуникационных технологий, по итогам 2018 года» // Следственный департамент МВД России. – М., 2018.

7. Веб-камеры Москвы онлайн [Электронный ресурс] // URL: http://youwebcams.net/online/category/russia/moscow.

8. FindClone [Электронный ресурс] // URL: https://findclone.ru.

Жукова Полина Николаевна[1]**,**
профессор кафедры информационно-компьютерных технологий в деятельности ОВД Белгородского юридического института МВД России имени И.Д. Путилина, доктор физико-математических наук, доцент

Золотухина Наталья Валерьевна[2]**,**
доцент кафедры уголовного процесса Военного университета Министерства обороны Российской Федерации, кандидат юридических наук

Насонова Валентина Афанасьевна[3]**,**
профессор кафедры информационно-компьютерных технологий в деятельности ОВД Белгородского юридического института МВД России имени И.Д. Путилина, кандидат физико-математических наук, доцент

ПРЕДУПРЕЖДЕНИЕ РАСПРОСТРАНЕНИЯ ЭКСТРЕМИЗМА В СЕТИ ИНТЕРНЕТ

Экстремизм – приверженность к крайним взглядам, методам действий является одной из наиболее сложных социально-политических проблем современного общества.

Многообразие форм проявления экстремизма говорит о динамичности и многосторонности этого явления. К широко известным проявлениям экстремизма относятся экстремизм международный, внутригосударственный, политический, национальный, религиозный. В последнее время наблюдается проявление экстремизма со стороны антиглобалистов, а также экологический экстремизм. Следует отметить, что представители экологического и антиглобалисткого экстремизма могут в своем движении использовать крайние, в том числе террористические средства для привлечения общественного внимания к наиболее актуальным, на их взгляд, проблемам.

Еще одной проблемой негативного распространения экстремизма является вовлечение молодежи в радикальную деятельность, что в конечном итоге может сформировать взгляды общества на ближайшие тридцать лет.

Наиболее опасным с точки зрения вступления в поле экстремистской активности является подростковый и юношеский период. В это время происходят значимые изменения как в психологическом и физиологическом, так и в социальном плане.

Подростковый возраст, как и юность характеризуются развитием самосознания и попытками определения ценности жизни. Указанный период вызывает у подростков потребность идентификации себя с группой по интересам или к которой он испытывает эмоциональную привязанность.

Однако физиология развития подростка характеризуется неустойчивой психикой – склонностью к внушению и манипулированию, что однозначно относит их в группу риска, на которую негативное влияние социальной среды чаще всего производит решающее воздействие.

К одной из основных причин вовлечения молодежи в экстремистские движения относятся проблемы уровня и качества образования. Молодежь вне школы (техникума, колледжа, вуза и т. д.) предоставлена самой себе, следовательно, возникают разнообразные молодежные группы, в том числе антиобщественные, которые, под преступным руководством, способны перерасти в экстремистские группировки. Таким образом, молодежь находится в ситуации возможного «попадания» в группы экстремистской активности.

В последние годы в школах, средне-специальных образовательных учреждениях происходят попытки формирования групп молодежи по интересам, путем создания различных дополнительных занятий и кружков. Путем привития подросткам и молодежи, в процессе обучения, социально-значимых и социально-адекватных норм поведения и восприятия внешних раздражителей, можно избежать радикализации рассматриваемой возрастной группы.

Таким образом, рассматриваемый подход по профилактике экстремистских проявлений в молодежной среде должен быть направлен на молодых людей, чья жизненная ситуация позволяет предположить возможность включения в группы экстремистской активности.

К таким категориям следует отнести:

– детей, находящихся в сложной жизненной ситуации – семьи с низким социально-экономическим статусом, подверженные алкоголизму, наркомании, физическому и моральному насилию;

– детей, подростков и молодежь, склонных к агрессии, силовому методу решения проблем и споров;

– «золотую молодежь», воспитанную в безнаказанности, вседозволенности, любящую экстремальный досуг и рассматривающую участие в экстремистской субкультуре как непосредственный образец времяпрепровождения;

– носителей молодежных субкультур, участников неформальных объединений и склонных к девиациям уличных компаний;

– участников экстремистских, политических, религиозных организаций, сект, движений.

Основными проблемными вопросами при профилактике проявлений экстремизма среди учащихся образовательных организаций являются:

1. Взаимодействие образовательных организаций с органами власти по вопросам предупреждения и профилактики экстремизма.

2. Правовые пределы реализации свободы совести и вероисповедания, свободы творчества и самореализации и экстремизма. Вопросы психологической и духовной безопасности подростка.

3. Способы и формы профилактики экстремизма учителями предметниками, социальными педагогами. Маркеры экстремистских настроений и установок несовершеннолетнего.

4. Безопасность школы при взаимодействии с некоммерческими организациями.

5. Правовые критерии и определение экстремизма. Как учителю определить в действиях ученика экстремистские взгляды и действия. Как отличить нормальные возрастные характеристики подростка (протест, чувство взрослости) и подростковый экстремизм?

6. Рискоориентированная модель. Мониторинг неформального лидерства. Алгоритмы.

7. Проблемы межкультурного диалога и вопросы гражданского единения. Толерантность и терпимость: сходства и различия. Религиозная активность и экстремизм.

Основываясь на опыте существующих программ профилактики экстремизма, имеющих правовое основание, приведем наиболее действенные направления, применимые в образовательных организациях. К таким направлениям следует отнести разработку мероприятий:

– направленных на создание психологически безопасных для молодежи при воздействии СМИ (проведение семинаров, бесед, тренингов, формирование ценностно-смысловой нормализации поведения обучающихся);

– направленных на воспитание терпимости к окружающим социальным группам, причем в данных мероприятия необходимо подчеркивать радикальную принадлежность ортогональных взглядов. Следует отметить что, при воспитании терпимости и «восприятия иного мнения», нельзя перейти черту равнодушия и попустительства;

– проведение мониторингов экстремистской направленности среди молодежи;

– воспитание уважительного межнационального общения через овладение знаниями о культурном многообразии мира.

Кроме выше перечисленного последнее время на территории Российской Федерации произошло распространение идей экстремизма через сеть Интернет. Рассматривая данную проблему более подробно, отметим, что террористическая и экстремистская пропаганда в Интернете направлена прежде всего на наиболее уязвимые и маргинальные группы общества. Это вызвано, в первую очередь, «психологическим состоянием обиды, унижения и изоляции», что зачастую служит благодатной почвой для антиобщественной пропаганды, которая умело ведет к радикализации, а, следовательно, и экстремизму. Отметим, что применение отдельных технологий по вербовке в экстремистскую и террористическую деятельность требуется с учетом возрастных, социальных и экономических, религиозных, демографических и этнических факторы.

Широко известно, что последнее время особое внимание экстремистских сайтов направлено на несовершеннолетних пользователей, поскольку формируя мышление нового поколения сейчас, определяется политика развития государства (создание либо решение проблемных вопросов) на ближайшие 30 лет.

Эта группа одна из самых многочисленных. Клиповое мышление, отсутствие критического подхода к информации, неумение анализировать служат хорошим фоном для сообщений, «мультиков» или видеоигр о доблестных тер-

ристах, смертников за правое дело. В качестве награды выступают виртуальные деньги, очки, фишки, которые надо собрать и сохранить.

Российским государством предлагается решение данной проблемы путем возложения на Минюст России функций по ведению, опубликованию и размещению в сети Интернет федерального списка экстремистских материалов[1]. Федеральный список экстремистских материалов формируется на основании поступающих в Минюст России копий вступивших в законную силу решений судов о признании информационных материалов экстремистскими.

При этом наименования и индивидуализирующие признаки информационных материалов включаются в федеральный список экстремистских материалов в строгом соответствии с резолютивной частью решения суда.

Информационные материалы признаются экстремистскими федеральным судом по месту их обнаружения, распространения или нахождения организации, осуществившей производство таких материалов, на основании представления прокурора или при производстве по соответствующему делу об административном правонарушении, гражданскому или уголовному делу.

Обжалование решений судов о признании информационных материалов экстремистскими осуществляется в порядке, предусмотренном законодательством Российской Федерации.

Законодательством Российской Федерации установлена ответственность за массовое распространение экстремистских материалов, включенных в опубликованный федеральный список экстремистских материалов, а равно их производство либо хранение в целях массового распространения. Федеральный список экстремистских материалов представлен на официальном сайте: https://minjust.ru/ru/node/243787.

В условиях неограниченного доступа несовершеннолетних к сети Интернет особое значение приобретает контроль над ситуацией в виртуальном пространстве. Особое место в распространении экстремизма в сети занимают социальные сети.

Профилактика информационной угрозы из Интернета с использованием различных средств, в том числе:

– использование программного комплекса для распознавания символьной графики экстремистского характера;

– использование специального программного обеспечения для мониторинга интернет-активности;

– привлечение к выявлению запрещенного контента киберволонтеров ячеек движения «Кибердружина»;

– использование Интернет ресурсов при профилактике экстремистских настроений в молодежных общественных группах;

– привлечение к информационной борьбе с экстремизмом общественных организаций;

---

[1] Статья 13 Федерального закона от 25 июля 2002 г. № 114-ФЗ «О противодействии экстремистской деятельности», п. 7 «Положения о Министерстве юстиции Российской Федерации», Указ Президента Российской Федерации от 13 октября 2004 г. № 1313.

– введение в школьную программу образовательного курса по критическому восприятию информации в Интернете, развитие у учащихся навыков распознавания материалов экстремистского содержания;

– активное использование Интернета для контрпропаганды, направленной против экстремизма, распространение в Интернете, особенно в социальных сетях;

– подготовка учителей-методистов в данной сфере, развитие системы школьных СМИ, посвященных соответствующей тематике. Действенной формой проведения разъяснительной работы с обучаемыми является организация просмотра ими тематических художественных и документальных фильмов, выпусков телепередач, видеороликов, посвященных разоблачению деструктивной роли идеологии терроризма и экстремизма, с последующим коллективным обсуждением. Для ее реализации необходимо обеспечить образовательные организации такими материалами или указать ссылки на них в сети «Интернет»;

– использование специального программного обеспечения в школах, для осуществления мониторинга интернет-активности учеников, включая их переписку в соцсетях, на предмет характерных терминов, употребляемых в экстремистской деятельности;

– анализ социальных сетей на предмет взаимодействия несовершеннолетнего с интернет контентом, содержащем экстремистские материалы.

Программные приложения для анализа социальных сетей:

Для анализа социальных сетей существует множество приложений для моделирования взаимодействий и процессов в сети, для вычисления определенных параметров сети и для визуализации графа сети. Например, приложения по визуализации сети «ВКонтакте» (*http://www.yasiv.com/vk*) или *Facebook* (*http://www.touchgraph.com/facebook*).

На основе заведомо известного списка групп социальной сети строится граф:

– вершины – группы социальной сети;

– ребра – наличие общих подписчиков;

– чем больше у данной группы подписчиков, тем больше размер вершины;

– чем больше у групп общих подписчиков, тем ближе друг к другу располагаются вершины.

К наиболее известным средствам автоматического мониторинга социальных сетей относятся:

– *YouScan* (*https://youscan.io*);

– *NetMiner* (*http://www.netminer.com/index.php*);

– *NetworkX* (*http://networkx.lanl.gov*);

– *SNAP* (*http://snap.stanford.edu*);

– *UCINet* (*http://www.analytictech.com/ucinet*);

– *Pajek* (*http://vlado.fmf.uni-lj.si/pub/networks/pajek*);

– *ORA* (см. *http://www.casos.cs.cmu.edu/projects/ora*);

– *Cytoscape* (*http://www.cytoscape.org*) и др.

В основу работы данных многофункциональных платформ входят анализ текста и фотографий в постах популярных социальных сетей («ВКонтакте»,

«Одноклассники», *Instagram*, *Twitter*, *Facebook*, *YouTube*, «Мой Мир» и др.), форумов, блогов, *Telegram*, отзовиков, карт и магазинов приложений, а также осуществляет мониторинг упоминаний в онлайн-СМИ.

Для подобных приложений важным требованием является возможность обрабатывать очень большое количество данных. В связи с этим процесс обработки часто распараллеливают.

Приложения, которые моделируют «теорию шести рукопожатий», которые выстраивают цепочку из связей (друзей) между двумя пользователями сети: для русскоязычной сети «ВКонтакте» (*http://ienot.ru/hand*), для англоязычных сетей (*http://www.sixdegrees.org*, *http://sixdegrees.com*). Эти цепочки, как правило, действительно получаются небольшой длины.

Бесплатный инструмент *BeSeed Engage View*, который отслеживает взаимодействия с YouTube-роликом в популярных социальных сетях «ВКонтакте», «Одноклассники», *Facebook*, *Twitter* и *Google +*.

Авторами выражается надежда, что приведенные материалы, рассматривающие проблемы профилактики в молодежной и образовательной среде таких явлений современного мира, как экстремизм, ксенофобия и терроризм, а также пути их решения, помогут работникам системы образования, в частности.

Список литературы

1. Обзор: НЦПТИ. – Вып. 1 (16). – Май 2019
2. Беличева С. А. Социально-педагогическая поддержка детей и семей «группы риска». – М., 2006.
3. Профилактика проявлений экстремизма и ксенофобии в образовательной среде : методические рекомендации. – АСОУ, 2011.
4. Экстремизм в современном обществе: сущность, формы проявления, пути противодействия : учебное пособие / Т. В. Гаврилова, С. А. Боровая, Л. Р. Никандрова. – М., 2011.

Иванов Вячеслав Юрьевич[1]**,**
начальник кафедры информационной безопасности УНК ИТ
Московского университета МВД России имени В.Я. Кикотя
кандидат технических наук, доцент

Пузарин Андрей Валерьевич[2]**,**
начальник кафедры специальных информационных технологий УНК ИТ
Московского университета МВД России имени В.Я. Кикотя

РОЛЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ СОВРЕМЕННОГО ТЕРРОРИЗМА И ЭКСТРЕМИЗМА

Мы живем в тот период, когда терроризм угрожает не только отдельно взятой стране, а распространяется по всему миру. Правоохранительные органы сталкиваются с его проявлениями практически по всему миру.

Благодаря современным информационным технологиям идеи терроризма и экстремизма поражают широкую аудиторию. Киберпространство – это среда без границ, удобное место, где безнаказанно можно проводить пропагандистскую деятельность по всему миру. Наиболее часто террористами и экстремистами для этих целей используется социальные сети. Социальные сети – это мощные платформы, которые позволяют вести пропаганду и привлекать новых сторонников свои ряды.

Каждая террористическая атака похожа на драматическое представление в которой интернет является сценой для широкой общественности. Террористические атаки часто используется для привлечения внимания средствами массовой информации и международной прессы. Терроризм нацелен на людей, которые смотрят это «представление», реальные жертвы не играют никакой роли.

Рис. 1. Изображения ИГИЛ (организация, запрещенная в Российской Федерации), распространяемые через социальные сети

Многие террористические группировки используют интернет-ресурсы каждый день. В сети активно работают не только члены исламского государства (организация, запрещенная в Российской Федерации), но другие группировки.

---

[1] © Иванов В. Ю., 2019.
[2] © Пузарин А. В., 2019.

Статистика показывает, что что начиная с двухтысячных годов количество сайтов, содержащих террористический и экстремистский контент, увеличилось в десятки раз. Террористические организации с возрастающим интересом обращаются к интернету, все большее число радикальных организаций используют даркнет. Все эти обстоятельства значительно увеличивают количество сайтов, которыми в настоящее время управляют террористические и экстремистские организации.

Каковы преимущества в использовании Интернета? Интернет предоставляет простой доступ к глобальной сцене, каждый проповедник может мгновенно достичь больших масс или нацелиться на определенные группы людей. При определенных обстоятельствах ресурсы Интернета могут предлагать анонимность пользователю, что является большим преимуществом для террористической организации, которая хочет распространять свои сообщения, оставаясь незамеченной. Интернет недорогой, группа террористов могла бы организовать эффективные пропагандистские кампании без больших экономических затрат. Но самое привлекательное в Интернете для террористических групп заключается в том, что он интерактивен. Проповедники могут непосредственно взаимодействовать со своими сторонниками по всему миру и использовать их для совершения террористических атак.

Сила террористических атак сегодня заключается в усилении эффекта, получаемого через социальные сети, когда террористы поражают свои цели и в то же время используют технологию, чтобы пропаганда распространяла страх среди широкой аудитории во всем мире.

Интернет и информационные технологии могут быть использованы террористическими организациями для нескольких целей:

- пропаганда;
- психологическая война;
- подбор и мобилизация боевиков;
- сбор средств;
- сбор информации;
- кибератаки;
- распространение программного обеспечения экстремистской направленности;
- подготовка террористических актов.

Интернет-пропаганда является наиболее распространенной технологией, которая используется террористическими организациями. Каждое видео тщательно продумано и подготовлено для формирования общественного мнения. Террористы используют новые социальные платформы, такие как *Facebook, Twitter,* и медиасервисы, такие как *YouTube*. Их язык прямой, молодой, и он может достичь определенной аудитории, используя изображения с высоким эмоциональным воздействием.

Интернет-пропаганда многоязычна. Он достигает не только арабского народа, но и легко доступна в любой стране мира. Эффект усиления достигается за счет легкого распространения контента, сочувствующие и средства массовой

информации позволяют легко обмениваться террористическими сообщениями через электронную почту, обмен сообщениями и мобильными приложениями.

Рис. 2. Видеосообщение ИГИЛ
(организация, запрещенная в Российской Федерации)

Наибольшей проблемой для спецслужб являются закрытые сообщества в социальных сетях, пропагандирующие терроризм и экстремизм. Эти сообщества, как правило. включают в себя большое количество подростков. Здесь предлагается контент, созданный в духе джихада с использованием «комического стиля», с впечатляющими видео и анимацией. Также можно найти инфографику и компьютерные игры, оба типа медиа контента очень популярны среди молодежи.

Платформы и форумы в социальных сетях используются террористическими организациями для обмена пропагандистскими и учебными материалами. В Интернете можно найти любые учебные материалы, в том числе пособия по приготовлению химического оружия и бомб. Эксперты также обнаружили документы, содержащие инструкции по похищению людей и методам пыток. Опять же, технология берет на себя решающую роль для террористов, которые также делятся руководствами по оптимизации использования социальных сетей и коммуникационных платформ, избегая мониторинга, управляемого правоохранительными органами.

Предполагаемые члены Исламского государства (организация, запрещенная в Российской Федерации) запустили новый журнал о кибервойнах для джихадистов под названием «Кибернетик», который рассказывает боевикам о технологиях.

Журнал призван обучить джихадистов тому, как участвовать в кибервойне против западных неверных. Члены ИГИЛ (организация, запрещенная в Российской Федерации) считают технологию важнейшим инструментом в борьбе против своих противников, и журнал *Kybernetiq* объясняет это.

В одной из статей в первом номере под названием «Цифровой бренд» говорится о важности использования шифрования для защиты связи, избегая любых модификаций известного алгоритма шифрования. Каждая модификация может

поставить под угрозу надежность алгоритма, поэтому автор публикации поощряет использование безопасных сквозных систем шифрования.

Статьи, включенные в журнал *Kybernetiq*, иллюстрируют членов ИГИЛ (организация, запрещенная в Российской Федерации), программы для защиты их анонимности, предотвращения подслушивания и как их использовать. Специальная сессия была написана, чтобы объяснить, как спецслужбы используют метаданные для отслеживания террористов. В разделе, озаглавленном «Метаданные могут убить», автор журнала четко предупредил о слежке, проводимой спецслужбами.

Рис. 3. Журнал *Kybernetiq*

Многие веб-сервисы могут быть использованы для получения информации, связанной с конкретным местом, которое намерены атаковать террористы. Карты *Google* могут дать злоумышленникам аэрофотоснимок места атаки. Эти фотографии могут показать присутствие наблюдательного персонала, контрольно-пропускных пунктов, заборов, точек входа и многое другое.

Эту информацию можно сопоставить с данными, полученными с помощью других служб, таких как *worldc.am*, предоставляющая злоумышленнику изображения, снятые пользователями *Instagram* в определенном месте.

Рис. 4. Сбор информации из *Google Maps*

Другим аспектом, связанным с использованием технологий, используемой террористической организацией, является коммуникация. Современные террористы широко используют мобильные приложения и другие решения для безопасной связи.

Приведенные ниже инструменты были разработаны с использованием инструмента «Секреты моджахедов», используемого террористами Аль-Каиды (организация, запрещенная в Российской Федерации):

1. *Tashfeer al-Jawwa*, мобильная платформа шифрования, разработанная Глобальным исламским медиа-фронтом (*GIMF*).
2. *Asrar al-Ghurabaa*, еще одна альтернативная программа шифрования, разработанная Исламским Государством Ирак и Аль-Шамом.
3. *Amn al-Mujahid*, программа для шифрования, разработанная Техническим комитетом *Al-Fajr*, которая является основной организацией Аль-Каиды.

Рис. 5. Мобильное приложение для *Android*, разработанное террористами

Члены групп террористов во многих случаях также используют мобильные приложения, доступные на рынке, которые реализуют сквозное шифрование, включая популярный чат для обмена сообщениями, такой как *Telegram* или *Signal*.

Все, рассмотренное выше, демонстрируют большой интерес современного терроризма к информационным технологиям. Интернет становится точкой притяжения для членов террористических организаций и их последователей и приобретает еще большую глобальную значимость.

Лунёв Юрий Станиславович[1]*,*
старший преподаватель кафедры автоматизированных информационных систем органов внутренних дел Воронежского института МВД России, кандидат технических наук

Панкратова Марина Евгеньевна[2]*,*
доцент кафедры иностранных языков Воронежского института МВД России, кандидат философских наук

Толстых Андрей Андреевич[3]*,*
преподаватель кафедры тактико-специальной подготовки Воронежского института МВД России

О ВОЗМОЖНОСТИ АВТОМАТИЧЕСКОЙ КЛАССИФИКАЦИИ ТЕКСТОВ ЭКСТРЕМИСТСКОЙ НАПРАВЛЕННОСТИ

В настоящее время невозможно представить область деятельности человека, в которую не проникли информационные технологии. Большинство людей узнают последние новости и делятся своим мнением, используя различные веб-ресурсы. Наиболее популярны среди них социальные сети. Таким образом, на сотрудников органов внутренних дел ложится дополнительная нагрузка по своевременному выявлению и реагированию на информацию экстремистского характера в Интернете. Однако, обработать объем контента, генерируемого пользователями каждый день вручную не представляется возможным. В работе предлагается рассмотреть подходы к семантическому анализу текстовых данных и выделению их направленности.

Рассмотрим основные подходы к решению поставленной задачи, а также методы их технической реализации. На первом этапе для построения модели необходимо автоматически собрать текст с веб-ресурсов и разметить части речи, входящие в предложения. Для сбора данных с различных ресурсов, предлагается использовать инструмент для автоматизации действий веб-браузера – *Selenium WebDriver*, как наиболее универсальный для задач парсинга. Для корректной разметки частей речи использовался подход на основе двунаправленных LSTM-сетей [1]. Данный математический аппарат использует концепцию двунаправленных рекуррентных нейронных сетей. У рекуррентных нейронных сетей существует значительный недостаток – все шаги вносят в память сети одинаковый вклад, независимо от того, как далеко от t-го шага они расположены во временной последовательности. Для устранения данного недостатка используется LSTM-модель [2]. Типичная ячейка *LSTM* приведена на *рис. 1*.

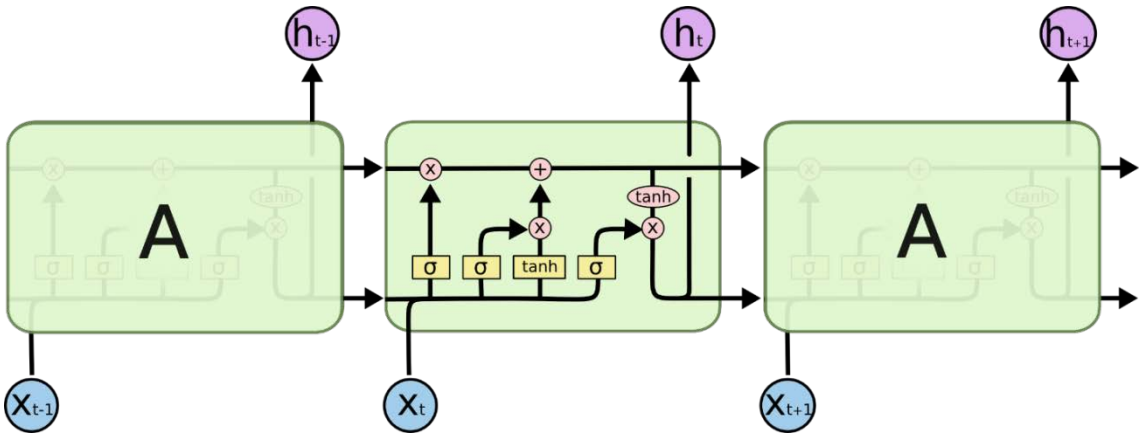

Рис. 1. Типичная архитектура *LSTM*

Формальное описание операций, производимых в каждой ячейке, происходит в соответствии с выражениями [2]:

$$f_t = \sigma\left(W_f\left[h_{t-1}, x_t\right] + b_f\right); \tag{1}$$

$$\begin{gathered} i_t = \sigma\left(W_i\left[h_{t-1}, x_t\right] + b_i\right); \\ \tilde{C}_t = \tanh\left(W_C\left[h_{t-1}, x_t\right] + b_C\right); \end{gathered} \tag{2}$$

$$C_t = f_t \square\ C_{t-1} + i_t \square\ \tilde{C}_t; \tag{3}$$

$$\begin{gathered} o_t = \sigma\left(W_o\left[h_{t-1}, x_t\right] + b_o\right); \\ h_t = o_t \square\ \tanh\left(C_t\right). \end{gathered} \tag{4}$$

Двунаправленные LSTM-сети на вход получают как прямую последовательность символов, так и обратную. Обучая подобную модель на корпусе размеченных текстов возможность классификации частей речи.

Второй этап подготовки текста состоит в проведении операции токенизации (*tokenizing*), под ней понимается выделение предложений и иных синтаксических конструкций. Для этого целесообразно использовать скрытые марковские модели [3]. В работе приводятся результаты для различных языков: чешского, немецкого, английского, французского и итальянского – разброс точности составляет не более 15 %.

Последним этапом в решении поставленной задачи выступает автоматическая аннотация текста и выделение основной направленности. Для реализации данного этапа целесообразно использовать все данные, полученные на предыдущих этапах в обобщенном классификаторе. Современные исследования показывают, что наиболее эффективным является применение моделей глубокого обучения [2].

В работе проведен анализ подходов к решению задачи семантического анализа текстовых данных и выделению их направленности с помощью инструментов машинного обучения. В дальнейшем планируется работа по следующим направлениям в рамках решаемой задачи:

– во-первых, разработать языковую модель, необходимую для корректной оценки эффективности работы классификатора;

– во-вторых, собрать из открытых источников образцы текстовых данных, и провести соответствующую разметку (относится ли конкретный образец к тексту экстремистского содержания);

– в-третьих, имплементировать рассмотренные алгоритмы на языках программирования, оценить их эффективность и устойчивость.

Список литературы

1. Bernd B. Morphosyntactic Tagging with a Meta-BiLSTM Model over Context Sensitive / B. Bernd, R. McDonald, D. Andor // CoRR. – 2018. – T. abs/1805.08237.

2. Гудфеллоу Я. Глубокое обучение / Я. Гудфеллоу, И. Бенджио, А. Курвилль – М. : ДМК Пресс, 2017. – 652 с.

3. Bryan J. Word and Sentence Tokenization with Hidden Markov Models / J. Bryan, W. Kay-Michael // JLCL. – 2013. – T. 28. – pp. 61–83.

Мозговая Дина Александровна[1]**,**
доцент кафедры криминалистики
Московского университета МВД России имени В.Я. Кикотя,
кандидат юридических наук

ИНФОРМАЦИОННЫЙ ЭКСТРЕМИЗМ В СОВРЕМЕННЫХ УСЛОВИЯХ

Двадцать первый век – не только век высоких скоростей, технологий, глобальных преобразований в социальной и экономической жизни общества, но и век в котором трансформируются способы, средства и орудия совершения преступления, переходя в информационную среду. Отмечая положительные стороны процесса информатизации в развитии российского общества, нельзя не назвать такое его отрицательное проявления, как создание благоприятных условий для распространения социально опасной или как ее еще называют «вредоносной» информации. К сожалению, из-за множественности такой информации и увеличивающихся коммуникативных потоков государственные органы самостоятельно, без привлечения органов местного самоуправления, общественных организаций не в силах в полной мере контролировать и своевременно реагировать на ее появление.

Работы ряда современных юристов, политологов, социологов и психологов посвящены феномену информационного экстремизма: сформулировано его определение, отмечены обстоятельства, способствующие его проявлению, выделены характерные черты[2].

Обращаясь к понятию «информационный экстремизм», необходимо отметить, что авторы по-разному его определяют, но в основе существующих точек зрения лежит один важный признак − использование вредоносной информации. Анализируя, приведенные в научной литературе определения, отметим, что нами разделяется мнение, в котором информационный экстремизм трактуется как деятельность, связанная с:

а) созданием, хранением и (или) распространением информации, содержащей предусмотренные законом признаки экстремистской деятельности;

б) использованием информации, обрабатываемой компьютером, компьютерной системой и (или) компьютерной сети, осуществляемой в целях воздействия на принятие решения органами государственной власти, органами местного самоуправления или международными организациями, сопряженным с различными формами психического или опосредованного физического насилия (кибертерроризм);

в) использованием информации, оказывающей деструктивное воздействие на психику людей, не осознаваемой ими[3].

---

[1] © Мозговая Д. А., 2019.

[2] Упорников Р. В. Политико-правовые технологии противодействия информационному экстремизму в России : дис. … канд. юрид. наук. Ростов н/Д, 2007. с. 148 ; Мозговой В. Э. Информационный экстремизм в условиях социокоммуникативных трансформаций российского общества : дис. … канд. социолог. наук. Краснодар, 2015. с. 146.

[3] Жукова О. С., Иванченко Р. Б., Трухачев В. В. Информационный экстремизм как угроза безопасности Российской Федерации // Вестник ВИ МВД России. 2007. № 1. С. 53.

Назвав информационный экстремизм новеллой современной преступности, Г. А. Городенцев выделил его специфические признаки, среди которых следующие: радикальность (экстраординарность) действий в достижении каких-либо целей; антисоциальность, так как нарушает сложившиеся традиции социально-правового регулирования общественных отношений[1].

В рамках предупреждения, выявления и расследования преступлений экстремистской направленности особый упор необходимо делать не только на совершенствование соответствующей нормативной правовой базы. Рассматривая информационный экстремизм как противоправное деяние, необходимо изучить его отображение в материальном мире и на основе полученных данных разработать рекомендации по выявлению, фиксации и исследованию его следов. Данная задача может быть поставлена перед наукой криминалистикой и в ближайшее время найти свое отражение в научных исследованиях, проводимых, в том числе на междисциплинарном уровне.

[1] Городенцев Г. А. Информационный экстремизм как феномен общества начала XXI века // Право и государство: проблемы методологии, теории и истории : материалы V Всероссийской научно-практической конференции. 2016. С. 114.

Молчанова Татьяна Витальевна[1]**,**
доцент кафедры криминологии
Московского университета МВД России имени В.Я. Кикотя,
кандидат юридических наук, доцент

ПРОБЛЕМЫ ИНФОРМАЦИОННЫХ РЕСУРСОВ В ОЦЕНКЕ ОРГАНИЗОВАННОЙ ПРЕСТУПНОСТИ В СФЕРЕ ЭКОНОМИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ

«Не приходится сомневаться в том, что в России, как и в других странах, нежелательные поступки, ужасные поступки, поступки, очевидным образом противоречащие отечественному и международному законодательству порой совершаются не одним человеком, а целой группой лиц, иногда это довольно значительные группы лиц, которые могут состоять из людей одного возраста, пола, национальности, случается, что они объединяются в иерархические структуры, подчас контролируя определенные территории, подкупая представителей власти, убивая своих конкурентов». Речь, очевидно, идет об организованной преступности.

Организованная преступность, в частности, является поистине глобальным явлением, которое затрагивает повседневную жизнь всех нас. Подлинные масштабы организованной преступности неизвестны. Проблема оценки масштабов организованной преступности осложняется основными взаимосвязанными факторами: усилиями по сокрытию информации, предпринимаемыми организованными преступными группами и преступными сообществами; непредставлением информации жертвами преступных посягательств; степенью участия организованной преступности в том или ином конкретном преступлении и разнообразными формами проявлений этого преступного явления.

Организованная преступность является более скрытой, чем многие другие виды преступности, поскольку предпринимаются весьма существенные усилия для того, чтобы она не стала известна. Особый характер организованной преступности снижает вероятность того, что жертвы, свидетели, очевидцы не сообщают об этих преступлениях в правоохранительные органы.

Усложнение задач противодействия организованной преступности в сфере экономической деятельности обусловливают необходимость осмысления как существующих традиционных методов изучения преступности, так и возможности выхода за рамки таких методов.

Необходимо отметить, что для формирования оценки состояния организованной преступности в сфере экономической деятельности в России применяется статистическая отчетность ГИАЦ МВД России, но социально-криминологическая характеристика преступности, содержащаяся в сборниках ГИАЦ МВД России, преимущественно охватывает информацию о субъектном составе противоправных посягательств, не акцентируя внимание на отдельных криминологически значимых индикаторах, в связи с чем ее использование без существенной переработки не представляется эффективным и достаточным. Издания, предлагаемые Росстатом, МВД России, ФСИН России, Генеральной Прокуратурой Российской

Федерации, Следственным комитетом, не предназначены для исследования преступности.

Существующие формы государственной статистической отчетности фиксируют лишь совершение отдельных преступлений в составе организованной преступной группы, в исключительных случаях в составе преступного сообщества. Использование официальной государственной статистики для измерения уровня организованной преступности порождает множество искажений в ее оценке. Официальная статистика в ряде случаев способна правильно показывать лишь тенденцию. На сегодня описываемая криминологическая проблема не имеет фактической оценки ее современного состояния. Это связано, прежде всего, с особой сложностью статического измерения, технологии сбора и анализа информации, выбора инструментария и методологии исследования, выбора теоретической модели прогнозирования организованной преступности, установления ее прогнозных тенденций и закономерностей.

Таким образом, данные о преступлениях, зарегистрированных в статистической отчетности органов внутренних дел не позволяют измерить преступность как таковую, а предоставляют информацию о преступлениях, о которых стало известно и которые сами зафиксировали.

В этой связи, крайне необходимо иное понимание совершенствования имеющихся знаний и возможностей в области оценки организованной преступности в сфере экономической деятельности с тем чтобы пресечь и предотвратить такого рода преступные группы и сообщества, однако эти усилия не всегда помогают нам определить истинные масштабы такой организованной преступной деятельности.

Хотелось бы быть уверенным, что по мере укрепления потенциала правоохранительных органов они становятся все более эффективными в выявлении организованной преступности во всех ее формах и проявлениях, в результате такого рода тенденций должна выявляться и пресекается деятельность большего числа организованных преступных групп. С другой стороны, по-прежнему сложно предсказать, меняются ли реальные уровни организованной преступности.

На сегодня существует один из альтернативных вариантов (методов) оценки организованной преступности с учетом проблем измерения и необходимости выработки конкретных руководящих указаний в отношении усилий по пресечению и предупреждению данного вида преступности. Этот метод является попыткой измерить организованную преступность путем оценки различных товарных рынков и потоков. Так, в 2010 г. УНП ООН опубликовало доклад «Глобализация преступности: оценка угрозы транснациональной организованной преступности», который впервые позволил провести глобальный обзор рынков и потоков незаконной продукции. Впоследствии ЮНОДК подготовило несколько других докладов, в которых основное внимание уделяется проблемам транснациональной организованной преступности в конкретных регионах мира, с тем чтобы обеспечить более конкретные руководства к действию[1].

[1] Управление Организации Объединенных Наций по наркотикам и преступности. (2010): Глобализация преступности: оценка угрозы транснациональной преступности. Vienna : UNODC. P. 2.

Данные, на которых основан этот доклад, взяты из имеющейся информации об арестах, судебных протоколах, сообщениях средств массовой информации, докладах НПО и экспертных заключениях на местах во многих различных странах мира, которые непосредственно сталкиваются с этими незаконными рынками перемещения товаров. К рынкам, включенным в доклад, относятся торговля людьми, незаконный ввоз мигрантов, торговля кокаином и героином, торговля огнестрельным оружием, торговля дикой флорой и фауной, контрафактная продукция, морское пиратство и киберпреступность.

Этот глобальный анализ помог изменить подход к организованной преступности, акцентируя внимание на разнообразные источники информации о конкретных организованных преступных групп и отдельных видах преступной деятельности, на незаконные рынки перемещения товаров из источников в пункты назначения. В докладе освещаются направления финансовых потоков, которые используются для извлечения прибыли организованными преступными группами.

Оценка риска должна также учитывать причиненный ущерб. Эти виды ущерба включают финансовый ущерб юридическим и физическим лицам, экономике государства (путем вымогательства и неуплата налоговых сборов и платежей на незаконные товары и услуги), а также физический ущерб (люди, эксплуатируемые при предоставлении незаконных товаров и услуг; жертвы угроз и принуждения). Другие виды вреда, причиняемого организованной преступностью, включают снижение доверия общественности к деятельности всех видов органов государственной власти.

На сегодня, большинство оценок деятельности организованной преступности сосредоточены на выявлении организованных форм преступных групп. Эти оценки были проведены правоохранительными органами для определения того, какие группы подвергаются наибольшему риску или представляют наибольшую угрозу. Методы, используемые для определения риска, включают выявление наиболее известных организованных преступных групп в конкретном регионе и последующее ранжирование их по признакам и потенциальной серьезности.

Фактическую оценку рисков на практике провести сложно. Это связано с тем, что оценка основывается на неточных показателях характера и масштабов преступной деятельности, причиненного вреда, а также субъективных оценках следователей, экспертов и общественности, которые могут существенно отличаться. Оценка на основе данных о преступлениях, собранных на различных этапах уголовного судопроизводства (уголовное преследование, осуждение, тюремное заключение), также может вводить в заблуждение. Например, весьма проблематично ожидать, что успешное судебное преследование лиц, причастных к организованным преступным группам, приведет к нарушению функционирования этой группы или рынка незаконных товаров и услуг.

Оценка риска организованной преступности в сфере экономической деятельности является весьма важным инструментом для правоохранительных органов. Это понимание помогает определить выбор приоритетных направлений

в выявлении, раскрытии, расследовании и профилактике организованной преступности в сфере экономической деятельности.

Значительное увеличение объема данных, источниками и средствами распространения которых являются социальные объекты, приводит к формированию новых технологий обработки информации об организованной преступности в сфере эконмической деятельности.

Так, согласно консенсус-прогнозу ведущих криминологов и правоохранителей, переход к объективному мониторингу организованной преступности на основе интернета, с использованием различного формата данных, обрабатываемых искусственным интеллектом, возможно оценить в полном объеме в период 2023–2025 гг.

На сегодня, современные средства статистического сбора и обработки данных представлены в разнообразном виде, но стержневой составляющей, пронизывающей различные технологические кластеры новых промышленных революций и превращающей их в единый технологический процесс, являются, без сомнения, информационные технологии. Существенные шаги в этом направлении в нашей стране уже сделаны: создаются электронные учеты, реестры, оптимизируются всевозможные государственные услуги и способы аутентификации человека в них, развивается интернет-банкинг и т. д.

В этой связи проставляется необходимость использования большого объема структурированной и неструктурированной информации данных при изучении и оценке количественных параметров организованной преступности в сфере экономической деятельности. Это дает значительные возможности для использования больших данных в формулировании прогнозных тенденций изменения организованной преступности, а также использование новых технологий в теории и практике предупреждения организованной преступности.

Прогнозирование и предупреждение организованной преступности представляется весьма затруднительным процессом, а иногда и невозможным получить эмпирические подтверждения, а тем более прогностическую верификацию той или иной концепции. Соответственно, традиционные научные подходы до настоящего времени практически не работают в сфере изучения организованной преступности. Между тем правоохранительные органы должны располагать знаниями о структуре преступности, появлении новых форм организации преступных сообществ, изменения преступного поведения под воздействием технологий новой технологической революции и т. п.

Мысина Анастасия Ильинична[1]***,***
адъюнкт 2-го года обучения факультета подготовки
научно-педагогических и научных кадров
Московского университета МВД России имени В.Я. Кикотя
по кафедре прав человека и международного права

МЕЖДУНАРОДНО-ПРАВОВОЕ РЕГУЛИРОВАНИЕ ПРОТИВОДЕЙСТВИЯ ФИНАНСИРОВАНИЮ ТЕРРОРИЗМА С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

В современных условиях развития мирового сообщества одним из наиболее общественно опасных киберпреступлений является финансирование терроризма с использованием информационных технологий.

Следует отметить, что 9 октября 1999 г. резолюцией 54/109 Генеральной Ассамблеи Организации Объединенных Наций (далее – ООН) принята Международная Конвенция ООН о борьбе с финансированием терроризма [1]. Необходимо обратить внимание на то, что указанный международный договор не закрепляет положений, посвященных противодействию финансированию терроризма с использованием информационных технологий, и подписан гораздо раньше, чем региональные международно-правовые акты, направленные на регламентацию вопросов сотрудничества государств по противодействию киберпреступности.

К их числу, в первую очередь относится Конвенция Совета Европы о киберпреступности 2001 г., в положениях которой не находят отражения международно-правовые нормы, регулирующие вопросы сотрудничества государств по противодействию финансированию терроризма с использованием информационных технологий [2].

В Соглашении между правительствами государств – членов ШОС о сотрудничестве в области обеспечения информационной безопасности 2009 г. впервые на уровне международно-правового регулирования закрепляется понятие «информационный терроризм», которое в соответствии с рассматриваемым соглашением представляет собой использование информационных ресурсов и (или) воздействие на них в информационном пространстве в террористических целях [3]. Так, например, использование в преступной деятельности криптовалют (или, так называемых, цифровых финансовых активов) в целях финансирования терроризма будет подпадать под обозначенное понятие и представлять собой одну из разновидностей преступления в сфере информационных технологий.

В Конвенции Лиги арабских государств о борьбе с преступлениями в сфере информационных технологий 2012 г. к числу противоправных деяний, подлежащих криминализации в соответствии с нормами национального уголовного права государств – участников, относится, в частности, «финансирование и подготовка террористических операций, а также содействие коммуникации между террористическими организациями» [4].

---

[1]

Анализ Конвенции Африканского союза о кибербезопасности и защите персональных данных 2014 г. [5] и Соглашения о сотрудничестве государств – участников СНГ в борьбе с преступлениями в сфере информационных технологий 2018 г. [6] позволяет констатировать отсутствие в их положениях международно-правовых норм, регламентирующих вопросы сотрудничества государств по противодействию финансированию терроризма с использованием информационных технологий.

С учетом изложенного представляется сообразным отметить, что международно-правовое регулирование противодействия рассматриваемого рода преступлениям является достаточно фрагментарным. В целях совершенствования международно-правовых основ сотрудничества государств при борьбе с транснациональной преступностью предлагаем разработать и заключить специализированный международный договор, регламентирующий вопросы сотрудничества государств по противодействию финансированию терроризма с использованием информационных технологий.

В отношении национального правового регулирования ответственность за финансирование терроризма устанавливается в ч. 1.1 ст. 205.1 Уголовного кодекса Российской Федерации (далее – УК РФ) «Содействие террористической деятельности» [7]. Однако в рассматриваемом нормативном правовом акте не детализированы вопросы уголовной ответственности за совершение финансирования терроризма с использованием информационных технологий.

Позиционно, осуществление финансирования терроризма представляет наибольшую общественную опасность в случае, если совершается с использованием информационных технологий. Поскольку в большинстве случаев реализуется при помощи криптовалют, что в свою очередь, значительно повышает скорость, анонимность и латентность финансирования терроризма. В связи с чем на наш взгляд представляется сообразным предусмотреть в УК РФ возможность более сурового наказания за финансирование терроризма с использованием информационных технологий.

Кроме того, в УК РФ закреплены и другие преступления, общественная опасность которых повышается в случае использования информационных технологий. К таковым, например, можно отнести Легализацию (отмывание) денежных средств или иного имущества, приобретенных другими лицами преступным путем (ст. 174 УК РФ) и незаконный оборот наркотиков (ст. 228 УК РФ) [8], торговлю людьми (ст. 127.1 УК РФ) [9] и т. д.

В современных условиях верховенства права [10] в целях оптимизации правового регулирования [11, 12] финансирования терроризма и ряда других преступлений, общественная опасность которых увеличивается в случае использования при их совершении различных информационных технологий, в рамках национального уголовного права предлагаем в рамках ст. 63 «Обстоятельства, отягчающие наказание» закрепить следующую норму: «Судья (суд), назначающий наказание, в зависимости от характера и степени общественной опасности преступления, обстоятельств его совершения и личности виновного может признать совершение преступления с использованием информационных технологий отягчающим обстоятельством». Нормативно-правовое предписание

данного содержания позволит избежать повышения уголовной ответственности в тех случаях, когда использование информационных технологий не повлияло на общественную опасность совершения того или иного преступления.

Подводя итоги всему вышеизложенному, необходимо сделать вывод о том, что преступления в сфере информационных технологий активно развиваются и все чаще приобретают транснациональный характер. К числу наиболее опасных среди них относится финансирование терроризма с использованием информационных технологий. Международно-правовое регулирование сотрудничества государств по противодействию преступлениям подобного рода развито достаточно слабо и требует совершенствования. В качестве одного из решений данной проблемы выступает разработка и заключение специализированного международно-правового акта, посвященного вопросам транснационального сотрудничества по противодействию финансированию терроризма с использованием информационных технологий. В целях оптимизации уголовно-правового регулирования противодействия финансированию терроризма и ряда других преступлений, общественная опасность которых увеличивается в случае использования при их совершении различных информационных технологий, считаем сообразным предусмотреть в УК РФ возможность признания по усмотрению суда совершения преступления с использованием информационных отягчающим обстоятельством при назначении наказания с учетом характера и степени общественной опасности преступления, обстоятельств его совершения и личности виновного.

Список литературы

1. Международная Конвенция ООН о борьбе с финансированием терроризма 1999 г. // Конвенции: Официальный сайт ООН. – URL: https://www.un.org/ru/documents/decl_conv/conventions/terfin.shtml (дата обращения: 18.10.2019).

2. Конвенция Совета Европы о киберпреступности 2001 г. // Справочно-правовая система «Гарант». – URL: http://base.garant.ru/4089723 (дата обращения: 23.07.2019).

3. Конвенция Лиги арабских государств о борьбе с преступлениями в сфере информационных технологий 2012 г. // URL: http://itlaw.wikia.com/wiki/Arab_Convention_on_Combating_Information_Technology_Offences (дата обращения: 23.07.2019).

4. Соглашение между правительствами государств – членов Шанхайской Организации Сотрудничества о сотрудничестве в области обеспечения информационной безопасности 2009 г. // Официальный сайт ШОС. – URL: https://ccdcoe.org/sites/default/files/documents/SCO-090616-IISAgreementRussian (дата обращения: 23.07.2019).

5. Конвенция Африканского союза о кибербезопасности и защите персональных данных 2014 г. // URL: https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection (дата обращения: 23.07.2019).

6. Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной

информации 2001 г. // Справочно-правовая система «ГАРАНТ». – URL: http://base.garant.ru/ 12123778 (дата обращения: 19.07.2019).

7. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ // Справочно-правовая система «ГАРАНТ». – URL: http://base.garant.ru/5761986 (дата обращения: 22.07.2019).

8. Ализаде В. А. Судебная практика по делам о преступлениях в сфере незаконного оборота наркотиков, совершенных с использованием криптовалюты: от разных подходов к предложению единого понимания / В. А. Ализаде, А. Г. Волеводз // Библиотека криминалиста: Научный журнал. – 2018. – № 1 (36). – С. 306–333.

9. Козлова А. А. Международно-правовые основы сотрудничества государств в сфере противодействия незаконному обороту человеческих органов : дис. … канд. юрид. наук. – М., 2019.

10. Каламкарян Р. А. Господство права Rule of Law в международных отношениях. – М., 2014. – С. 176–178.

11. Котляров И. И. Международное право и его роль в деятельности органов внутренних дел России / И. И. Котляров, Ю. В. Пузырева // Вестник экономической безопасности. – 2015. – № 7. – С. 52–61.

12. Гончар В. В. Совершенствование государственной политики по противодействию преступлениям в сфере информационных технологий // Вестник экономической безопасности. – 2017. – № 3. – С. 130–135.

Овчинский Анатолий Семенович[1]**,**
профессор кафедры информационной безопасности УНК ИТ
Московского университета МВД России имени В.Я. Кикотя,
доктор технических наук, профессор, академик РАЕН

ПРИОРИТЕТНЫЕ НАПРАВЛЕНИЯ ПРОТИВОДЕЙСТВИЯ ЭКСТРЕМИЗМУ И ТЕРРОРИЗМУ

Подходя к приоритетным направлениям противодействия экстремизму и терроризму в цифровом мире, обратим внимание на то, что одним из наиболее значимых факторов нашей жизни стало стремительное накопление самых разнообразных данных, сведений, сигналов.

Возникает образ информационного взрыва, информационного катаклизма или даже апокалипсиса. Западные социологи пишут об информационной перегрузке, когда нет возможности позитивно использовать доступные объемы данных. В стремительном накоплении самих данных усматривается сингулярность, когда, скажем, их количество удваивается с течением времени и счет идет уже не на годы, а на недели и дни. И, главное, пределов роста пока не просматривается.

В контексте борьбы с экстремизмом и терроризмом результаты весьма обстоятельных исследований показывают, что с неудержимым увеличением количества генерируемых данных информационные сферы, информационный эфир нашей жизни все плотнее наполняется некими суррогатами, осколками разнообразных идеологий, мировоззренческих доктрин прошлого, искаженных и часто исковерканных представлений об исторических событиях. Потоки самых разнообразных данных часто просто смывают общепризнанные смыслы жизни.

Все это открывает дорогу деструкции, создает психологическую, идеологическую, историческую, мировоззренческую базу экстремизму и терроризму все цветов и оттенков. Воронки многочисленных сетевых деструктивных сообществ последовательно втягивают в себя миллионы людей, молодежь, подростков, школьников, детей. Накапливаются потенциалы деструктивной социально-психологической энергии, разрядка которых приводит к суицидам, расстрелам, террористическим актам или к протестным выступлениям, переходящим в погромы и разрушения.

Очевидно, что в противодействии экстремизму и терроризму необходимо мониторить информационные сферы, выявлять очаги деструкции, криминальной идеологии, формирование и распространение идей терроризма, центры притяжения экстремистских устремлений. Центры нужно ликвидировать, узлы сетевых структур вырезать. Такая работа ведется. Есть определенные успехи. Удается предотвращать террористические акты, расстрелы в школах, суициды детей.

Однако объемы данных, несущих лживую негативную информацию, неумолимо нарастают. И нарастают с такой скоростью, что противоборствовать деструкции все сложнее и сложнее. Но, главное, даже когда удается очистить какие-либо сегменты от деструктивной информации, возникает основная про-

блема: чем и как ее заменить? При этом необходимо представлять, что информационная деструкция – это не только какие-либо и где-либо данные и сведения, это, в первую очередь, содержание и наполнение сознания миллионов людей, которые все глубже погружаются в виртуальные миры.

Понятно, что ни информационные сферы, ни сознание людей, сообществ, народов не потерпит пустоты. Противоборство с одним открывает дорогу другому. Естественно возникает вопрос о приоритетных направлениях собственно информационного противоборства с экстремизмом, терроризмом, криминалом, социальной деструкцией.

И здесь мы должны от стремительно возрастающих данных обратиться к сути собственно информации.

В научном и методологическом планах проблема заключается в том, что представления об информации развивались по весьма разнообразным траекториям. На условно гуманитарном пути информацию связывали с новыми знаниями, с сенсационными сообщениями. В кибернетике она представала в управляющих сигналах. Она проходила этапы формализации в математических моделях, обогащала вычислениями теории связи и управления. В философии выделялись атрибутивный и функциональный подходы к информации.

Однако сейчас встретить результаты фундаментальных исследований природы собственно информации не удается. Аналогично, когда создавалась атомная бомба, исчезли работы по ядерной физике. В то же время, если применение ядерного оружия не требует углубления в суть нейронно-протонных взаимодействий, то успехи или неудачи операций информационной войны, как и эффективность информационного противоборства, напрямую связаны с сущностными проявлениями самой информации.

«Увидеть» возникновение и проявление собственно информации можно в реакциях на воздействия и побуждения. Реакции присущи всем объектам живой природы, а сейчас и роботизированным системам. В сознании человека реактивная информация возникает как функция целевой интерпретации поступающих сообщений и сигналов. И если в природных и технических системах роль информации состоит в обеспечении адекватных реакций, то сознанию человека именно реактивная информация позволяет понимать смысл происходящего, быть личностью, ощущать связь с прошлым, планировать будущее, иметь представление о том, что находится за пределами нашей реальности.

В отличии от реактивной ресурсная информация фиксируется, накапливается и транслируется на определенных носителях. В живой природе это осуществляется физико-химическими и биологическими взаимодействиями. Истинно биологическая ресурсная информация, закрепленная в генетических кодах, в строении органов и тканей и передаваемая от вида к виду из поколения в поколение обеспечивает эволюцию жизни.

Социальная ресурсная информация требует внешних искусственных, уже созданных человеком носителей. Информационные технологии сегодня коренным образом меняют весь уклад жизни людей. Но и в прежние времена основные этапы в развитии цивилизации были связаны с методами и средствами получения и использования социальной ресурсной информации. Наскальные

рисунки, петроглифы, иероглифы, алфавитная письменность, бумажные носители, книгопечатание, массовые издания, фото и киноизображение, радио и телевидение, электронные носители и интернет – это технологии фиксации, накопления и трансляции социальной ресурсной информации.

Наконец фоновая информация непосредственно отражает окружающую реальность. Так же как реактивная и ресурсная, фоновая информация выступает атрибутом мироздания, проявляя фундаментальное свойство – отражение и создавая собственно фон как природной, так и социальной жизни. Она выполняет и свою функциональную роль, скажем, воздействуя на людей часто в обход защитных механизмов сознания.

Если реактивная информация позволяет выживать объектам природы, обеспечивая адекватность реакции, а людям понимать смыслы происходящего, ресурсная информация фиксирует и передает опыт выживания и развития, то фоновая информация включает механизмы адаптации к изменяющимся условиям обитания или социального окружения [1].

Важно, что представление информации в триединстве реактивных, ресурсных и фоновых проявлений, отражающих ее сущностные качества, дает еще и новую универсальную систему координат, в которой в трехмерном пространстве раскрываются самые разнообразные понятия, поскольку все явления и процессы нашей жизни и деятельности так или иначе построены на информационных взаимодействиях.

В трехмерном пространстве информационных координат информационную войну против России, которая десятилетиями ведется западными странами, можно представить в единстве психоисторической, психоидеологической и психодемографической войны.

Идеи психодемографической войны восходят от мальтузианства и социодарвинизма. Они оформились в недрах Британской империи, прошли апробацию как на многочисленных колонизированных народах, так и на беднейших слоях населения самой Англии. Непосредственным уничтожением миллионов людей свой след в истории оставили фашистская Германия и милитаристская Япония. В последние, условно мирные десятилетия, на сокращение населения стран и регионов были направлены волны сексуальных революций, разрушения семейных ценностей, движения за права сексуальных меньшинств.

Заметим, что если в планах Адольфа Гитлера после победы в войне с Советским Союзом было оставить в живых не более 50 млн русских рабов, то Маргарет Тетчер после разрушения Советского Союза уже в преддверье новой промышленной революции заявляла, что в России достаточно иметь только 15 млн жителей для обслуживания нефтепромыслов, газопроводов и добывающей промышленности. И в «лихие» 1990-е гг. под ударами психодемографической войны население нашей страны ежегодно сокращалось на 600–700 тысяч человек.

Информационная война на разных уровнях общественного сознания велась и ведется и на идеологических фронтах. Идеологию необходимо рассматривать не столько как систему взглядов, отражающих отношение к окружающей действительности, сколько как глобальную мотивационную матрицу, обосновывающую право на те или иные действия и поступки, на образ жизни и мыслей.

Угрозы социальной деструкции вызревают с криминальной идеологией, идеологиями экстремизма и терроризма, обосновывающими право на преступную деятельность, на убийства и самоубийства, на разрушение основ государственности [2].

Возрастающие в виртуальном пространстве сетей, блогов, сайтов информационные потоки наполняются зловещими смыслами. Огромный спектр информационных ресурсов: от отечественных криминальных сообществ, до американских расистских и неонацистских групп ненависти, от политических радикалов и протестных сообществ до уличных бойцов, от сайтов террористических организаций до виртуальных сект (неоязычиских, религиозных, сатанинских, тоталитарных, коммерческих) разрушает сознание многих миллионов людей, побуждая их к противоправным, асоциальным действиям, все чаще приводя к кровавым инцидентам с массовыми убийствами в самых разных местах планеты [3].

Можно по-разному оценивать роль и значение идеологии, но, применив систему информационных координат, увидим, что реально борьба за сознание людей в современном мире ведется в пространстве трех основных мировых идеологии: либерализма, консерватизма и социализма.

При этом реактивный вектор – либерализм, агрессивно провозглашая приоритет правам человека, настойчиво формирует человека-потребителя, человека-мобильного (у которого Родина там, где лучше) и уже человека бесполого (сам выберет себе пол, когда подрастет).

Ресурсный вектор мировых идеологий – консерватизм, негативно воспринимаемый сторонниками прогресса, однако возвращает нас к человеку – защитнику, человеку долга, человеку патриоту своего отечества, ценящего духовные традиции своего народа.

Наконец, фоновый вектор – социализм, а в перспективе и коммунизм, незаслуженно снятые с пьедестала в нашей стране, отдавая приоритеты коллективизму и справедливости, напоминают, что высшее призвание человека заключается в творчестве, а смысл общественного развития – в формировании личности и раскрытии ее потенциалов.

Если операции психодемографической и психоидеологической войн, как правило, имеют скрытый характер, то наиболее «горячие» информационные сражения сегодня происходят на психоисторическом фронте.

Ресурсный вектор истории в информационных координатах – это дошедшие до нас свидетельства, документы, артефакты, воспоминания очевидцев. Однако построение истории требует определенной интерпретации прошлого (это уже реактивный вектор построения истории). Но интерпретация отражает позицию исследователя, можно даже сказать, преследует определенные цели (здесь включается фоновый вектор истории, который, как правило, определяется идеологией, а часто и непосредственно стоящими задачами).

Если мыслители прошлого замечали, что история – это факел, высвечивающий будущее, то практика уже информационной эпохи показывают, что для изменения вектора развития страны меняют ее историю.

Информационные координаты отражают и уровни психоисторической войны: фактологический (фальсификация фактов), концептуальный (заданная интерпретация), метафизический (разрушение смыслов).

Одна из основных задач психоисторической войны состоит в том, чтобы скрыть субъекты глобального управления и истинные причины мировых потрясений. Сегодня именно Россия является эпицентром психоисторической войны как непреодолимый барьер к мировому господству. При этом главной мишенью информационных атак стала Победа в Великой Отечественной войне [4]. Хотя основные угрозы психоисторической войны состоят в отсутствии единого консолидированного подхода к построению своей героической истории.

Намечая глобальные стратегии, которые должны быть взяты на вооружение в борьбе с внешними и внутренними деструктивными силами, следует обратиться к основным концептуальным приоритетам в управлении социальными процессами и международными отношениями [5].

Если ранее сложились и продолжают господствовать такие приоритеты как военно-силовой, финансово-экономический и рефлекторно-психологический, то сейчас становится все более очевидным, что активные наступательные действия в информационном пространстве должны опираться в первую очередь на свою осмысленную и развивающуюся систему приоритетов.

Такими высшими приоритетами управления общественным развитием должны стать идеологический, исторический и мировоззренческий. Раньше эти приоритеты использовались весьма узкими, часто закрытыми, иногда тайными, иногда полумистическими элитарными сообществами, претендующими на управление мировыми процессами. Сегодня, в цифровом мире они должны защитить массовое сознание от деградации и социальной деструкции.

Стремительно возрастающие потоки информации должны нести такие смыслы и направляться в такие русла, в которых они не будут дробить сознание народов, отуплять людей, порождать деструкцию, толкать на убийства и самоубийства.

Повышение эффективности противоборства разрушительным акциям информационной войны требует наполнения информационных сфер, социальных сетей, блогов, сайтов Интернета, средств массовой информации, культурно-образовательной среды мощным позитивным патриотическим контентом.

Такой контент должен быть сформирован на основе ясной идеологии, обосновывающей право на национальный суверенитет, на защиту традиционных духовных ценностей, на творчество в достижении высоких жизненных целей. Нужно целенаправленно создавать и мировоззренческий фон, который будет адекватен как научным представлениям о мироздании, так и духовным достижениям, раскрывающим глубокие смыслы существования человечества и цивилизационного развития. Наконец, требуется консолидированный подход к отечественной истории не как к «признанию российской катастрофы XX века», а как к героическому прошлому, наполненному великими свершениями и победами.

При последовательном использовании в информационном противоборстве высших приоритетов управления реактивная информация, давая идеологиче-

скую мотивацию и порождая энергию действий и поступков, ресурсная информация, связывая прошлое, настоящее и будущее и образуя мировоззренческую основу, фоновая информация, отражая окружающую реальность и наполняя смыслами общественные отношения и коммуникации, станут теми базовыми элементами, теми рычагами и инструментами, которые требуются для преодоления угроз социальной деструкции в условиях информационной войны против России.

Список литературы

1. Овчинский А. С. Информационные воздействия и организационная преступность. – М. : Инфра-М, 2007.
2. Овчинский А. С. Матрица преступности / А. С. Овчинский, С. О. Чеботарева – М. : Норма, 2006.
3. Сундиев И. Ю. Теории и технологии социальной деструкции / И. Ю. Сундиев, А. А. Смирнов. – М. : Русский биографический институт; Институт экономических стратегий, 2016.
4. Фурсов А. И. Психоисторическая война: Скрытые субъекты глобального управления и фальсификация истории // Изборский клуб. – URL: Izbjrsk-club.ru/2439.
5. Ефимов В. А. Концептуальная власть. – М. : Издательский дом «Общественная инициатива», 2003.

Серезевский Алексей Вадимович[1]**,**
заместитель начальника кафедры
специальных информационных технологий УНК ИТ
Московского университета МВД России им. В.Я. Кикотя

К ВОПРОСУ О ЗАПРЕТЕ ПРИЗНАНИЯ ЭКСТРЕМИСТСКИМИ МАТЕРИАЛАМИ ТЕКСТОВ БИБЛИИ, КОРАНА, ТАНАХА (СВЯЩЕННОЕ ПИСАНИЕ ИУДАИЗМА) И ГАНДЖУРА (БУДДИЙСКИЙ КАНОН)

Не так страшен бес, как тот, кто его видел.

23 ноября 2015 г. Президент Российской Федерации В. В. Путин подписал закон о запрете на признание экстремистскими священных текстов мировых религий. Таким образом, в закон о противодействии экстремистской деятельности внесена ст. 3.1 «Особенности применения законодательства Российской Федерации о противодействии экстремистской деятельности в отношении религиозных текстов", которая звучит следующим образом: «Библия, Коран, Танах и Ганджур, их содержание и цитаты из них не могут быть признаны экстремистскими материалами».

Однако, как следует из сообщений новостных лент множества российских источников, в первых числах декабря 2019 года, широкой общественности стало известно о том, что убийство девятилетнего Давида в Екатеринбурге, пожалуй, никогда бы не раскрылось, если бы не звонок с неизвестного номера на горячую линию «Ребенок в опасности», что в лесопарке «Юго-Запад» во влажной земле лежит труп мальчика. Там полицейские обнаружили тело ребенка, завернутое в простыню. Правоохранительным органам удалось установить, что причиной смерти стало удушение от перекрытия дыхательных путей. Звонок поступил 28 ноября, а второго декабря в Уфе на вокзале задержали сорокалетнего предполагаемого убийцу Ивана Казанцева и 48-летнюю Земфиру Гайнуллину – одного из членов и лидера странствующей христианской харизматической секты. Казанцева обвинили в умышленном убийстве несовершеннолетнего, Гайнуллину – в пособничестве убийце.

При восстановлении картины происходящего установлено, что у мальчика во рту был кляп, а на теле видны следы, предположительно нанесенные плеткой. Перед смертью Давида били плетью, проводя церемонию экзорцизма – «изгнания бесов», а, чтобы он не кричал, засунули в рот кляп. Мальчик скончался от удушья, его тело бросили в парковой зоне, присыпав его землей и листьями. Труп лежал непогребенным предположительно с конца октября – начала ноября.

Новостные источники также активно повествуют о других аналогичных случаях. Жительница одного из городов на северо-востоке Подмосковья задушила своего сына при попытке изгнать из него бесов. Другая 29-летняя женщина избивала сына клюшкой и вколола 12-летнему мальчику димедрол для того, чтобы изгнать из него бесов.

Врач высшей категории Гуарша Абдулатипова, заведующая седьмым женским отделением психоневрологического диспансера Республики Дагестан в интервью корреспонденту РИА «Новости»: «К нам приводят пациентов, которые уже побывали у всех знахарей, по всем святым местам проехались, из них даже джиннов пытались изгнать. У нас такие случаи происходили неоднократно: к нам привозили больного, который был весь избит, тело в гематомах – оказывается, это родственники возили его изгонять джиннов. А в итоге пациент оказывается у нас – мы для родственников последняя инстанция: когда уже ничего не помогает, привозят его к нам».

Следует отметить, что под экзорцизмом понимают обычай или обряд в рамках различных религий и верований, состоящий в изгнании из человека (или места) бесов, джиннов или другой вселившейся в них «силы», путем принуждения одержимого лица к прочтению молитвы или иного ритуала той или иной степени сложности.

Одним из основных источников формирования таких представлений и оправдания совершения подобных экстремистских действий является Библия, в которой приводится несколько примеров людей, якобы одержимых бесами или находящихся под их воздействием. Из них можно выделить определенные симптомы «демонического воздействия», а также получить представление о том, как демон явно владеет человеком. Также можно ознакомиться с примерами ритуалов «изгнания бесов» из человека. Вот некоторые библейские тексты: Матфея 9:32-33; 12:22; 17:18; Марка 5:1-20; 7:26-30; Луки 4:33-36; 22:3; Деяния 16:16-18. В некоторых случаях, описанных в этих стихах, одержимость приводила к физическим недугам, выраженным в потере дара речи, эпилептических симптомах, слепоте и пр. В других случаях она побуждала человека к плохим поступкам (Иуда – главный пример). В Деяниях 16:16-18 дух дал служанке способность знать о вещах, выходящих за рамки ее собственных познаний. Бесноватый из земли Гадаринской, «одержимый» множеством демонов, якобы владел сверхчеловеческой силой, ходил нагим и обитал среди могил. Согласно текстам писания, злым духам было позволено беспокоить царя Саула, восставшего против Господа, что проявлялось в депрессивном настроении и навязчивом желании убить Давида (1 Царств 16:14-15; 18:10-11; 19:9-10).

Пункт 3 ст. 1 Федерального закона от 25 июля 2002 года № 114-ФЗ «О противодействии экстремистской деятельности» определяет понятие «экстремистские материалы», а ст. 13 данного Федерального закона устанавливает порядок и последствия признания информационных материалов экстремистскими.

В соответствии с п. 3 ст. 1 данного Федерального закона к экстремистским материалам относятся в том числе предназначенные для обнародования информационные материалы:

– призывающие к осуществлению экстремистской деятельности;

– обосновывающие необходимость осуществления экстремистской деятельности.

В качестве вывода из вышеизложенного материала следует отметить то, что закон о запрете на признание экстремистскими священных текстов мировых религий является противоречащим понятию «экстремизм» и способствует совершению преступлений, суть которых изложена в начале данной статьи.

Сборник материалов
Всероссийской научно-практической конференции
«Противодействие экстремизму и терроризму
в информационных системах» 3 декабря 2019 г.

Противодействие терроризму и экстремизму в информационных системах

Научное электронное издание

Компьютерная верстка *Фомин И. Е.*
3,27 усл. печ. л.

Систем. требования: CPU 1,5 Гц; RAM 512 Мб; Windows XP SP3;
1 Гб свободного места на жестком диске.
Подписано к изданию 26.12.2019 г.

ISBN 978-5-9694-0825-8

Московский университет МВД России имени В.Я. Кикотя
117997, г. Москва, ул. Академика Волгина, д. 12