

УДК 343.326

*Шаров Руслан Александрович,
обучающийся Университета «Синергия», 1 курс,
Россия, г. Тула, e-mail: ruslan.sharoff@mail.ru
Научный руководитель: И.С. Лапшин*

**О НЕКОТОРЫХ СОВРЕМЕННЫХ ТЕНДЕНЦИЯХ
ПРЕСТУПЛЕНИЙ ЭКСТРЕМИСТСКОЙ И ТЕРРОРИСТИЧЕСКОЙ
НАПРАВЛЕННОСТИ**

***Аннотация.** Статья посвящена некоторым современным тенденциям, наблюдаемым в сфере преступлений террористической и экстремистской направленности, в частности, проблематике вовлечения в такие преступления несовершеннолетних лиц, а также вопросу анонимизации в интернете и основных проблемных аспектов, влияющих на профилактику такой преступности и правоприменение, вопросу информатизации общества и использованию соцсетей и мессенджеров как площадки для поиска исполнителей преступлений террористической и экстремистской направленности.*

***Ключевые слова:** цифровое пространство, соцсети, вовлечение, терроризм, экстремизм.*

*Sharov Ruslan Aleksandrovich,
1st year student at the Synergy University,
Russia, Tula, email: ruslan.sharoff@mail.ru
Scientific adviser: I.S. Lapshin*

**ON SOME CONTEMPORARY TRENDS IN EXTREMIST AND
TERRORIST CRIMES**

***Abstract.** This article examines some current trends observed in terrorist and extremist crimes, particularly the problem of involving minors in such crimes, as well as the issue of online anonymization and key problematic aspects affecting the prevention of such crimes and law enforcement, the digitalization of society, and the use of social media and instant messaging apps as a platform for identifying perpetrators of terrorist and extremist crimes.*

***Keywords:** digital space, social media, involvement, terrorism, extremism.*

Мы живём в эпоху новейшего, информационного общества. Это накладывает свой отпечаток на многие сферы жизни – включая и незаконные общественные отношения.

Преступность в новом мире имеет свои особенные тенденции, в том числе, и особенно, преступность террористической направленности.

В определённом смысле сейчас лучшее время для существования преступных сообществ, занимающихся террористической деятельностью. Да, с одной стороны, в современном мире огромное количество механизмов отслеживания – от камер видеонаблюдения до средств мониторинга интернет-пространства и соцсетей в частности. С другой – сколько существует механизмов противодействия, столько есть и путей их обхода.

Вообще тенденция такова, что преступления террористической направленности всё глубже уходят в цифровое пространство.

С одной стороны, это наблюдается уже довольно давно, с другой – прекращаться, кажется, не собирается. Этому способствует как существования так называемых «глубинных уровней» сети Интернет, в частности, darknet, так и удобство, собственно, методов. Та же криптовалюта, механизмы регулировки которой до сих пор не отлажены, предоставляет широкий спектр возможностей для преступной деятельности.

А если говорить об анонимности в интернете, то становится понятно, почему эти методы пользуются популярностью. Да, мы знаем, что отследить, по сути, можно кого угодно, но совершенствование путей обхода и маскировки, использование VPN и прокси-серверов, а также возможностей искусственного интеллекта значительно увеличивает для организаторов возможность остаться в тени.

В настоящее время, особенно в условиях проведения специальной военной операции, когда подрывная деятельность внутри страны противника особенно востребована, мы видим взрывной рост преступлений террористической направленности, связанной, в том числе, с посягательствами на объекты транспортной безопасности, а также преступлений экстремистской направленности.

Причём речь идёт именно о вовлечении граждан, не имеющих стойкой цели и стремления к совершению террористического акта или осуществлению экстремистской деятельности, в таковые.

По сути, схема вовлечения низового звена исполнителей преступления проста, изящна и действенна. Подростки, люди в трудной жизненной ситуации и просто те, кому по каким-либо причинам срочно нужно большое количество денег, охотно идут на такую «работу», тем более что вакансии активно распространяются в социальных сетях и мессенджерах – за совершение преступных действий обычно предлагают плату. Причём иногда для распространения информации опять же привлекаются технологии, в частности, боты, осуществляющие рассылку максимальному числу пользователей. Впрочем, нередкий случай и связь с реальным, максимально анонимизированным лицом, которое, при этом, тоже является исполнителем, просто чуть более высокого порядка.

Примечательно, что наблюдается рост числа исполнителей именно со стороны молодёжи. Вероятно это связано как с общим чувством безнаказанности, характерным для многих несовершеннолетних, так и с их

активным присутствием в интернет-пространстве, где они легко попадают в поле зрения преступных сообществ, ищущих рабочую силу.

Важно при этом отметить, что низовое звено в таких схемах является, в общем, расходным материалом, за который не держатся. Исполнители непосредственного преступления, как правило, не знают даже, от кого получают задание, и их поимка никак не сказывается на преступном сообществе в целом, а цель при этом, даже пусть и мелкая, оказывается достигнута.

Вообще автоматизация процессов, бесконтактность и лёгкое отношение к вероятной (очень вероятной) потере исполнителя и являются причинами, по которым схемы вовлечения в преступную деятельность только расширяются. Роль играет и малоопытность подростков, которых, как мы упоминали, активно вовлекают в преступную деятельность – можно отследить, как часто в последнее время появляются новости об очередном несовершеннолетнем, совершившем, например, поджог релейного шкафа на железнодорожном объекте.

Вопрос о необходимости запрета на использование лицами, не достигшими определённого возраста, социальных сетей, является спорным и не входит в сферу нашего исследования, однако имеет определённое значение, в чём можно убедиться на приведённых нами примерах.

Несовершеннолетние используют социальные сети и мессенджеры – это объективная действительность. Причём начинают пользование ими примерно с возраста шести-восьми лет, то есть, приблизительно с момента поступления в школу. С одной стороны, это оправдано необходимостью поддерживать связь с одноклассниками. Кроме того, Интернет, в том числе социальные сети и мессенджеры, являются площадкой, на которой размещается информация о проведении различных развлекательных и научных мероприятий, в которых ребёнок может изъявить желание участвовать.

С другой стороны, бесспорно и очевидно, что пользователями сетей являются не только дети. И не только законопослушные взрослые. В местах скопления большого количества пользователей, увы, уже почти неизбежно пересечение подростка и лица, осуществляющего преступную деятельность.

Да, можно отметить, что взрослые и пожилые люди часто вовлекаются в совершение преступлений такого рода и через телефонную связь, и иными путями, однако подростки и молодые взрослые в возрасте 18-30 лет гораздо больше присутствуют именно в информационном пространстве. В качестве примера можно вспомнить резонансное дело об убийстве военкора Владлена Татарского, совершённое на тот момент двадцатипятилетней Треповой, которая, по версии следствия, действовала в соответствии с указаниями, полученными от неких лиц, реальное имя одного из которых даже неизвестно[1].

Сама Трепова при этом утверждала, что думала, будто в статуэтке, в которой оказалось взрывное устройство, только устройство для прослушки.

И здесь мы говорим о совершеннолетнем человеке, имеющим какой-никакой жизненный опыт. Если же рассматривать подростков, которые, хоть и получают более простые «задания», как правило, но, тем не менее, в зависимости от ситуации и конкретных действий могут оказаться участниками реально террористического акта, то понятно, почему схема работает.

Кроме того, существует целый пласт преступлений, которые в принципе совершаются в сети Интернет. В первую очередь, конечно, речь о призывах и пропаганде, предусмотренных ст. 205.2 и ст. 280-280.4 Уголовного кодекса Российской Федерации (УК РФ). Здесь спектр возможностей как преступных сообществ, так и отдельных лиц, не всегда даже осознающих общественную опасность своих действий, расширяется кратно.

Кибертерроризм до сих пор находится в подвешенном состоянии, не имея чёткой дефиниции, хотя нормы, регламентирующие его компоненты, содержатся в УК РФ. С одной стороны, область применения этого понятия понятна: информационное пространство, с другой – он крайне многообразен, принимает разные формы и существует в огромном количестве различных областей: от диверсионной деятельности до устранения конкуренции крупными компаниями. Из-за этого дифференциация понятия действительно усложняется[2].

Что касается правоприменения, то, как мы уже отмечали, самая большая проблема – анонимность и возможность скрыться в сети. Да, исполнители, безусловно, несут свою часть вины за совершение преступлений. Однако нам видится куда более важной задачей поиск непосредственных организаторов преступной деятельности, особенно когда участниками этой деятельности становятся уязвимые слои населения, включая несовершеннолетних.

Таким образом, сеть Интернет на данный момент является одним из основных полей организации террористической и экстремисткой деятельности, а также вовлечения в эту деятельность граждан, особенно несовершеннолетних.

Видится, что единственным методом противостояния этому развитию является не столько работа, проводимая в отношении конечных исполнителей, сколько совершенствование методов работы в цифровом пространстве, поскольку гораздо более сложной и важной задачей по-прежнему можно считать поиск именно организаторов, которые зачастую остаются не только не пойманными, но даже не признанными.

Также спорным остаётся вопрос о присутствии несовершеннолетних в «общем Интернете». Мы не готовы утверждать, что запрет на использование детьми до какого-то возраста мессенджеров и соцсетей даст немедленный положительный результат. Скорее, дело снова должно

сводиться к устранению угрозы их вовлечения – то есть, организаторов преступных сообществ или хотя бы среднего звена рекрутеров.

Литература

1. СКР переквалифицировал дело об убийстве Владлена Татарского на теракт [Электронный ресурс]. URL: <https://www.kommersant.ru/doc/5913505> (дата обращения: 30.01.2026).

2. Попова Е. А., Кузнецова И. С. Экстремизм и терроризм в сети Интернет как преступления в сфере компьютерной информации мирового масштаба [Электронный ресурс] // CyberLeninka : [сайт]. URL: <https://cyberleninka.ru/article/n/istoriya-razvitiya-instituta-konfiskatsii-imuschestva> (дата обращения: 30.01.2026).