Вестник Сибирского юридического института МВД России

УДК 343.97

DOI 10.51980/2542-1735_2023_3_196

Никита Андреевич ИЛЬИНЫХ,
адъюнкт Омской академии МВД России
nikitailinyh491@yandex.ru

СТРУКТУРА, УРОВЕНЬ И ДИНАМИКА КИБЕРЭКСТРЕМИЗМА В РОССИЙСКОЙ ФЕДЕРАЦИИ

STRUCTURE, LEVEL AND DYNAMICS OF CYBER EXTREMISM IN THE RUSSIAN FEDERATION

Статья посвящена изучению структуры, уровня и динамики экстремистских преступлений, совершаемых с использованием возможностей информационно-телекоммуникационных технологий (киберэкстремизм). Исследование основано на анализе материалов судебных решений и актуальных статистических данных. Сделаны выводы о том, какую часть составляют киберэкстремистские преступления в общей совокупности преступлений экстремистской направленности, а также о высоком уровне латентности отдельных киберэкстремистских преступлений. Определены категории населения, представители которых наиболее часто осуществляют публичные призывы к экстремистской деятельности в киберпространстве. Предложены рекомендации по использованию результатов исследования для противодействия экстремизму в России.

The article is devoted to the study of the structure, level and dynamics of extremist crimes committed using the capabilities of information and telecommunication technologies (cyber extremism). The research is based on the analysis of materials of court decisions and up-to-date statistics. Conclusions are drawn about the proportion of cyber extremist crimes in the total number of extremist crimes, as well as about the high level of latency of particular cyber extremist crimes. The categories of the population whose representatives most often publicly call for extremist activities in cyberspace are identified. Recommendations on using the results of the study to counter extremism in Russia are given as well.

Ключевые слова: криминология, экстремизм, статистика, информационно-телекоммуникационные технологии.

Keywords: *criminology, extremism, statistics, information and telecommunication technologies.*

Сегодня крайне актуальной становится проблема противодействия таким наиболее общественно опасным преступлениям, как экстремистские. Согласно официальной статистике ГИАЦ МВД России, в период с 2019 по 2022 гг. наблюдается постоянный рост числа преступлений указанного вида: в 2019 г. их совершено 585; 2020 г. – 833; 2021 г. – 1057; 2022 г. – 1566. Данную проблему в своих исследованиях отмечают П.В. Тепляшин [14], Ю.В. Леонтьева и О.А. Овчинко [9], И.Л. Морозов и А.Э. Абрамов [12], А.М. Алхастов [3] и др.

Еще большую актуальность данная проблема приобрела в 2022 году. Прослеживается тенденция к значительному увеличению числа экстремистских преступлений, что отчетливо видно из анализа статистических

данных, характеризующих географию данного вида преступности. Отмечается резкий рост числа экстремистских преступлений в столичных городах и приграничных с вновь присоединенными по итогам референдума 30 сентября 2022 г. южными субъектами Российской Федерации. В Москве с января по декабрь 2022 г. были зарегистрированы 280 таких преступлений, тогда как за аналогичный период 2021 г. – 59, прирост составил свыше 474%. Схожая ситуация наблюдается и в Санкт-Петербурге (+387%). Резкий рост числа преступлений указанного вида по итогам 2022 г. наблюдается в Республике Крым (+313%), Ростовской области (+247%) и Ставропольском крае (+187%). При этом в Республике Дагестан, которая исторически была лидером в этом отношении, число таких преступлений даже снизилось (-3,6%) [4].

Помимо вышеуказанного сегодня наблюдается тенденция к усилению роли средств информационно-телекоммуникационных технологий (далее – ИТТ) в совершении всех видов преступлений. В январе-декабре 2022 г. были зарегистрированы 522,1 тыс. преступлений, совершенных с использованием ИТТ, что на 0,8% больше чем в 2021 г. Увеличился и удельный вес таких преступлений в общем числе зарегистрированных преступлений (с 25,8% до 26,5%). Согласно статистическим данным ГИАЦ МВД России, почти три четверти (72,8%) киберпреступлений совершаются с использованием сети Интернет (342,5 тыс.; +1,9%), более трети (40,4%) – с помощью средств мобильной связи (190,1 тыс.; -5,6%)[1].

С учетом повсеместного использования преступниками возможностей ИТТ значительной трансформации подвергся и способ совершения преступлений экстремистской направленности. По заявлению судьи Верховного Суда РФ Е.В. Пейсиковой, в 2020 г. до 90% осужденных за публичные призывы к осуществлению экстремистской деятельности использовали в своей деятельности возможности сети Интернет[2]. Стремительное развитие возможностей ИТТ и всеобщая вовлеченность граждан в их использование создают благоприятную почву для преступников, распространяющих экстремистскую идеологию. Кроме того, при помощи современных технологий преступники активно организуют свою деятельность, а также осуществляют ее финансирование. Тенденцию к росту количества экстремистских преступлений с использованием возможностей ИТТ в своих исследованиях отмечают В.Ю. Мельников [11], О.В. Обернихина [13], Д.А. Акимова [2], В.Н. Макашова и Е.В. Чернова [10], Г.И. Узембаева [15] и др. Кроме того, все большую актуальность приобретает проблема резкого роста числа экстремистских преступлений, связанных с публичным распространением фейковой информации об использовании Вооруженных Сил РФ. При этом, как отмечает А.М. Абдулатипов, ключевую роль в данном процессе играет именно использование экстремистами возможностей социальных сетей и иных средств ИТТ [1].

Указанный факт в совокупности с высокой степенью общественной опасности экстремистских преступлений, совершаемых указанным способом, позволяет утверждать о необходимости выделить такие деяния в отдельную категорию – киберэкстремистские преступления (киберэкстремизм). Однако в связи с отсутствием в нормативных правовых актах закрепленного точного перечня экстремистских преступлений, а также с наличием множества различных мнений исследователей по данному вопросу охарактеризовать структуру киберэкстремизма путем определения соответствующего исчерпывающего списка преступлений на данный момент не представляется возможным.

Тем не менее, на наш взгляд, в структуре киберэкстремизма можно выделить следующие категории составов преступлений, обязательным признаком которых является

1 Министерство внутренних дел Российской Федерации. Состояние преступности в Российской Федерации. URL: https://xn--b1aew.xnp1ai/reports/item/28021552 (дата обращения:19.02.2023)

2 Более 40% осужденных за экстремизм получили приговоры за призывы в Интернете // Российская газета. URL: https://rg.ru/2021/10/28/bolee-40-osuzhdennyh-za-ekstremizm-poluchili-prigovory-za-prizyvy-v-internete.html (дата обращения: 29.02.2023).

специфический способ их совершения, а именно использование средств ИТТ:

– экстремистские преступления, связанные с искажением информации в противоправных целях (п. «д» ч. 2 ст. 207.3 УК РФ, п. «в» ч. 2 и ч. 4 ст. 354.1 УК РФ) или с ее использованием в любых формах для распространения экстремизма (ч. 2 ст. 280 УК РФ, ч. 2 ст. 280.1 УК РФ, ст. 282 УК РФ);

– организация экстремистского сообщества и участие в его деятельности (ст. 282.1 УК РФ и ст. 282.2 УК РФ);

– преступления, связанные с финансированием экстремистской деятельности (ст. 282.3 УК РФ).

Указанные категории выделены на основе анализа материалов 103 судебных решений по преступлениям экстремистской направленности за 2020-2022 гг., в большинстве из которых в качестве способа совершения преступления использовались средства ИТТ. Отметим, что совокупность вышеприведенных составов преступлений не образует исчерпывающий список киберэкстремистских преступлений, однако они в целом дают общее представление о структуре данного вида преступности.

Отметим, что на сегодняшний день, согласно официальным статистическим данным ГИАЦ МВД России и Судебного департамента при Верховном Суде РФ, наиболее часто совершаемыми киберэкстремистскими преступлениями являются деяния, предусмотренные ч. 2 ст. 280 УК РФ (публичные призывы к осуществлению экстремистской деятельности, совершенные с использованием информационно-телекоммуникационных сетей или СМИ). В 2022 г. удельный вес данных преступлений составил 30,2% от всей совокупности зарегистрированных преступлений экстремистской направленности (473 из 1566). Данный показатель остается стабильно высоким на протяжении последних лет: 2019 г. – 44%, 2020 г. – 40%, 2021 г. – 43% (диаграмма 1).

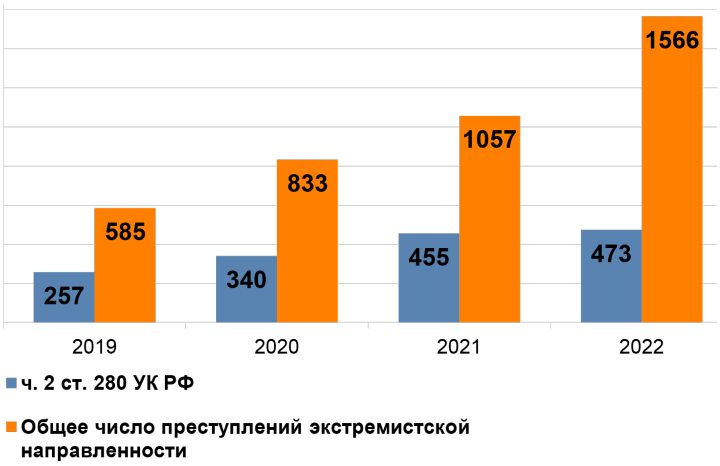

Диаграмма 1. Доля публичных призывов к осуществлению экстремистской деятельности с использованием ИТТ в общей совокупности экстремистских преступлений

В ходе проведенного анализа судебной практики по данным преступлениям удалось выявить наиболее часто используемые экстремистами средства ИТТ. Установлено, что для указанных целей преступники наиболее часто использовали социальные сети «ВКонтакте», «Одноклассники», «Instagram» и «Facebook» (диаграмма 2).

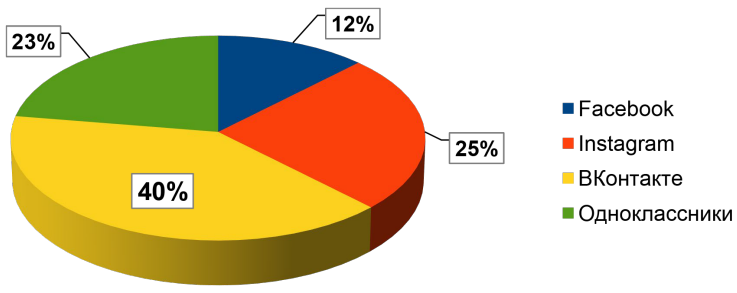

Диаграмма 2. Социальные сети, используемые для распространения экстремистских материалов и привлечения новых последователей)

На наш взгляд, приоритет отечественных социальных сетей для преступников обусловлен их наибольшей популярностью среди граждан России.

Однако сфера применения преступниками средств ИТТ не ограничивается исключительно осуществлением призывов к экстремистской деятельности.

На основе материалов судебной практики установлено, что новые возможности средств ИТТ активно используются экстремистами для организации и финансирования своей деятельности, а также для связи между собой. Для организации деятельности и связи экстремисты активно используют возможности мессенджеров с защищенными протоколами шифрования сообщений («Open Whisper Signal» у WhatsApp и «MTProto» у «Telegram»). Для финансирования экстремистской деятельности все чаще используются анонимные средства платежа (криптовалюта).

Кроме того, характеризуя способ совершения киберэкстремистских преступлений, следует отметить активное использование злоумышленниками средств ИТТ, позволяющих им скрывать свою личность и местоположение. В качестве примера такой технологии можно привести VPN (Virtual Private Network). Данная технология позволяет устанавливать защищенное соединение между устройством пользователя и Интернетом. Она шифрует данные, которые передаются через Интернет, и маскирует пользовательский IP-адрес, скрывая тем самым местоположение пользователя. В результате снижается эффективность деятельности правоохранительных органов по выявлению указанных преступлений и лиц, их совершающих. По нашему мнению, данный факт может свидетельствовать о высоком уровне латентности экстремистских преступлений, совершаемых с использованием ИТТ.

Характеризуя структуру лиц, совершивших указанные виды преступлений, отметим, что прослеживается тенденция к уменьшению количества преступлений, совершенных лицами в возрасте 18-29 лет. По состоянию на первое полугодие 2022 г. удельный вес осужденных по ч. 2 ст. 280 УК РФ лиц в указанной возрастной категории составил 32%. За аналогичный период 2021 г. данное значение составляло 42%. В научном исследовании И.В. Бурова содержится информация о том, что в 2018 г. в 57% случаев указанные преступления совершались молодыми людьми до 30 лет [5]. Д.Н. Еремин отмечает, что по состоянию на 2011 г. доля молодых людей, совершивших экстремистские преступления в Интернете, составляла 70% [6]. Таким образом, можно говорить об уменьшении количества лиц в возрасте до 30 лет, осуществляющих публичные призывы к экстремистской деятельности с использованием ИТТ, и увеличении их в возрастной категории от 30 до 49 лет. При этом в качестве главной цели своего деструктивного воздействия такие преступники чаще всего выбирают молодых людей в возрасте 18-29 лет.

Далее приведем еще ряд немаловажных фактов, характеризующих личность киберэкстремиста, на основе статистических данных Судебного Департамента Верховного Суда РФ. Установлено, что лица, осужденные за экстремизм с использованием ИТТ, чаще всего имеют среднее профессиональное (39,2%) или среднее общее образование (25,5%). Как правило, указанные виды преступлений совершаются людьми без постоянной работы (52,5%) либо представителями рабочих профессий (35,6%).

Традиционно доля указанных преступлений, совершаемых женщинами, является небольшой (в 2022 г. – 8,8%). Однако по сравнению с данными 2021 г. (5,7%) наблюдается увеличение показателя.

Подавляющее большинство осужденных за кибеэкстремистские преступления являются постоянными жителями данной местности (94,4%). Для сравнения: доля экстремистских преступлений, совершаемых без использования ИТТ постоянными жителями (на примере ч. 1 ст. 280 УК РФ), достигает 100%. Однако возможности ИТТ позволяют распространять экстремистскую идеологию из любой точки мира, чем активно пользуются злоумышленники. Кроме того, как отмечают В.В. Меркуев и О.В. Боброва, сегодня в указанных процессах растет роль экстремистских организаций, курируемых недружественными странами [4]. По нашему мнению, выявление их представителей и привлечение к уголовной ответственности в силу целого ряда технических и организационных проблем на сегодняшний день крайне затруднительно, что не может не отражаться на статистических данных.

Таким образом, установлено, что за последний год преобладающим мотивом совер-

шения экстремистских преступлений вместо религиозного стал политический. Кроме того, наблюдается и резкое изменение в географии указанного вида преступности. Наиболее криминогенными стали приграничные с территорией Украины южные регионы России, а также столичные города. При планировании противодействия экстремизму следует обращать наиболее пристальное внимание на сложившуюся ситуацию.

Результаты исследования показали, что использование средств ИТТ играет все большую роль в совершении преступлений экстремистской направленности. Установлено, что подавляющее большинство данных преступлений так или иначе совершаются с использованием средств ИТТ. Наиболее часто встречающимся на данный момент являются преступления, связанные с публичными призывами к осуществлению экстремистской деятельности с использованием средств ИТТ, а также деяния, связанные с распространением определенной фейковой информации в киберпространстве.

Отметим, что новые возможности современных технологий позволяют экстремистам наиболее эффективно и анонимно организовывать свою деятельность (ст. 282.1 УК РФ и ст. 282.2 УК РФ) и осуществлять ее финансирование (ст. 282.3 УК РФ). К тому же полагаем, что в результате использования экстремистами особенностей функционирования отдельных технологий значительное количество указанных преступных деяний остаются скрытыми от правоохранительных органов. Данный факт может свидетельствовать о высоком уровне латентности отдельных киберэкстремистских преступлений.

В результате исследования также установлено изменение среднего возраста совершения киберэкстремистских преступлений. Прослеживается тенденция к ежегодному снижению доли указанных преступлений, совершаемых молодыми людьми в возрасте 18-29 лет. В 2022 г. свыше 62% указанных деяний совершались людьми в возрасте 30-49 лет. Молодежь по-прежнему остается наиболее подверженной воздействию экстремистских идей, к тому же они наиболее активно используют в повседневной жизни мессенджеры, социальные сети и другие инструменты ИТТ, чем активно пользуются экстремисты более старшего возраста. О том, что молодежь сегодня активно вовлекается в экстремистскую деятельность, свидетельствуют результаты многочисленных научных исследований. Данная проблема по-прежнему актуальна, и ее решение требует дальнейшей научной проработки. Вместе с тем считаем, что при разработке мер профилактики и предупреждения киберэкстремизма необходимо уделять больше внимания населению средней возрастной категории, поскольку преступники именно указанного возраста наиболее часто осуществляют публичные призывы к экстремистской деятельности в киберпространстве, избирая своей целью молодых людей.

Библиографический список

1. Абдулатипов, А.М. Уголовно-правовая характеристика публичного распространения под видом достоверных сообщений заведомо ложной информации, содержащей данные об использовании Вооруженных сил Российской Федерации в целях защиты интересов Российской Федерации и ее граждан, поддержания международного мира и безопасности / А.М. Абдулатипов // Юридический вестник Дагестанского государственного университета. – 2022. – N 2. – С. 121-126.

2. Акимова, Д.А. Современные каналы формирования и распространения идей экстремизма и терроризма в молодежной среде / Д.А. Акимова // Экстремизм и терроризм в киберпространстве: угрозы миру и безопасности человечества : сборник статей по итогам III Всероссий-

ской студенческой научно-практической конференции. – Барнаул: Алтайский государственный университет, 2020. – С. 98-105.

3. Алхастов, А.М. Актуальные проблемы молодежного экстремизма: юридический анализ, современные способы противодействия / А.М. Алхастов // Юридическая наука. – 2022. – N 7. – С. 130-134.

4. Боброва, О.В. Радикальные религиозные организации угроза национальной безопасности и средства противодействия им / О.В. Боброва, В.В. Меркурьев // Обозреватель. – 2022. – N 10. – С. 106-126.

5. Буров, И.В. Криминалистическая характеристика личности преступника-экстремиста в Интернете / И.В. Буров // Вестник науки. – 2019. – N 1. – С. 57-60.

6. Еремин, Д.Н. Применение дерматоглифических исследований в решении следственных задач при расследовании преступлений, связанных с экстремизмом / Д.Н. Еремин // Вестник Балтийского федерального университета им. И. Канта. – 2011. – N 9. – С. 138-142.

7. Клейменов, М. П. Криминология в современном мире / М.П. Клейменов, И.М. Клейменов // Криминологический журнал Байкальского государственного университета экономики и права. – 2011. – N 1. – С. 5-13.

8. Куликов, Е.А. Цифровой экстремизм: общее, особенное и единичное / Е.А. Куликов // Экстремизм и терроризм в киберпространстве: угрозы миру и безопасности человечества : сборник статей по итогам III всероссийской студенческой научно-практической конференции. – Барнаул: Алтайский государственный университет, 2020. – С. 11-13.

9. Леонтьева, Ю.В. Экстремизм в России: цифры и размышления / Ю.В. Леонтьева, О.А. Овчинко // Вестник Сибирского юридического института МВД России. – 2020. – N 3. – С. 133-140.

10. Макашова, В.Н. Информационные технологии как фактор распространения идей киберэкстремизма в молодежной среде / В.Н. Макашова, Е.В. Чернова // Современные информационные технологии и ИТ-образование. – 2013. – N 9. – С. 328-335.

11. Мельников, В. Ю. Преступления экстремистской направленности в Российской Федерации / В.Ю. Мельников // Журнал юридических исследований. – 2020. – Т. 5. – N 2. – С. 14-22.

12. Морозов, И.Л. Государственная стратегия противодействия экстремизму в современной России / И.Л. Морозов, А.Э. Абрамов // Общество: политика, экономика, право. – 2020. – N 8. – URL: https://cyberleninka.ru/article/ngosudarstvennaya-strategiya-protivodeystviya-ekstremizmu-v-sovremennoyrossi (дата обращения: 03.03.2023).

13. Обернихина, О.В. Криминологическая характеристика киберэкстремистской преступности в России и способы ее профилактики / О.В. Обернихина // Экстремизм и терроризм в киберпространстве: угрозы миру и безопасности человечества : сборник статей по итогам III всероссийской студенческой научно-практической конференции. – Барнаул: Алтайский государственный университет, 2020. – С. 29-34.

14. Тепляшин, П.В. Криминологические аспекты идеологии молодежного терроризма в информационно-телекоммуникационных сетях / П.В. тепляшин // Актуальные проблемы противодействия терроризму и экстремизму: история, современное состояние, перспективы : сборник научных статей всероссийской научно-практической конференции с международным участием.– Новосибирск: Новосибирский военный институт имени генерала армии И.К. Яковлева войск Национальной гвардии Российской Федерации, 2017. – С. 208-212.

15. Узембаева, Г.И. Преступления экстремистской направленности, совершаемые с использованием средств массовой информации либо информационно-телекоммуникационных сетей : автореф. дис. … канд. юрид. наук / Г.И. Узембаева. – М., 2016. – 24 с.