

Федеральное государственное казенное образовательное учреждение
высшего образования
«Омская академия Министерства внутренних дел Российской Федерации»

На правах рукописи



Ильиных Никита Андреевич

**КРИМИНОЛОГИЧЕСКАЯ ХАРАКТЕРИСТИКА И ПРЕДУПРЕЖДЕНИЕ
ПРЕСТУПЛЕНИЙ ЭКСТРЕМИСТСКОЙ НАПРАВЛЕННОСТИ,
СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-
ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ**

Специальность 5.1.4. Уголовно-правовые науки

ДИССЕРТАЦИЯ

на соискание ученой степени

кандидата юридических наук

Научный руководитель:
Заслуженный работник высшей
школы Российской Федерации,
доктор юридических наук,
профессор
Бабурин Василий Васильевич

Омск 2025

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ	3
ГЛАВА 1. ПОНЯТИЕ И КРИМИНОЛОГИЧЕСКАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ ЭКСТРЕМИСТСКОЙ НАПРАВЛЕННОСТИ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО- ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ.....	18
§ 1. Понятие и сущность киберэкстремизма в современной России	18
§ 2. Состояние киберэкстремистской преступности. Структура и тенденции преступлений экстремистской направленности, совершаемых с использованием информационно-телекоммуникационных технологий	37
§ 3. Криминологическая характеристика личностей киберэкстремистов и их влияние на формирование экстремистских воззрений у населения	61
ГЛАВА 2. ПРЕДПОСЫЛКИ УГОЛОВНОГО КИБЕРЭКСТРЕМИЗМА И ЕГО ПРЕДУПРЕЖДЕНИЕ В РОССИЙСКОЙ ФЕДЕРАЦИИ.....	89
§ 1. Объективные и субъективные предпосылки совершения преступлений экстремистской направленности посредством использования информационно- телекоммуникационных технологий.....	89
§ 2. Обеспечение информационно-психологической безопасности граждан как мера нивелирования деструктивного информационно-психологического воздействия и предупреждения киберэкстремистских преступлений	110
§ 3. Организационно-тактические и технические меры по предупреждению преступлений экстремистской направленности, совершаемых с использованием информационно-телекоммуникационных технологий	139
ЗАКЛЮЧЕНИЕ.....	163
СПИСОК ЛИТЕРАТУРЫ	171
ПРИЛОЖЕНИЯ	198

ВВЕДЕНИЕ

Актуальность темы исследования. Сегодня продолжается тенденция всеобщей цифровизации большинства сфер жизни российского общества. Все больше людей ежедневно используют информационно-телекоммуникационные технологии (далее – ИТТ). Согласно официальным данным Федеральной службы государственной статистики сегодня 90,4% граждан имеют доступ к сети Интернет. В связи с этим, несмотря на очевидные преимущества от использования ИТТ, возникают и новые криминальные угрозы, характеризующиеся существенной трансформацией преступности в результате активного применения новых технологий для совершения преступлений. По официальным статистическим данным Главного информационно-аналитического центра Министерства внутренних дел Российской Федерации (далее – ГИАЦ МВД России), каждое четвертое преступление совершается с использованием ИТТ¹.

Значительной трансформации сегодня подвергается и экстремистская преступность. Свыше половины всех преступлений экстремистской направленности совершается с использованием ИТТ. Указанный факт подтверждается официальными статистическими данными ГИАЦ МВД России. За последние 5 лет средний удельный вес данных преступлений, совершенных с использованием ИТТ, составил 56,42% от общей совокупности всех зарегистрированных преступлений экстремистской направленности. Отчетливо прослеживается и рост их общего количества. С 2020 по 2024 гг. темп прироста составил 97,8% – с 473 до 936 зарегистрированных деяний.

Вместе с тем, несмотря на относительно небольшую долю рассматриваемых деяний в общей массе совершаемых в стране преступлений, любой факт проявления экстремизма может повлечь за собой существенные негативные последствия для общественной безопасности. Как справедливо отмечается в Указе Президента Российской Федерации от 28 декабря 2024 г. № 1124 «Об утверждении

¹ Министерство внутренних дел Российской Федерации. Состояние преступности в Российской Федерации. URL: <https://xn--blaew.xnplai/reports/item/28021552> (дата обращения: 19.04.2025).

Стратегии противодействия экстремизму в Российской Федерации», рассматриваемые деяния ведут к нарушению гражданского мира и согласия, основных прав и свобод человека и гражданина; подрывают государственную и общественную безопасность; создают реальную угрозу суверенитету, единству и территориальной целостности Российской Федерации, основам конституционного строя Российской Федерации, а также межнациональному (межэтническому), межконфессиональному единству и гражданскому единению, культурному развитию, политической и социальной стабильности¹.

В свою очередь использование ИТТ при совершении преступлений экстремистской направленности обуславливает ряд специфических особенностей по отношению к традиционным способам их совершения (например, печатная или устная агитация).

В частности, ИТТ позволяют экстремистам в кратчайшие сроки анонимно распространять среди неограниченного круга лиц экстремистские материалы, публикуя их на популярных среди граждан информационных ресурсах. Учитывая высокую вовлеченность населения в использование социальных сетей, мессенджеров и других ИТТ, сегодня граждане регулярно сталкиваются с экстремистскими материалами. Таким образом, на человека в информационно-телекоммуникационном пространстве регулярно оказывается деструктивное информационно-психологическое воздействие, которое направлено на его устрашение или на возбуждение в нем чувства ненависти по отношению к представителям различных социальных групп, объединенных по политическим, религиозным, национальным, или идеологическим признакам. В результате часть граждан приобретают экстремистские взгляды и убеждения, что в свою очередь может стать причиной совершения ими соответствующих преступлений.

Отдельные ИТТ также открывают перед экстремистскими организациями и сообществами новые возможности для быстрой и анонимной организации своей

¹ Об утверждении Стратегии противодействия экстремизму в Российской Федерации до 2030 года: Указ Президента РФ от 28 декабря 2024 г. № 1124. Доступ из справ.-правовой системы «КонсультантПлюс».

деятельности, осуществления ее финансирования, вербовки новых участников и склонения граждан к совершению преступлений экстремистской направленности.

Вместе с тем сегодня существует множество различных позиций относительно того, что следует понимать под экстремизмом, осуществляемым с использованием ИТТ. Одними авторами указанное явление определяется излишне широко, и под ним предлагается понимать совокупность всех деяний, связанных с оборотом любой деструктивной информации в киберпространстве. С другой стороны, нередко в криминологических и уголовно-правовых исследованиях авторы ограничиваются изучением лишь узкого круга преступлений экстремистской направленности, наиболее часто совершаемых с использованием ИТТ. Сложившаяся ситуация отнюдь не способствует определению целостной криминологической характеристики рассматриваемой преступности и препятствует разработке эффективных мер ее предупреждения.

Отдельно необходимо отметить факт постоянного совершенствования как самих ИТТ, так и способов их использования при совершении преступлений экстремистской направленности, что свидетельствует о необходимости своевременного реагирования со стороны как государства в целом, так и правоохранительной системы в частности.

Изложенное указывает на необходимость проведения углубленного комплексного теоретического и практического исследования, направленного на установление существенных признаков киберэкстремизма и криминологической характеристики преступлений экстремистской направленности, совершаемых с использованием ИТТ, определение их детерминирующих факторов, а также разработку рекомендаций по их предупреждению, что и подтверждает актуальность темы диссертационного исследования.

Степень научной разработанности темы исследования.

Изучению криминологической характеристики экстремизма и киберпреступности, их детерминант, личностных особенностей преступников, проблем противодействия данным преступным посягательствам посвящены работы таких ученых,

как Ю. М. Антонян, Я. И. Гилинский, М. Д. Давитадзе, В. В. Лунеев, Е. В. Никульченкова, И. Ю. Сундиев, И. Л. Трунов, Э. Г. Юзиханова и др.

На уровне докторских диссертационных исследований вопросами противодействия экстремизму занимались Р. С. Тамаев («Организация правоохранительной деятельности в сфере противодействия экстремизму», 2010), С. Н. Фридинский («Противодействие экстремистской деятельности (экстремизму) в России: социально-правовое и криминологическое исследование», 2011), А. В. Ростокский («Преступления экстремистской направленности как проявления субкультурных конфликтов молодёжных объединений: уголовно-правовые и криминологические проблемы», 2012), А. В. Петрянин («Противодействие преступлениям экстремистской направленности: уголовно-правовой и криминологический аспекты», 2014).

Противодействие экстремизму в целом и его отдельным видам на уровне кандидатских диссертационных исследований рассматривали А. Г. Хлебушкин («Преступный экстремизм: понятие, виды, проблемы криминализации и пенализации», 2007), Р. О. Кочергин («Противодействие молодежному экстремизму: правовые и криминологические проблемы», 2008), Р. М. Узденов («Экстремизм: криминологические и уголовно-правовые проблемы противодействия», 2008), Е. П. Сергун («Экстремизм в российском уголовном праве», 2009), А. С. Скудин («Правовые меры противодействия экстремизму», 2011), Г. И. Узембаева («Преступления экстремистской направленности, совершаемые с использованием средств массовой информации либо информационно-телекоммуникационных сетей: уголовно-правовая и криминологическая характеристика», 2016), С. В. Криштопов («Уголовно-правовое противодействие преступлениям экстремистской направленности», 2022), Ю. С. Магнутов («Уголовно-правовое противодействие специальным организованным формам экстремистской деятельности (ст. 282.1 и ст. 282.2 УК РФ): теория, техника, практика», 2022), Т. Г. Сироткина («Криминологическая характеристика и предупреждение экстремистской преступности несовершеннолетних», 2024), А. С. Ахметшин («Уголовно-правовое противодействие преступлениям с признаками экстремистской деятельности при

обеспечении основ конституционного строя и безопасности государства», 2025), П. А. Глущенко («Криминологические основы противодействия финансированию экстремистской и террористической деятельности», 2025) и др.

Результаты диссертационных исследований по предупреждению киберпреступности в целом нашли свое отражение в работах Т. Л. Тропиной («Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы», 2005), И. Г. Чекунова («Криминологическое и уголовно-правовое обеспечение предупреждения киберпреступности», 2013), Д. В. Пучкова («Уголовно-правовая модель защиты телекоммуникаций от преступных посягательств», 2022) и др.

Вопросы правового противодействия распространению различной деструктивной информации рассмотрены в рамках исследований О. С. Жуковой («Правовые меры противодействия информационному экстремизму», 2006), Р.В. Упорникова («Политико-правовые технологии противодействия информационному экстремизму в России», 2007) и др.

Объектом диссертационного исследования выступила совокупность общественных отношений, складывающихся в связи с совершением преступлений экстремистской направленности с использованием ИТТ, а также их предупреждением.

Предметом диссертационного исследования является киберэкстремистская преступность, ее состояние и динамика, детерминирующие ее процессы и явления, правовое регулирование и практика предупреждения.

Цель и задачи исследования. *Цель* исследования состояла в получении нового криминологического знания о преступлениях экстремистской направленности, совершаемых с использованием ИТТ, и разработке на данной основе теоретически обоснованных предложений по их предупреждению.

Достижение указанной цели обусловило необходимость постановки и решения следующих *задач*:

- 1) определить сущностные признаки и сформулировать определение киберэкстремизма в России;
- 2) оценить современное состояние киберэкстремистской преступности, ее структуру и современные тенденции;

3) определить криминологическую характеристику личностей киберэкстремистов и оценить их влияние на формирование экстремистских взглядов и убеждений у населения;

4) установить круг объективных и субъективных предпосылок совершения киберэкстремистских преступлений;

5) разработать комплекс мер, направленных на обеспечение информационно-психологической безопасности личности, для предупреждения киберэкстремизма и нивелирования его негативного эффекта;

6) предложить ряд организационно-тактических и технических мер по предупреждению преступлений экстремистской направленности, совершаемых с использованием информационно-телекоммуникационных технологий.

Теоретической основой исследования послужили фундаментальные труды ученых в области криминологии, уголовного права, иных отраслей наук. В работе проанализированы научные воззрения ученых, изложенные в диссертационных и монографических исследованиях, научных статьях, посвященных вопросам определения криминологической характеристики и предупреждения преступлений экстремистской направленности, в том числе совершаемых с использованием ИТТ.

Научная новизна исследования определяется тем, что установлены отличительные признаки экстремистских деяний, совершаемых с использованием ИТТ, позволяющие отделить их от смежных деяний. Сформулировано понятие киберэкстремизма.

В ходе работы представлен подробный обзор современного состояния и тенденций киберэкстремистской преступности в России. Установлены наиболее часто используемые для экстремистской деятельности информационно-телекоммуникационные технологии.

В результате исследования определены категории личностей, наиболее часто совершающих преступления экстремистской направленности с использованием ИТТ. Предложена их авторская классификация.

Установлен ряд объективных и субъективных предпосылок совершения киберэкстремистских преступлений, которые предложено дополнительно классифицировать на внешние и внутренние.

Результатом диссертационного исследования стал комплекс правовых, организационно-тактических и технических мер противодействия деструктивному информационно-психологическому воздействию на население и повышения эффективности деятельности правоохранительных органов по выявлению, прогнозированию и предупреждению киберэкстремистских преступлений путем разработки и внедрения технологий искусственного интеллекта и специального программного обеспечения для автоматизированного поиска информации по открытым источникам данных в киберпространстве.

Теоретическая и практическая значимость исследования определяется тем, что выводы и предложения, изложенные в диссертационном исследовании, дополняют теоретическую базу современной концепции борьбы с преступлениями экстремистской направленности. Определение криминологической характеристики киберэкстремистских преступлений, а также установление их предпосылок вносят существенный вклад в решение проблемы предупреждения указанных деяний и нивелирования их деструктивного информационно-психологического воздействия на население.

Практическое значение результатов настоящего исследования состоит в научно обоснованных рекомендациях и иных исследовательских материалах, которые могут быть использованы правоохранительными органами для своевременного прогнозирования, выявления и предупреждения преступлений экстремистской направленности, совершаемых с использованием ИТТ, а также в законотворческой и научно-исследовательской деятельности, в учебном процессе образовательных организаций высшего образования.

Результаты диссертационного исследования могут применяться в образовательном процессе и использоваться при изучении учебных дисциплин «Криминология» и «Предупреждение преступлений и административных

правонарушений органами внутренних дел», а также при подготовке научных работ и учебно-методических материалов по соответствующей проблематике.

Методология и методы исследования. Достоверность и объективность выводов исследования обеспечена применением диалектического и основанных на нем общенаучных и частнонаучных методов познания.

При определении признаков киберэкстремизма, обосновании его предпосылок, а также мер предупреждения применялся формально-юридический метод (в сочетании с синтезом, индукцией и дедукцией).

Системно-структурный метод и метод анализа позволили классифицировать: совокупность преступлений экстремистской направленности, совершаемых с использованием ИТТ; личностные особенности киберэкстремистов; предпосылки и меры предупреждения киберэкстремистских преступлений.

Такие методы, как статистический (сводка, группировка, статистический анализ) и опрос (в виде анкетирования, интервьюирования), позволили проанализировать состояние, структуру и тенденции киберэкстремистской преступности, определить положительный опыт в предупреждении преступлений экстремистской направленности, совершаемых с использованием ИТТ, а также выделить ключевые проблемы на пути к их эффективному предупреждению.

Положения, выносимые на защиту:

1. В целях дальнейшего совершенствования системы мер предупреждения преступлений экстремистской направленности, совершаемых с использованием ИТТ, предложено авторское определение понятия «киберэкстремизм», под которым понимается социальное, относительно массовое явление, характеризующееся совокупностью запрещенных законом деяний, совершаемых по экстремистским мотивам, с обязательным использованием технологий, моделирующих информационно-телекоммуникационное пространство (киберпространство).

Учитывая специфику киберэкстремистских преступлений, для выработки наиболее эффективных теоретических положений их предупреждения указанные

деяния целесообразно разделить на 2 группы по направленности использования ИТТ для экстремистской деятельности:

а) не связанные с деятельностью экстремистских сообществ и организаций;

б) связанные с деятельностью экстремистских сообществ и организаций.

2. Около двух третей всех преступлений экстремистской направленности совершается с использованием ИТТ. Наиболее высок данный показатель в группе деяний, не связанных с организацией деятельности экстремистских сообществ и организаций (87,3%).

В структуре киберэкстремистских преступлений преобладают политический (44,9%) и религиозный (26,1%) мотивы. По мотивам национальной ненависти и вражды, а также по идеологическим мотивам с использованием ИТТ в среднем совершается 16,2% и 12,8% преступлений соответственно.

Сохраняется значительное число фактов, связанных с распространением недостоверной информации относительно использования Вооруженных Сил Российской Федерации и исполнения государственными органами Российской Федерации своих полномочий.

3. Киберэкстремистами, деяния которых не связаны с деятельностью экстремистских сообществ или организаций, чаще всего являются мужчины со средним профессиональным образованием, не имеющие постоянного места работы либо трудящиеся в промышленном секторе, рожденные в 70–90-х гг. XX века. Среди данных лиц выделены две подгруппы в зависимости от их отношения к сохранению своей анонимности:

а) «неосмотрительные» (составляют около 80% киберэкстремистов в рассматриваемой группе). Их отличает безразличное отношение к сокрытию личности в киберпространстве. Данные лица легко внушаемы, обладают достаточно узким кругозором, а также склонны к импульсивным и необдуманным действиям.

Уровень влияния данных лиц на формирование экстремистских воззрений у населения оценивается как низкий, поскольку их противоправная деятельность весьма непродолжительна, не спланирована и не систематична;

б) «осторожные» (составляют около 20%) – киберэкстремисты, предпринимающие больше усилий для сохранения своей анонимности. Они могут вести «двойную» жизнь, выступая в киберпространстве в роли активиста, однако никак не проявляя своих экстремистских взглядов и убеждений уже в реальном мире.

Негативное влияние данных лиц представляется более существенным. За счет возможности долгое время скрывать свою личность противоправная деятельность данных лиц может быть продолжительной.

Представителями организованного киберэкстремизма, как правило, являются образованные трудоспособные мужчины в возрасте 30–49 лет, целенаправленно вступившие в (либо создавшие) экстремистское сообщество или организацию, отождествляющие себя с ней и готовые к последовательным скоординированным преступным действиям экстремистской направленности в киберпространстве.

Данные лица нередко обладают специализированными управленческими и техническими навыками, позволяющими им организовывать функционирование экстремистских сообществ и организаций на постоянной и профессиональной основе с привлечением профильных специалистов по созданию привлекающих внимание широкого круга пользователей экстремистских материалов в различных форматах.

Влияние данных лиц на формирование у населения экстремистских взглядов и убеждений является наиболее существенным и опасным. Крайне опасной представляется ситуация, при которой их деструктивные идеи начинают транслировать популярные среди населения личности. Используя свой авторитет и доверие, они гораздо быстрее формируют экстремистские взгляды и убеждения у населения.

4. В ходе исследования определен ряд объективных и субъективных предпосылок совершения киберэкстремистских преступлений. В свою очередь их целесообразно подразделять на внешние (непосредственно связанные с участием зарубежных стран) и внутренние (обусловленные процессами, протекающими без непосредственного участия в них зарубежных стран).

К внешним объективным предпосылкам отнесено непосредственное участие представителей зарубежных государств в совершении киберэкстремистских преступлений, которое выражается: в организации массовых экстремистских акций

посредством использования ИТТ; в фабрикации и вбросе в киберпространство недостоверных сведений экстремистского содержания; в поддержке крупных информационных площадок, на которых активно распространяются экстремистские материалы.

В качестве внутренней объективной предпосылки выступает имплицитное информационно-деструктивное воздействие на личность, которое выражается в следующих формах:

- а) пропаганда деструктивных ценностей в фильмах, видеоиграх, книгах и т.д.;
- б) формирование негативного отношения к какой-либо социальной группе, объединенной по политическим, религиозным, национальным или идеологическим признакам, путем распространения в киберпространстве сведений относительно совершения правонарушений с прямым указанием на представителя группы как виновного.

Внешней субъективной предпосылкой выступает восприятие значительной частью населения России идеологии либерализма как вседозволенности на фоне проводимых при активном участии недружественных стран после распада СССР реформ, совпавшее с началом широкого распространения в стране в 90-х гг. XX в. информационно-телекоммуникационных технологий, что в совокупности с недостаточным контролем за киберпространством со стороны правоохранительных органов способствовало формированию у отдельных граждан чувства безнаказанности за распространение экстремистских материалов при помощи ИТТ.

Внутренними субъективными предпосылками совершения киберэкстремистских преступлений являются:

- а) высокая восприимчивость населения к экстремистским материалам, распространяемым в информационно-телекоммуникационном пространстве;
- б) низкий уровень осведомленности граждан относительно форм проявления экстремизма и ответственности за совершение деяний экстремистской направленности.

5. Учитывая, что публикуемая в новостных сообществах в социальных сетях общественно значимая информация может вызывать у пользователей сильные

негативные чувства, провоцируя распространение информации экстремистского содержания, в совокупности с высокой популярностью среди населения данного формата получения новостной информации, целесообразно законодательно урегулировать порядок администрирования данных новостных сообществ. В целях обеспечения контроля предлагается создание реестра новостных сообществ аналогично порядку, предусмотренному для владельцев персональных страниц, объем аудитории которых составляет более десяти тысяч пользователей, а также для новостных агрегаторов, СМИ и социальных сетей.

6. Для противодействия распространению недостоверной общественно значимой информации предложена концепция программного обеспечения, представляющего собой систему автоматизированной верификации новостной информации (САВНИ). В основу работы САВНИ может быть положена технология искусственного интеллекта в области обработки естественного языка (NLP), которая будет выполнять задачу по анализу содержания проверяемой информации и сопоставлять ее с данными, размещенными на официальных информационных порталах государственных органов и в СМИ. Указанную систему предлагается использовать по следующим направлениям:

а) пресечение распространения недостоверной общественно значимой информации в информационно-телекоммуникационном пространстве путем внедрения в деятельность правоохранительных органов для повышения эффективности их работы по выявлению, обработке и блокировке противоправного контента;

б) предоставление возможности гражданам самостоятельно, быстро и в удобной форме осуществлять предварительную оценку степени достоверности интересующих их новостных публикаций в информационно-телекоммуникационном пространстве.

7. Для предупреждения негативного воздействия на несовершеннолетних через пропаганду деструктивных ценностей в фильмах, видеоиграх, книгах и т.д. предлагается особое внимание уделять следующим перспективным направлениям по обеспечению информационно-психологической безопасности:

а) мониторинг содержания информации, распространяемой популярными среди несовершеннолетних блогерами, путем привлечения к указанной деятельности общественных организаций, родительского сообщества и педагогических работников при координационной роли правоохранительных органов в целях своевременного выявления деструктивных идей;

б) увеличение в киберпространстве объема социально полезных материалов, пропагандирующих традиционные российские духовно-нравственные ценности и усиливающих их роль в воспитании у детей чувства неприязни к различным деструктивным идеям;

в) взаимодействие государства, педагогических работников и родительского сообщества по вопросам просветительской деятельности относительно новых деструктивных течений, появляющихся в киберпространстве.

8. В целях внедрения в деятельность правоохранительных органов технологий искусственного интеллекта для идентификации экстремистских материалов, публикуемых на общедоступных страницах в социальных сетях и мессенджерах, необходимо обеспечить постоянную передачу соответствующей информации для ее обработки технологиями искусственного интеллекта. В указанных целях предлагается внести законодательные изменения, которые обязывали бы владельцев социальных сетей организовывать автоматическую пересылку содержания публикаций с общедоступных страниц пользователей. Обязанность по принятию данной информации и предварительной обработке результатов ее анализа технологиями искусственного интеллекта целесообразно возложить на Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций. В случае обнаружения материала, который программа определила как экстремистский, его следует оперативно передавать соответствующим подразделениям правоохранительных органов, занимающихся противодействием экстремизму.

Степень достоверности и апробация результатов исследования подтверждены широким диапазоном использованных методик и эмпирической базой, включающей: статистику Генеральной прокуратуры Российской Федерации и Су-

дебного департамента при Верховном Суде Российской Федерации за 2003–2024 гг.; сведения, полученные при анализе 111 судебных решений по делам о преступлениях экстремисткой направленности, совершенных с использованием ИТТ; анкетный опрос 32 сотрудников Центра по противодействию экстремизму УМВД России по Омской области, 134 сотрудников полиции, проходящих службу в подразделениях участковых уполномоченных полиции; по делам несовершеннолетних; следствия МВД России по Омской, Новосибирской, Тюменской, Кемеровской, Томской областям, Красноярскому и Алтайскому краям, Ямало-Ненецкому и Ханты-Мансийскому автономным округам, 53 работников в сфере школьного образования, а также 853 жителей Омской области; результаты контент-анализа 70 публикаций и комментариев к ним в 25 новостных сообществах 3 социальных сетей и 2 мессенджеров; результаты уголовно-правовых и иных исследований ученых, занимающихся проблемой киберэкстремизма, а также данные по теме исследования, размещенные в информационно-телекоммуникационной сети Интернет.

Основные результаты проведенного исследования нашли свое отражение в 15 научных публикациях общим объемом 5,74 п. л., из которых 5 – в рецензируемых научных изданиях, входящих в перечень, определенный Высшей аттестационной комиссией при Минобрнауки России для публикации основных научных результатов диссертаций.

Основные теоретические положения и выводы диссертационного исследования были изложены автором на научных и научно-практических конференциях, в том числе международного и всероссийского уровней: всероссийской научно-практической конференции адъюнктов и соискателей «Правоохранительная деятельность органов внутренних дел в контексте современных научных исследований» (Санкт-Петербург, 2022 г.); международной научно-практической конференции «Современные проблемы и тенденции развития юриспруденции и вопросы правоприменительной практики» (Актюбинск, Республика Казахстан, 2023 г.); международной научно-практической конференции «Актуальные проблемы борьбы с преступностью: вопросы теории и практики» (Красноярск, 2023, 2024 гг.); международной научно-практической

конференции «Современные тенденции развития юридической науки», посвященной 100-летию со дня рождения Б. Бейсенова (Караганда, Республика Казахстан, 2023 г.); международной научной конференции адъюнктов, аспирантов и соискателей «Преемственность и новации в юридической науке» (Омск, 2023–2025 гг.); международном научно-практическом семинаре «Актуальные проблемы профилактики преступлений» (Омск, 2024 г.).

Результаты исследования в виде обзора «Криминологическая природа и состояние преступлений экстремистской направленности, совершаемых с использованием информационно-телекоммуникационных технологий» внедрены в образовательный процесс Омской академии МВД России, Сибирского юридического института МВД России, Барнаульского юридического института МВД России и используются при изучении учебных дисциплин «Криминология» и «Предупреждение преступлений и административных правонарушений органами внутренних дел».

Программа для ЭВМ «Система автоматизированного мониторинга и извлечения данных из сервисов обмена мгновенными сообщениями», внесенная в Реестр программ для ЭВМ, регистрационный № 2024688641, внедрена в практическую деятельность подразделений: Управления по организации борьбы с противоправным использованием информационно-коммуникационных технологий ГУ МВД России по Красноярскому краю, Центра противодействия экстремизму УМВД России по Омской области, Управления на транспорте МВД России по Сибирскому федеральному округу (г. Новосибирск).

Структура и объем работы. Структура диссертации определена объектом, предметом, целью и задачами исследования, а также логикой изложения материала и включает введение, основную часть, состоящую из двух глав, объединяющих шесть параграфов, заключение, список литературы и приложения.

ГЛАВА 1. ПОНЯТИЕ И КРИМИНОЛОГИЧЕСКАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ ЭКСТРЕМИСТСКОЙ НАПРАВЛЕННОСТИ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

§ 1. Понятие и сущность киберэкстремизма в современной России¹

Сегодня преобладает тенденция к повсеместному внедрению ИТТ. Указом Президента РФ от 9 мая 2017 г. № 203 утверждена Стратегия развития информационного общества в Российской Федерации. В ней провозглашены задачи и меры по реализации внутренней и внешней политики Российской Федерации в сфере применения информационных и коммуникационных технологий, направленные на развитие информационного общества, формирование национальной цифровой экономики, обеспечение национальных интересов и реализацию стратегических национальных приоритетов².

Цифровизация общества и экономики влечет за собой ряд положительных последствий. В частности, в сфере экономики наблюдается активное развитие бизнеса, который все чаще основывается на широком использовании интернет-сервисов и облачных технологий. Одним из ярких примеров положительного влияния цифровизации на общество является увеличение доступности различных услуг, включая образовательные. Сегодня существует множество виртуальных библиотек, электронных баз данных диссертаций и других научных исследований. Активное использование ИТТ способствует расширению доступа к знаниям, стимулирует процессы обучения и научных исследований.

¹ Основные положения данного параграфа отражены в публикации автора: Ильиных Н. А. Киберэкстремизм: понятие и разграничение с иным информационным деструктивным воздействием на человека в киберпространстве // Известия Юго-Западного государственного университета. Серия: История и право. 2023. Т. 13, № 1. С. 64-74.

² О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы: Указ Президента РФ от 9 мая 2017 г. № 203. Доступ из справ.-правовой системы «КонсультантПлюс».

Для целей настоящего исследования при определении обобщенного неисчерпывающего перечня ИТТ согласимся с мнением Е. З. Сидоровой, которая, помимо прочих, в качестве таковых выделяет¹:

1. Сервисы мгновенного обмена сообщения (далее – мессенджеры) (WhatsApp, Viber, Telegram и т.д.);
2. Социальные сети (Одноклассники, ВКонтакте и т.д.);
3. Мобильные приложения для видеосвязи (ЯндексТелемост, Zoom, FaceTime и др.);
4. Даркнет;
5. Транзакции в криптовалюте;
6. Банковские онлайн-переводы;
7. Сотовую мобильную связь.

По нашему мнению, данный перечень целесообразно также дополнить такой популярной среди граждан технологией, как видеохостинг, которая используется для сохранения, доставки и показа видео.

Граждане все чаще используют вышеперечисленные ИТТ в повседневной жизни. Согласно официальным статистическим данным Федеральной службы государственной статистики за последние 5 лет наблюдается постоянный рост доли граждан, которые регулярно используют ИТТ (рисунок 1)².

¹ Сидорова Е. З. Уголовно-правовое противодействие финансированию экстремистской деятельности и терроризма: монография. Иркутск: Восточно-Сибирский институт МВД России, 2023. С. 53-57.

² Федеральная служба государственной статистики. URL: <https://rosstat.gov.ru/statistics/infocommunity> (дата обращения: 18.05.2025).

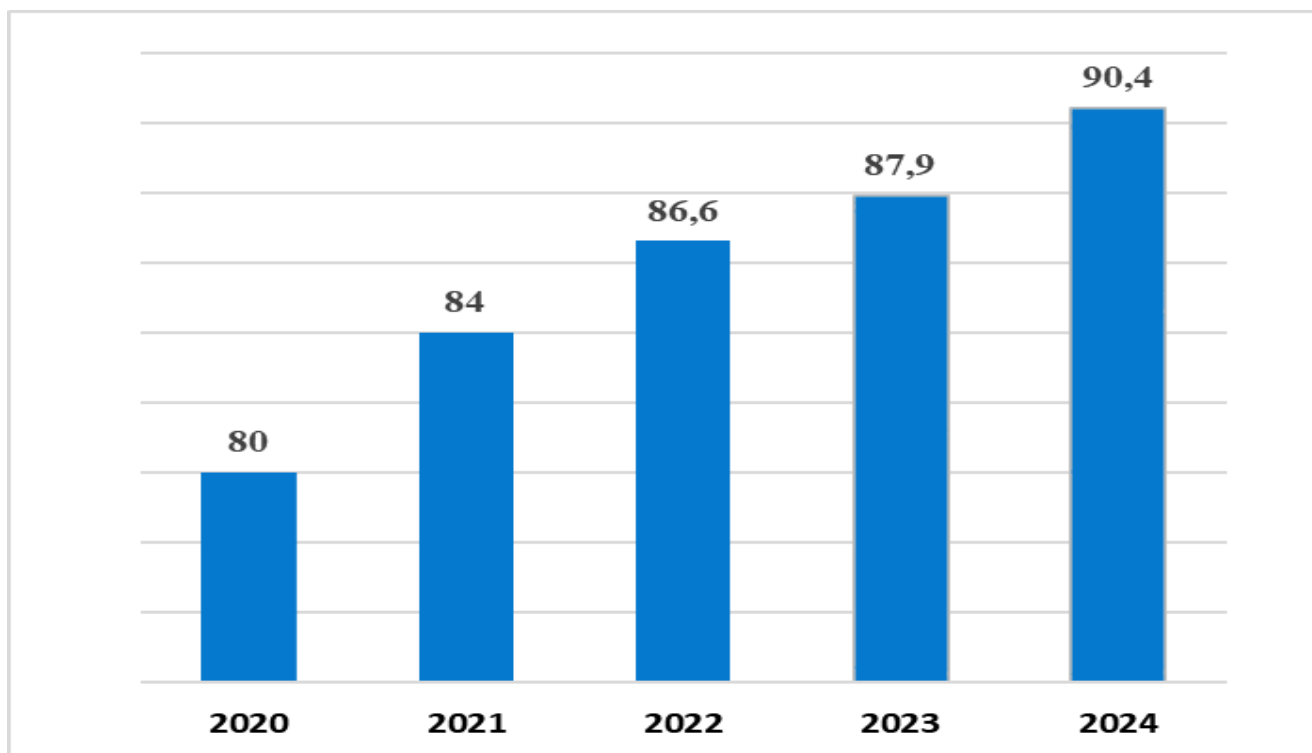


Рисунок 1 – Доля граждан Российской Федерации, являющихся активными пользователями информационно-телекоммуникационных технологий

Особенно возросла популярность среди граждан Российской Федерации социальных сетей и мессенджеров. Люди все чаще используют их для общения между собой, а также для получения информации об актуальных новостях. На данный момент до 74% населения хотя бы раз месяц пользуются самой крупной отечественной социальной сетью «ВКонтакте», около 45% населения – ежедневно¹.

Как уже было отмечено ранее, несмотря на очевидные преимущества, которые влечет за собой развитие и активное использование ИТТ, как справедливо отмечает Е. В. Никульченкова, в связи с этим возникают и новые виды преступлений, при которых активно используются интернет-технологии и киберпространство².

¹ Аудитория интернета в 2024 году / Mediascope. URL: https://mediascope.net/upload/iblock/f33/ual5i70kf7n9df7qzkq0gf238bidh3xv/%D0%9C%D0%B5%D0%B4%D0%B8%D0%B0%D0%BF%D0%BE%D1%82%D1%80%D0%B5%D0%B1%D0%BB%D0%B5%D0%BD%D0%B8%D0%B5%202024_%D0%9D%D0%90%D0%A2_27.08.2024.pdf (дата обращения: 18.12.2024).

² Никульченкова Е. В. Неопределенность терминологии и проблемы квалификации киберпреступлений (по материалам судебной практики) // Психопедагогика в правоохранительных органах. 2024. Т. 29, № 3. С. 362.

На сегодняшний день наблюдается тенденция к усилению роли ИТТ в совершении всех видов преступлений. В 2024 году зарегистрировано 765,4 тыс. преступлений, совершенных с использованием ИТТ или в сфере компьютерной информации, что на 13,1% больше, чем за аналогичный период 2023 года¹.

Информационно-телекоммуникационные технологии играют значительную роль и в совершении преступлений экстремистской направленности. В рамках подавляющего большинства научно-практических конференций, посвященных проблемам распространения экстремизма, исследователи и практические сотрудники выражают глубокую озабоченность по поводу нарастающего использования современных ИТТ в целях внедрения в массовое сознание людей экстремистских идей².

Согласно официальным статистическим данным ГИАЦ МВД России в период с 2020 по 2024 гг. средний удельный вес преступлений экстремистской направленности, совершенных с использованием ИТТ, составил 56,42%. Информационно-телекоммуникационные технологии активно применяются для распространения экстремистских материалов, осуществления публичных призывов к экстремистской деятельности. Злоумышленники также активно используют ИТТ для организации взаимодействия между собой и финансирования своей деятельности.

Полагаем, что преступления экстремистской направленности, совершаемые с использованием ИТТ, характеризуются высокой степенью общественной опасности. Как отмечают исследователи, киберпреступность в целом представляет серьезную опасность для общества. Например, А. Л. Осипенко в качестве отличительных характеристик киберпреступности (приставка «кибер» от слова «кибернетика» – наука об управлении и обмене информацией среди людей

¹ Министерство внутренних дел Российской Федерации. Состояние преступности в Российской Федерации. URL: <https://xn--b1aew.xnplai/reports/item/28021552> (дата обращения: 27.02.2025).

² Министерство внутренних дел Российской Федерации. В Москве открылась III Международная конференция по проблеме распространения идеологии экстремизма. URL: https://xn--b1aew.xn--p1ai/mvd/structure1/Glavnie_upravlenija/Glavnoe_upravlenie_po_protivodejstvu_j/Publikacii_i_vistuplenija/item/42057790/ (дата обращения: 27.09.2023).

и машин¹⁾ выделяет: особую подготовленность преступников, повышенную скрытность, трансграничный, дистанционный характер и многообразие способов совершения преступлений²⁾. Аналогичные особенности киберпреступлений отмечают также А. А. Коновалов, С. А. Наумов, Д. Д. Колесникова³⁾.

Использование ИТТ при совершении преступлений экстремистской направленности способствует распространению экстремистских материалов среди неограниченного круга лиц в кратчайшие сроки. При высокой вовлеченности населения в использование социальных сетей, мессенджеров и других ИТТ сегодня граждане регулярно сталкиваются с экстремистскими материалами, в результате часть из них могут приобретать экстремистские взгляды и убеждения.

Кроме того, возможности ИТТ позволяют лидерам экстремистских организаций и сообществ быстро и анонимно организовывать свою преступную деятельность, осуществлять ее финансирование, а также вербовать новых участников и склонять граждан к совершению преступлений экстремистской направленности.

О высокой общественной опасности преступлений экстремистской направленности, совершаемых с использованием ИТТ, в своих исследованиях утверждают В. В. Баранов, Г. И. Узембаева, В. Ю. Мельников, О. В. Обернихина, В. Н. Макашова и Е. В. Чернова⁴⁾ и др.

¹⁾ Меркушева О. В., Попова М. В. Современные процессы словообразования в аспекте когнитивной семантики // Известия ВГПУ. 2021. № 4. С. 143.

²⁾ Осипенко А. Л. Сетевая компьютерная преступность. Теория и практика борьбы: монография. Омск: Омская академия МВД России, 2009. С. 109-110.

³⁾ Коновалов А. А., Наумов С. А., Колесникова Д. Д. Киберпреступность как глобальная угроза экономической безопасности: виды, особенности, проблемы противодействия // Ростовский научный журнал. 2018. № 1. С. 20-27.

⁴⁾ Баранов В. В. Правовые и организационные основы деятельности органов внутренних дел по противодействию проявлениям экстремизма в глобальной компьютерной сети: дис. ... канд. юрид. наук. М., 2021. 290 с.; Узембаева Г. И. Преступления экстремистской направленности, совершаемые с использованием средств массовой информации либо информационно-телекоммуникационных сетей: автореф. дис. ... канд. юрид. наук. М., 2016. 24 с.; Мельников В. Ю. Преступления экстремистской направленности в Российской Федерации // Журнал юридических исследований. 2020. Т. 5, № 2. С. 15; Обернихина О. В. Криминологическая характеристика киберэкстремистской преступности в России и способы ее профилактики // Экстремизм и терроризм в киберпространстве: угрозы миру и безопасности человечества: сб. ст. по итогам III Всерос. студенческой науч.-практ. конф. Барнаул: Алтайский государственный университет, 2020. С. 30; Макашова В. Н., Чернова Е. В. Информационные технологии как фактор

Аналогично данный факт отмечают и практические сотрудники Центра по противодействию экстремизму УМВД России по Омской области (далее – ЦПЭ)¹. Результаты проведенного нами опроса свидетельствуют о том, что около двух третей (62,5%) опрошенных считают использование ИТТ более общественно опасным способом совершения преступлений экстремистского характера по сравнению с другими (например, печатной или устной агитацией).

Полагаем, что сохраняющаяся тенденция к росту числа преступлений экстремистской направленности, совершаемых с использованием ИТТ, в совокупности с высокой степенью общественной опасности указанных деяний обуславливают необходимость всестороннего рассмотрения данного негативного социально-правового явления. Полагаем, что для целей настоящего исследования необходимо объединить данные проявления экстремизма единым термином «киберэкстремизм» и определить его существенные признаки.

В указанных целях, прежде всего, необходимо определиться с тем, что сегодня понимается под термином «киберпреступление». В законодательных актах не содержится точной дефиниции. Вместе с тем большинство исследователей сходятся во мнении относительно того, что ключевым показателем, позволяющим отнести преступление к категории кибернетических, является способ его совершения, а именно – использование ИТТ, моделирующих киберпространство. Здесь также важно отметить, что, как справедливо отмечает Е. В. Никульченкова, понятие «киберпреступность» не следует отождествлять исключительно с «компьютерными» преступлениями (название главы 28 УК РФ), поскольку такие преступления могут совершаться не только с использованием компьютера, но и с помощью любых электронных носителей и средств связи².

М. С. Самурханов определяет киберпреступность как совокупность преступлений, совершаемых в киберпространстве с помощью или посредством

распространения идей киберэкстремизма в молодежной среде // Современные информационные технологии и ИТ-образование. 2013. № 9. С. 330.

¹ См. Приложение 1.

² Никульченкова Е. В. О необходимости введения дефиниции «киберпреступление» в уголовный закон Российской Федерации // Вестник Омского университета. Серия: Право. 2022. Т. 19, № 3. С. 101.

компьютерных систем или компьютерных сетей, а также иных средств доступа к киберпространству, в рамках компьютерных систем или сетей и против компьютерных систем, компьютерных сетей и компьютерных данных¹.

По мнению А. В. Маслова и Э. А. Аллахвердиевой, «киберпреступление – противоправное деяние, посягающее на объект уголовно-правовой охраны, совершенное с использованием информационно-телекоммуникационных технологий»².

И. Г. Чекунов определяет киберпреступность «в качестве самостоятельного вида преступности, определяемого на основе обнаружения обязательного присутствия в преступлениях таких признаков объективной стороны, как средство или орудие, в качестве которых выступает компьютерная программа или программно-техническое средство, подключенное к компьютерной сети или сотовому оператору связи»³.

Т. Л. Тропина в качестве основного признака, характеризующего киберпреступления, определяет совершение преступления «с помощью или посредством компьютеров, компьютерных сетей и программ, а также с помощью или посредством иных устройств доступа к моделируемому с помощью компьютера информационному пространству»⁴.

М. А. Простосердов под киберпреступлением понимает «преступление, причиняющее вред разнородным общественным отношениям, совершаемое дистанционно, путем использования средств компьютерной техники и информационно-телекоммуникационных сетей и образованного ими киберпространства»⁵.

¹ Самурханов М. С. Понятие и особенности киберпреступности // Международный журнал гуманитарных и естественных наук. 2020. № 4-3. С. 218.

² Аллахвердиева Э. А., Маслов А. В. Понятие киберпреступности и киберпреступлений: теория и практика // Общество. Закон. Правосудие. 2021. № 4. С. 34-37.

³ Чекунов И. Г. Криминологическое и уголовно-правовое обеспечение предупреждения киберпреступности: автореф. дис. ... канд. юрид. наук. М., 2013. С. 7.

⁴ Тропина Т. Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: автореф. дис. ... канд. юрид. наук. Владивосток, 2005. С. 9.

⁵ Простосердов М. А. Экономические преступления, совершаемые в киберпространстве, и меры противодействия им: дис. ... канд. юрид. наук. М., 2016. С. 30.

При определении сущности кибернетического пространства мы придерживаемся точки зрения Д. В. Пучкова, который в своем диссертационном исследовании представил следующее определение: «Кибернетическое пространство (киберреальность, виртуальная реальность) – информационно-телекоммуникационная сеть или сети, в границах которой или которых создается информация, уникальная информационная среда и условия для высокоскоростного коммуникативного управления ими при совокупности взаимодействий определенно-конкретных процессов и компьютерной техники, электронных и информационно-телекоммуникационных систем, а также необходимого программного обеспечения»¹.

Принимая за основу вышеуказанные точки зрения, в рамках настоящего исследования под киберпреступлениями понимаются все уголовно наказуемые деяния, которые совершаются с использованием технологий, моделирующих киберпространство. Также содержательно являются равнозначными понятия «преступность с использованием ИТТ» и «киберпреступность».

Переходя к определению признаков киберэкстремизма, отметим, что среди исследователей нет единого мнения относительно содержательной составляющей рассматриваемого явления. Полагаем, данная ситуация во многом обусловлена тем, что на сегодняшний день дискуссионным остается вопрос относительно определения понятия «экстремизм». На данный момент отсутствует законодательно закрепленное понятие экстремизма. Существующая правовая неопределенность порождает множество споров и на уровне доктрины. В результате нередко исследователи, характеризуя киберэкстремизм, включают в него даже те деяния, которые с законодательной точки зрения экстремизмом не являются. В связи с этим полагаем, что необходимо определить общий признак киберэкстремизма, позволяющий однозначно отделить его от иных, выходящих за рамки юридических исследований, толкований данного понятия.

¹ Пучков Д. В. Уголовно-правовая модель защиты телекоммуникаций от преступных посягательств: проблемы теории и практики: дис. ... д-ра. юрид. наук. Екатеринбург, 2022. С. 34.

На наш взгляд, такой ключевой разграничительной характеристикой киберэкстремизма должна выступать противоправность, которая вытекает из содержания законодательных положений относительно сущности самого экстремизма, а также из результатов правовых исследований по данному вопросу.

Как мы уже отметили, в законе отсутствует четко сформулированное определение экстремизма. Однако во множестве законодательных актов Российской Федерации разного уровня экстремизм определяется через характеристики отдельных форм его проявления, которые выражаются в виде запретов на совершение определенных действий. Так, характеристики отдельных форм проявления экстремизма содержатся в положениях ст. 13 и 19 Конституции Российской Федерации. В Федеральном законе от 25 июля 2002 г. № 144-ФЗ «О противодействии экстремистской деятельности» экстремизм также определяется через раскрытие содержания определенных действий¹. Аналогичный подход к определению экстремизма законодатель демонстрирует в Шанхайской конвенции о борьбе с терроризмом, сепаратизмом и экстремизмом². Безусловно, более конкретизированные запреты содержатся в Кодексе Российской Федерации об административных правонарушениях (далее – КоАП РФ) и в Уголовном кодексе Российской Федерации (далее – УК РФ).

На наш взгляд, отдельного внимания заслуживает содержательная составляющая положений Стратегии противодействия экстремизму в Российской Федерации до 2030 года, касающихся определения сущности экстремизма³. В данном акте также отсутствует точное определение, однако присутствуют такие дефиниции, которые явно указывают на стремление законодателя наделить экстремизм такой характеристикой, как противоправность:

¹ О противодействии экстремистской деятельности: федеральный закон от 25 июля 2002 г. № 144-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

² Шанхайская конвенция о борьбе с терроризмом, сепаратизмом и экстремизмом (заключена в г. Шанхае 15.06.2001). Доступ из справ.-правовой системы «КонсультантПлюс».

³ Об утверждении Стратегии противодействия экстремизму в Российской Федерации до 2030 года: Указ Президента РФ от 28 декабря 2024 г. № 1124. Доступ из справ.-правовой системы «КонсультантПлюс».

1. Экстремистская идеология – совокупность взглядов и идей, пропагандирующих насильственные и иные противоправные действия как основное средство разрешения политических, расовых, национальных, религиозных и социальных конфликтов и противоречий.

2. Проявления экстремизма (экстремистские проявления) – общественно опасные противоправные действия, совершаемые по мотивам ненависти или вражды по признакам политической, идеологической, расовой, языковой, национальной или религиозной принадлежности либо по мотивам ненависти или вражды в отношении какой-либо социальной группы или представителей органов публичной власти, способствующие возникновению или обострению межнациональных (межэтнических), межконфессиональных и региональных конфликтов, угрожающие конституционному строю Российской Федерации, суверенитету, единству и территориальной целостности Российской Федерации или направленные на умышленное искажение истории, реабилитацию нацизма, а также иные публичные действия, направленные на разжигание ненависти.

Точку зрения о том, что экстремизм в первую очередь характеризуется совокупностью прямо запрещенных законом деяний, разделяет и ряд исследователей. Например, Е. П. Сергун утверждает, что одним из ключевых признаков экстремизма является «претворение экстремистских воззрений уголовно наказуемыми способами»¹. Аналогичное мнение в своем исследовании высказывает и А. Г. Хлебушкин, характеризуя экстремизм как «противоправную деятельность, осуществление которой причиняет или может причинить существенный вред основам конституционного строя или конституционным основам межличностных отношений»². В своем исследовании С. В. Борисов также особое внимание акцентирует на противоправном характере экстремизма³.

¹ Сергун Е. П. Экстремизм в российском уголовном праве: автореф. дис. ... канд. юрид. наук. Тамбов, 2009. С. 9.

² Хлебушкин А. Г. Публичные призывы, направленные на нарушение территориальной целостности РФ (ст. 280.1 УК РФ): уголовно-правовая характеристика и вопросы квалификации // Российский следователь. 2014. № 11. С. 27.

³ Борисов С. В. Преступления экстремистской направленности: проблемы законодательства и правоприменения: дис. ... д-ра юрид. наук. М., 2012. С. 8.

В рамках своей монографической работы А. В. Петрянин утверждает, что «экстремизм – это исключительно противоправное явление»¹. Аналогичной позицию в своих исследованиях выражают также К. Д. Рыдченко, Н. Е. Макаров, Ц. С. Дондоков, Р. М. Узденов, А. С. Скудин, В. В. Бирюков² и др.

Из анализа данных понятий, а также мнений исследователей можно сделать вывод о том, что одним из ключевых отличительных признаков киберэкстремизма является противоправность. Таким образом, данные явления характеризуют исключительно те деяния, которые прямо запрещены действующим законом и за совершение которых предусмотрена юридическая ответственность.

В связи с этим, не преуменьшая безусловную научную значимость исследований для целей предупреждения экстремистских деяний, полагаем, что не вполне корректным будет излишне широко трактовать термин, характеризующий рассматриваемое нами явление, и включать в него любые иные не запрещенные законом деяния.

Например, Д. А. Акимова в понятие экстремизма, совершаемого с использованием ИТТ, включает скрытое распространение в сети Интернет вредоносных концепций³.

По мнению О. С. Жуковой, преступления экстремистской направленности, совершенные при помощи информационно-телекоммуникационных технологий,

¹ Петрянин А. В. Концептуальные основы противодействия преступлениям экстремистской направленности: теоретико-прикладное исследование: монография. М.: Проспект, 2017. С. 81.

² Рыдченко К. Д. Государственная система противодействия обороту недостоверной информации и сведений экстремистского характера: монография. Краснодар: Краснодарский университет МВД России, 2019. С. 124; Макаров Н. Е., Дондоков Ц. С. Понятие и идеология экстремизма в современных условиях // Закон и армия. 2005. № 11. С. 56-57; Узденов Р. М. Экстремизм: криминологические и уголовно-правовые проблемы противодействия: автореф. дис. ... канд. юрид. наук. М., 2008. С. 7; Скудин А. С. Правовые меры противодействия экстремизму: дис. ... канд. юрид. наук. М., 2011. С. 43; Бирюков В. В. В отношении изменений, внесенных в Федеральный закон № 114 «О противодействии экстремистской деятельности» // Военно-юридический журнал. 2007. № 12. С. 22.

³ Акимова Д. А. Современные каналы формирования и распространения идей экстремизма и терроризма в молодежной среде // Экстремизм и терроризм в киберпространстве: угрозы миру и безопасности человечества: сб. ст. по итогам III Всерос. студенческой науч.-практ. конф. Барнаул: Алтайский государственный университет, 2020. С. 99.

характеризуются в том числе использованием информации, которая негативно влияет на психологическое состояние людей, даже когда они этого не осознают¹.

Р. В. Упорников, исследуя политические и правовые меры против «информационного экстремизма», включает в определение экстремизма также социально-психологическое и косвенное физическое негативное воздействие на человека².

В своем социологическом анализе В. А. Пономарев относит к экстремизму, например, замену позитивных ценностных ориентиров общества на социальный и моральный цинизм, который проявляется в воздействии на человека через сцены жестокости и порнографии³.

Полагаем, что все вышеописанное можно охарактеризовать как имплицитное (т.е. неявное или скрытое) деструктивное информационно-психологическое воздействие на человека в киберпространстве (далее – ИДИПВ). Считаем, что не вполне корректно включать такое воздействие в понятие «киберэкстремизм». Несмотря на взаимосвязанность данных явлений, они имеют различную юридическую природу. Под «имплицитным деструктивным информационно-психологическим воздействием» здесь следует понимать не запрещенные действующим законодательством действия, а значит, их нельзя характеризовать как экстремизм, совершаемый в том числе и с использованием ИТТ. Далеко не всякое (пускай и деструктивное) информационно-психологическое воздействие, оказываемое на человека в киберпространстве, по действующему законодательству образует состав какого-либо правонарушения.

Следует отметить, что противодействие ИДИПВ в киберпространстве является одной из приоритетных задач криминологии на пути к достижению цели выработки эффективных мер предупреждения киберэкстремизма. Считаем, что

¹ Жукова О. С. Правовые меры противодействия информационному экстремизму: автореф. дис. ... канд. юрид. наук. Воронеж, 2006. С. 6.

² Упорников Р. В. Политико-правовые технологии противодействия информационному экстремизму в России: автореф. дис. ... канд. юрид. наук. Ростов-н/Д, 2007. С. 14.

³ Пономарев В. А. Информационный экстремизм и информационный терроризм в пространстве PR-технологий, СМИ и открытой информационной сети (Интернет): концептуальный аспект // Вопросы теории и практики журналистики. 2018. № 2. С. 311.

ИДИПВ на личность в киберпространстве следует рассматривать в качестве детерминанты формирования у пользователей экстремистских взглядов и совершения ими преступлений экстремистской направленности с использованием ИТТ в будущем.

Определяя существенные признаки киберэкстремизма, необходимо также обратиться к положениям подп. 4 п. 25 Стратегии национальной безопасности Российской Федерации, где в качестве одной из основных государственных угроз определено деструктивное информационно-психологическое воздействие. При определении сущности деструктивного информационного психологического воздействия на личность следует отметить, что его негативный эффект может затрагивать разные сферы жизни общества. Например, в своем исследовании В. Е. Лепский в качестве доказательства эффективности информационно-психологического воздействия наряду с широким распространением экстремистских течений приводит успех финансовых пирамид или политических партий, у которых отсутствовали разумные программы, но были деньги на то, чтобы проводить массовую агитационную программу в Интернете¹.

Однако считаем, что сегодня деструктивное информационно-психологическое воздействие на личность в киберпространстве направлено в первую очередь на формирование у населения экстремистских убеждений. Как отмечается в Доктрине информационной безопасности Российской Федерации², информационно-психологическое воздействие преимущественно носит транснациональный характер, направлено на дестабилизацию внутривнутриполитической и социальной ситуации в различных регионах мира и приводит к подрыву суверенитета и нарушению территориальной целостности других государств.

Таким образом, в рамках настоящего исследования считаем необходимым обозначить соотношение понятий «киберэкстремизм»,

¹ Лепский В. Е. Информационно-психологическая безопасность субъектов дипломатической деятельности // Дипломатический ежегодник. 2002: сб. ст. М.: Научная книга, 2003. С. 238.

² Об утверждении Доктрины информационной безопасности Российской Федерации: Указ Президента РФ от 5 декабря 2016 г. № 646. Доступ из справ.-правовой системы «КонсультантПлюс».

«имплицитное деструктивное информационно-психологическое воздействие в киберпространстве» и «деструктивное информационно-психологическое воздействие на личность». Справедливым будет вывод о том, что понятие «деструктивное информационно-психологическое воздействие на личность» является общим по отношению к понятиям «киберэкстремизм» и «имплицитное деструктивное информационно-психологическое воздействие на личность в киберпространстве», поскольку в полной мере охватывает все их признаки.

Продолжая характеризовать существенные признаки киберэкстремизма, отметим, что с законодательной точки зрения ключевым критерием при отнесении какого-либо деяния к категории экстремистского является мотив его совершения. Обратимся к положениям примечания 2 к ст. 282.1 УК РФ, где указано, что под преступлениями экстремистской направленности следует понимать уголовно наказуемые деяния, совершенные по мотивам политической, идеологической, расовой, национальной или религиозной ненависти или вражды либо по мотивам ненависти или вражды в отношении какой-либо социальной группы, предусмотренные соответствующими статьями Особенной части УК РФ и пунктом «е» ч. 1 ст. 63 УК РФ. Аналогичные разъяснения содержатся в положениях Постановления Пленума Верховного Суда РФ от 28 июня 2011 г. № 11 «О судебной практике по уголовным делам о преступлениях экстремистской направленности»¹.

Таким образом, законодатель четко определяет, что деяния признаются экстремистскими, если они совершены по соответствующим мотивам. Учитывая положения законодательства, по мотивационному критерию можно выделить следующие основные виды экстремизма: политический, религиозный, националистический (в т.ч. расовый), идеологический. Однако отметим, что экстремистские проявления редко бывают исключительно политическими, религиозными, национальными или идеологическими. Зачастую они носят

¹ О судебной практике по уголовным делам о преступлениях экстремистской направленности: постановление Пленума Верховного Суда РФ от 28 июня 2011 г. № 11. Доступ из справ.-правовой системы «КонсультантПлюс».

смешанный характер, например, национально-идеологический или религиозно-политический.

Применительно к киберэкстремизму полагаем, что рассматриваемое нами явление в полной мере соответствует определенным законодателем критериям. Использование экстремистами новых ИТТ не изменило мотивационную составляющую совершаемых ими деяний. В данном случае активное использование ИТТ при совершении экстремистских проявлений позволяет утверждать о трансформации уже существующих видов экстремизма в новую форму. Здесь следует согласиться с мнением Е. А. Куликова о том, что использование преступниками возможностей ИТТ способствовало появлению и распространению новой формы проявления экстремизма, но не изменило содержательную составляющую данного явления. Как справедливо отмечает исследователь, «как он был политическим, религиозным, национальным и т.п., так он таковым и остался»¹.

Далее необходимо определить перечень деяний, характеризующих киберэкстремизм.

Несмотря на то, что КоАП РФ содержит ряд норм, закрепляющих ответственность за совершение экстремистских действий (ст. 20.3–20.3.4, 20.28, 20.29 и др.), рамками настоящего исследования охватываются только запрещенные уголовным законодательством проявления экстремизма, в первую очередь ввиду их наибольшей общественной опасности. Более того, во многих случаях соответствующие нормы административного законодательства отсылают правоприменителя к положениям УК РФ, поскольку повторное совершение в течение одного года административных правонарушений, предусмотренных большинством статей КоАП РФ об экстремизме (например, ст. 20.3–20.3.4), образует уже состав преступлений экстремистской направленности. Таким образом, далее в рамках исследования нами будет вестись речь преимущественно

¹ Куликов Е. А. Цифровой экстремизм: общее, особенное и единичное // Экстремизм и терроризм в киберпространстве: угрозы миру и безопасности человечества: сб. ст. по итогам III Всерос. студенческой науч.-практ. конф. Барнаул: Алтайский государственный университет, 2020. С. 12.

об уголовных проявлениях киберэкстремизма, которые характеризуются совокупностью преступлений экстремистской направленности, совершаемых с использованием ИТТ.

Перейдем к определению перечня киберэкстремистских преступлений. На сегодняшний день в УК РФ отсутствует исчерпывающий перечень преступлений экстремистской направленности. Деяния, характеризующие экстремизм, в УК РФ располагаются в разных частях, разделах и главах. В общей совокупности в Особенной части по состоянию на май 2025 г. содержится свыше 40 составов преступлений экстремистской направленности.

В рамках положений Постановления Пленума Верховного Суда РФ от 28 июня 2011 г. № 11 разъясняется, что к экстремистским в качестве примера следует относить преступления, предусмотренные п. «л» ч. 2 ст. 105, п. «е» ч. 2 ст. 111, п. «б» ч. 1 ст. 213, ст. 280, 280.1, 282, 282.1, 282.2, 282.3 УК РФ. Однако данный перечень не является исчерпывающим.

Единственным нормативно-правовым актом, где определяется перечень преступлений экстремистской направленности, является Указание Генпрокуратуры России № 462/11, МВД России № 2 от 25 июня 2024 г. «О введении в действие перечней статей Уголовного кодекса Российской Федерации, используемых при формировании статистической отчетности»¹. В рамках настоящего исследования нас интересуют перечни № 20 «Преступления экстремистской направленности» и № 25 «Преступления, совершенные с использованием (применением) информационно-телекоммуникационных технологий или в сфере компьютерной информации». Полагаем, что перечень киберэкстремистских преступлений может быть определен на основе симбиоза содержащихся в вышеуказанных списках преступлений.

В результате анализа содержания данных перечней, а также актуальных статистических данных к категории преступлений экстремистской

¹ О введении в действие перечней статей Уголовного кодекса Российской Федерации, используемых при формировании статистической отчетности: указание Генпрокуратуры России № 462/11, МВД России № 2 от 25 июня 2024 г. Доступ из справ.-правовой системы «КонсультантПлюс».

направленности, совершаемых с использованием ИТТ, нами отнесены следующие составы преступлений: ч. 2 ст. 119, ст. 136, 141–141.1, ч. 1 ст. 148, 149, п. «д» ч. 2, ч. 3 ст. 207.3, ч. 3 ст. 212, ст. 239, ч. 2 ст. 280, ч. 2 ст. 280.1, ст. 280.3, п. «в» ч. 2 ст. 280.4, ст. 282, 282.1, 282.2, 282.3, ч. 1 ст. 282.4, п. «в» ч. 2, ч. 4 ст. 354.1 УК РФ¹.

На наш взгляд, целесообразно разделить все вышеперечисленные деяния на 2 группы по направленности использования ИТТ для организации деятельности экстремистских сообществ и организаций:

1. Связанные с деятельностью экстремистских сообществ и организаций (ст. 239, 282.1, 282.2, 282.3 УК РФ.);

2. Не связанные с деятельностью экстремистских сообществ и организаций (ч. 2 ст. 119, ст. 136, 141–141.1, ч. 1 ст. 148, 149, п. «д» ч. 2, ч. 3 ст. 207.3, ч. 3 ст. 212, ч. 2 ст. 280, ч. 2 ст. 280.1, ст. 280.3, п. «в» ч. 2 ст. 280.4, ст. 282, ч. 1 ст. 282.4, п. «в» ч. 2, ч. 4 ст. 354.1 УК РФ).

Отметим, что вышеприведенная классификация носит достаточно условный характер. Тем не менее данный подход позволит охарактеризовать отличительные особенности криминологической характеристики уголовного киберэкстремизма, осуществляемого хорошо подготовленными экстремистскими сообществами и организациями, с одной стороны, а также лицами, не относящими себя к какому-либо экстремистскому сообществу или организации и действующими без инструкций и сугубо из своих личных побуждений, – с другой. Считаем, что использование данного подхода в дальнейшем при определении криминологической характеристики киберэкстремизма способствует всестороннему изучению рассматриваемой преступности, что в свою очередь позволит разработать наиболее эффективные способы предупреждения. В поддержку выбранного нами основания классификации добавим, что данный дифференцированный подход уже успешно находил свое отражение в научных трудах. Здесь следует отметить обширную ра-

¹ В указанный перечень не вошли составы преступлений, которые могут быть связаны с экстремистской деятельностью (из п. 3 перечня № 20), ввиду того что они не представляют существенного интереса в рамках настоящего исследования, поскольку за последние 5 лет по ним не зарегистрировано ни одного деяния, совершенного с использованием ИТТ. По аналогичному основанию в рассматриваемый перечень не вошли следующие составы преступлений: ч. 4 ст. 150, ч. 1.1 ст. 212 УК РФ.

боту Ю. С. Магнутова, который провел комплексное исследование, посвященное уголовно-правовому противодействию только организованным формам экстремистской деятельности¹.

В результате возросшая роль ИТТ в экстремистской преступности, а также неизбежно возникающие в связи с этим особенности детерминации и механизма деструктивного воздействия на личность обуславливают необходимость в комплексном криминологическом исследовании такой ее формы, как «киберэкстремизм».

Определяя существенные признаки киберэкстремизма, в первую очередь необходимо отметить, что он включает в себя исключительно противоправные деяния. Данный вывод следует из анализа содержащихся в действующем законодательстве признаков самого экстремизма. Таким образом, считаем, что необходимо разграничивать киберэкстремизм и имплицитное деструктивное информационно-психологическое воздействие на человека в киберпространстве (ИДИПВ).

В контексте настоящего исследования определено, что ИДИПВ представляет собой неявное, завуалированное влияние на психику человека, которое следует рассматривать в качестве предпосылки формирования экстремистских взглядов и убеждений. Тем не менее данный вид деструктивного информационно-психологического воздействия сам по себе не является экстремизмом, поскольку указанные действия не запрещены действующим законодательством. Полагаем, что дифференциация понятий «киберэкстремизм» и ИДИПВ позволит устранить имеющуюся на данный момент неопределенность в понимании сущности экстремистских проявлений, совершаемых с использованием ИТТ, а также соответствующих факторов, причин и условий. По нашему мнению, данный подход во многом способствует выработке эффективной системы предупреждения указанного негативного явления.

¹ Магнутов Ю. С. Уголовно-правовое противодействие специальным организованным формам экстремистской деятельности (ст. 282.1 и ст. 282.2 УК РФ): теория, техника, практика: дис. ... канд. юрид. наук. Нижний Новгород, 2022. 384 с.

Характеризуя киберэкстремизм, также необходимо отметить, что активное использование злоумышленниками ИТТ позволяет утверждать не о появлении принципиального нового вида экстремизма, а о существенной трансформации уже существующих форм его проявления. Согласно положениям действующего законодательства, ключевым критерием при отнесении деяния к категории экстремистского является мотив его совершения. Однако сам факт использования ИТТ не изменяет мотивационную составляющую. Поэтому при отнесении деяния к категории киберэкстремистского, помимо установления факта использования ИТТ, в качестве решающего критерия следует учитывать и мотив лица.

На основе вышеизложенных выводов, положений законодательства об экстремизме и мнений исследователей относительно определения специфических элементов понятия «киберпреступность» сделан вывод о том, что под киберэкстремизмом следует понимать социальное, относительно массовое явление, проявляющееся в совокупности запрещенных законом деяний, совершаемых по экстремистским мотивам, с обязательным использованием информационно-телекоммуникационных технологий, моделирующих киберпространство.

При определении круга киберэкстремистских преступлений нами были использованы перечни составов преступлений экстремистской направленности и преступлений, совершаемых с использованием (применением) информационно-телекоммуникационных технологий или в сфере компьютерной информации, которые содержатся в положениях Указания Генпрокуратуры России № 462/11, МВД России № 2 от 25 июня 2024 г. В результате для целей настоящего исследования нами определен перечень киберэкстремистских преступлений в который вошли следующие составы: ч. 2 ст. 119, ст. 136, 141–141.1, ч. 1 ст. 148, 149, п. «д» ч. 2, ч. 3 ст. 207.3, ч. 1.1 и 3 ст. 212, ч. 1-3 ст. 239, ч. 2 ст. 280, ч. 2 ст. 280.1, ст. 280.3, п. «в» ч. 2 ст. 280.4, ст. 282, 282.1, 282.2, 282.3, ч. 1 ст. 282.4, п. «в» ч. 2, ч. 4 ст. 354.1 УК РФ.

Учитывая специфику киберэкстремистских преступлений, для целей дальнейшего криминологического исследования, а также для выработки наиболее

эффективных теоретических положений по их предупреждению установлено, что указанные деяния целесообразно разделить на 2 группы по направленности использования ИТТ для экстремистской деятельности:

1. Не связанные с деятельностью экстремистских сообществ и организаций;
2. Связанные с деятельностью экстремистских сообществ и организаций.

Используя данную классификацию, перейдем к анализу совокупности качественных и количественных показателей киберэкстремистских преступлений.

§ 2. Состояние киберэкстремистской преступности. Структура и тенденции преступлений экстремистской направленности, совершаемых с использованием информационно-телекоммуникационных технологий¹

Качественное и всеобъемлющее изучение состояния, структуры и тенденций экстремистской преступности в целом и киберэкстремистской в частности является обязательным условием для определения детерминирующих признаков совершения указанных преступлений, установления особенностей личности киберэкстремистов, а также для выработки эффективных мер предупреждения данных преступлений.

Обратимся к официальной статистике ГИАЦ МВД России² относительно количества всех преступлений экстремистской направленности. За последние 20 лет (с 2005 по 2024 гг.) в Российской Федерации наблюдается постоянный рост числа зарегистрированных преступлений указанного вида (рисунок 2).

¹ Основные положения данного параграфа отражены в публикациях автора: Ильиных Н. А. Структура, уровень и динамика киберэкстремизма в Российской Федерации // Вестник Сибирского юридического института МВД России. 2023. № 3. С. 196-201; Ильиных Н. А. Структура преступлений экстремистской направленности, совершаемых с использованием информационно-телекоммуникационных технологий // Преемственность и новации в юридической науке: мат-лы междунар. науч. конф. адъюнктов, аспирантов и соискателей. Омск: Омская академия МВД России, 2024. Вып. 20. С. 52-54.

² Министерство внутренних дел Российской Федерации. Состояние преступности в Российской Федерации. URL: <https://xn--b1aew.xnplai/reports/item/28021552> (дата обращения: 19.03.2025).

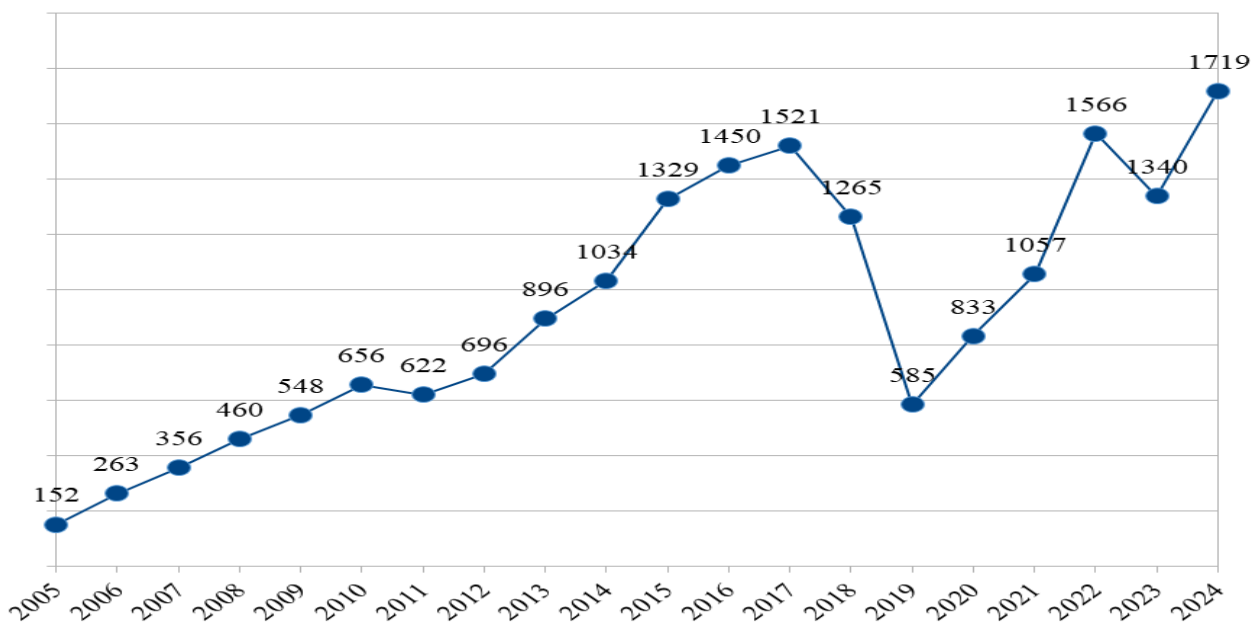


Рисунок 2 – Количество зарегистрированных преступлений экстремистской направленности в период 2005–2024 гг.

Полагаем, примечательным является тот факт, что в 2018 году Федеральным законом от 27 декабря 2018 г. № 519-ФЗ «О внесении изменения в статью 282 Уголовного кодекса Российской Федерации» были приняты поправки в ст. 282 УК РФ, согласно которым устанавливалась административная преюдиция¹. В связи с этим наблюдалось резкое снижение количества зарегистрированных преступлений по данной статье в последующем году. Однако даже с учетом действующей административной преюдиции уже в 2022 году показатель числа зарегистрированных преступлений экстремистской направленности (1566 преступлений) превысил отметку 2018 года (1265 преступлений).

Согласно данным из отчетов ГИАЦ МВД России с 2019 по 2022 гг. наблюдался постоянный рост числа зарегистрированных преступлений указанного вида: в 2019 г. их совершено 585; в 2020 г. – 833; в 2021 г. – 1057; в 2022 г. – 1566. Лишь в 2023 г. данный показатель незначительно снизился (1340 преступлений), однако он по-прежнему оставался высоким. Более того, в 2024 г. было зарегистрировано уже 1719 преступлений.

¹ О внесении изменения в статью 282 Уголовного кодекса Российской Федерации: федеральный закон от 27 декабря 2018 г. № 519-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

В свою очередь, проблему роста количества экстремистских проявлений в своих исследованиях также отмечают А. С. Ахметшин, П. В. Тепляшин, Ю. В. Леонтьева, О. А. Овчинко, И. Л. Морозов, А. Э. Абрамов, А. М. Алхастов¹ и др.

Особую актуальность данная проблема приобрела в 2022 году. В указанный период прослеживалась тенденция к значительному увеличению числа преступлений экстремистской направленности, что отчетливо видно из анализа статистических данных, характеризующих географию данного вида преступности. Отмечался резкий рост числа рассматриваемых противоправных деяний в столичных городах и приграничных с вновь присоединенными по итогам референдума 30 сентября 2022 г. южными субъектами РФ. В Москве с января по декабрь 2022 г. было зарегистрировано 280 данных преступлений, тогда как за аналогичный период 2021 г. – 59 преступлений. Таким образом, прирост составил свыше 474%. Схожая ситуация наблюдалась и в Санкт-Петербурге (+387%). Резкий рост числа преступлений указанного вида по итогам 2022 г. наблюдался в Республике Крым (+313%), Ростовской области (+247%) и Ставропольском крае (+187%). При этом в Республике Дагестан, которая исторически была лидером в данном отношении, число данных преступлений даже снизилось (–3,6%)².

Как уже было отмечено ранее, с учетом повсеместного использования преступниками возможностей ИТТ значительной трансформации подвергся и способ совершения преступлений экстремистской направленности. Первым наиболее яр-

¹ Ахметшин А. С. Уголовно-правовое противодействие преступлениям с признаками экстремистской деятельности при обеспечении основ конституционного строя и безопасности государства: дис. ... канд. юрид. наук. СПб., 2025. С. 80-81; Тепляшин П. В. Криминологические аспекты идеологии молодежного терроризма в информационно-телекоммуникационных сетях // Актуальные проблемы противодействия терроризму и экстремизму: история, современное состояние, перспективы: сб. науч. ст. всерос. науч.-практ. конф. с международным участием. Новосибирск: Новосибирский военный институт имени генерала армии И. К. Яковлева войск Национальной гвардии Российской Федерации, 2017. С. 208-212; Леонтьева Ю. В., Овчинко О. А. Экстремизм в России: цифры и размышления // Вестник Сибирского юридического института МВД России. 2020. № 3. С. 133-140; Морозов И. Л., Абрамов А. Э. Государственная стратегия противодействия экстремизму в современной России // Общество: политика, экономика, право. 2020. № 8. С. 18-22; Алхастов А. М. Актуальные проблемы молодежного экстремизма: юридический анализ, современные способы противодействия // Юридическая наука. 2022. № 7. С. 130-134.

² Боброва О. В., Меркурьев В. В. Радикальные религиозные организации угроза национальной безопасности и средства противодействия им // Обозреватель. 2022. № 10. С. 106-126.

ким примером активного использования ИТТ в распространении экстремистских идей на территории России можно считать деятельность экстремистской ультраправой организации «Северное братство», созданной в 2006 году¹. Представители данного движения активно публиковали на своем интернет-сайте призывы к насилию, примеры его одобрения вплоть до имитации казней на видео, а также пропагандировали расизм. Лидеры организации активно привлекали к сотрудничеству известных интернет-публицистов, которые в ходе обсуждений на форумах старались всячески заинтересовать пользователей идеями «Северного братства».

Наибольшую популярность указанная экстремистская организация приобрела после того, как ее представители в декабре 2007 года опубликовали на своем сайте информацию о запуске игры под названием «Большая игра: Сломай Систему». В аннотации к данной игре было указано: «Люди благодаря своему интеллекту стремились к прогрессу и свободе, однако «Система» использовала свою последнюю карту – инопланетян. Под защитой Мрака эти существа, внешне напоминающие людей из созвездия Южной Звезды, начали проникать в страны Светлой энергии, занимая ключевые позиции в их управлении и экономике. Год за годом, верно служа «Системе», инопланетяне продолжают вводить в страны Светлой энергии множество своих единомышленников, вытесняя местных».

Создатели «Игры» использовали альтернативную терминологию, чтобы избежать юридической ответственности. Однако ясно, что под «Системой» имелся в виду действующий в Российской Федерации режим, под «странами Светлой энергии» – европейские государства, в том числе Россия, под «местными» – представители «европейской расы», а под «инопланетянами из созвездия Южной Звезды» – представители других этнических групп, в первую очередь евреи, африканцы, цыгане и мигранты из стран Центральной Азии, прежних республик СССР. Цель «Игры» заключалась в проведении активностей, направленных на распространение идеологии «Северного братства», а также на психологическое и физическое

¹ Здесь и далее по тексту при упоминании данной организации: «Деятельность организации запрещена Решением Московского городского суда от 3 августа 2012 г. № 3-148/12 по основаниям осуществления экстремистской деятельности».

воздействие на «инопланетян» и представителей «Ордера», в том числе на сотрудников правопорядка.

Отметим, что указанный пример использования экстремистами ИТТ для распространения своей идеологии по времени совпадает с периодом активного распространения среди населения широкого доступа к информационно-телекоммуникационным технологиям в Российской Федерации. Считаем данный пример наиболее показательным и во многом определяющим в последующем приоритет в использовании преступниками ИТТ для совершения преступлений экстремистской направленности.

Сегодня тенденция к повсеместному использованию ИТТ в экстремистской деятельности сохраняется. Стремительное развитие возможностей ИТТ и всеобщая вовлеченность граждан в их использование создают благоприятную почву для преступников, распространяющих экстремистскую идеологию. Кроме того, при помощи современных информационно-телекоммуникационных технологий преступники активно организуют свою деятельность, а также осуществляют ее финансирование.

На рисунке 3 отображена динамика общего количества зарегистрированных преступлений экстремистской направленности, которые были совершены с использованием ИТТ, за последние 5 лет. Статистические данные свидетельствуют о существенной роли ИТТ в совершении рассматриваемых преступлений. Удельный вес киберэкстремистских преступлений в общей совокупности всех зарегистрированных преступлений экстремистской направленности стабильно превышал 50%.

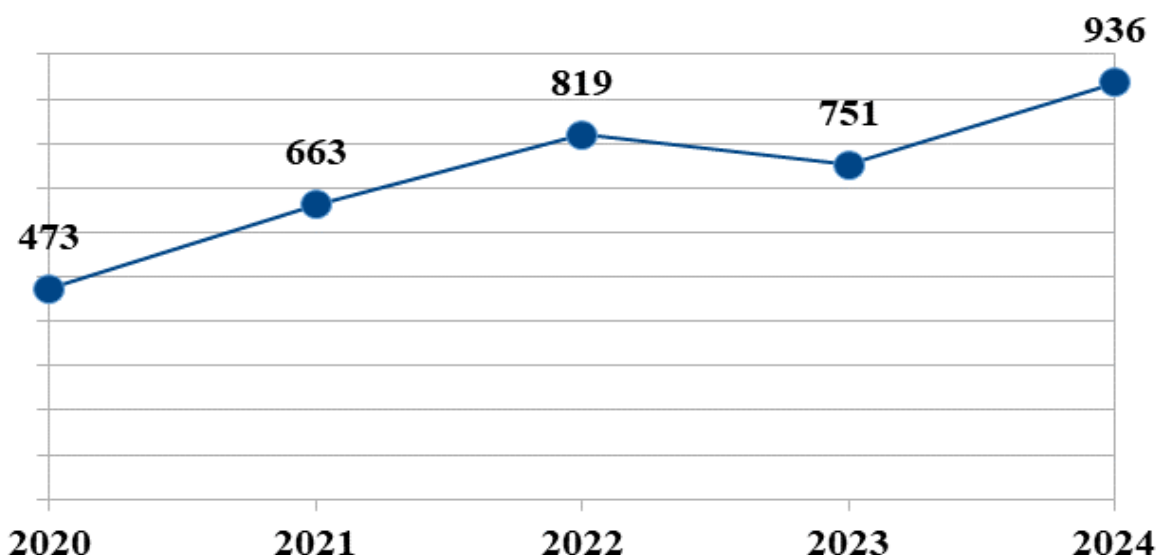


Рисунок 3 – Количество преступлений экстремистской направленности, совершенных с использованием ИТТ

Аналогично проблему использования ИТТ для совершения преступлений экстремистской направленности отмечают и практические сотрудники органов внутренних дел. Согласно результатам проведенного нами анкетирования сотрудников ЦПЭ, на вопрос: «Является ли, на Ваш взгляд, использование информационно-телекоммуникационных технологий (соцсети, мессенджеры, веб-сайты и т.д.) приоритетным для экстремистов способом совершения преступлений экстремистской направленности в Российской Федерации?» – утвердительно ответили 81,25% опрошенных¹.

Аналогичную тенденцию отмечают и ученые. В своем исследовании Э. Г. Юзиханова, проводя анализ современного состояния экстремизма в России, приходит к выводу о том, что «его (экстремизма) проявление в большей степени ориентировано через сеть Интернет с использованием информационно-телекоммуникационных технологий, т. е. в структуре экстремизма те преступления, которые связаны с непосредственным насилием, занимают меньшую часть, чем те преступления экстремистской направленности, которые ориентированы на

¹ См. Приложение 1.

публичные призывы, разжигание ненависти»¹. Тенденцию к активному использованию ИТТ при совершении преступлений экстремистского характера в своих исследованиях отмечают также В. Н. Макашова, Е. В. Чернова, Г. И. Узембаева, В. Ю. Мельников, О. В. Обернихина, Д. А. Акимова² и др.

Рассмотрение состояния киберэкстремистских преступлений согласно определенным нами в первом параграфе категориям начнем с соответствующей группы деяний, не связанных с деятельностью экстремистских сообществ и организаций. В ходе анализа статистики установлено, что именно данные преступления составляют подавляющее большинство (рисунок 4).

¹ Юзиханова Э. Г., Корсикова Н. А. Криминологический анализ экстремизма в молодежной среде на современном этапе развития общества // Правопорядок: история, теория, практика. 2024. № 4. С. 167.

² Макашова В. Н., Чернова Е. В. Информационные технологии как фактор распространения идей киберэкстремизма в молодежной среде // Современные информационные технологии и ИТ-образование. 2013. № 9. С. 328-335; Узембаева Г. И. Преступления экстремистской направленности, совершаемые с использованием средств массовой информации либо информационно-телекоммуникационных сетей: автореф. дис. ... канд. юрид. наук. М., 2016. 24 с.; Мельников В. Ю. Преступления экстремистской направленности в Российской Федерации // Журнал юридических исследований. 2020. Т. 5, № 2. С. 14-22; Обернихина О. В. Криминологическая характеристика киберэкстремистской преступности в России и способы ее профилактики // Экстремизм и терроризм в киберпространстве: угрозы миру и безопасности человечества: сб. ст. по итогам III Всерос. студенческой науч.-практ. конф. Барнаул: Алтайский государственный университет, 2020. С. 29-34; Акимова Д. А. Современные каналы формирования и распространения идей экстремизма и терроризма в молодежной среде // Экстремизм и терроризм в киберпространстве: угрозы миру и безопасности человечества: сб. ст. по итогам III Всерос. студенческой науч.-практ. конф. Барнаул: Алтайский государственный университет, 2020. С. 98-105.



Рисунок 4 – Доля киберэкстремистских преступлений неорганизованного характера

Таким образом, за последние 5 лет в среднем 87,3% всех выявленных киберэкстремистских преступлений составляли деяния, относимые нами к неорганизованному криминальному киберэкстремизму.

Среди общего количества киберэкстремистских преступлений, не связанных с деятельностью экстремистских сообществ и организаций, наиболее часто регистрируются деяния, предусмотренные ч. 2 ст. 280 УК РФ «Публичные призывы к осуществлению экстремистской деятельности». В 2024 г. удельный вес указанных преступлений в рассматриваемой группе составил 56,5%. Данный показатель остается стабильно высоким на протяжении последних 5 лет: 2020 г. – 80,5%, 2021 г. – 79,2%, 2022 г. – 67,9%, 2023 г. – 56,1%. Несмотря на прослеживающуюся тенденцию к снижению доли указанных деяний, они все еще остаются преобладающими в структуре киберэкстремистских преступлений неорганизованного характера.

Далее перечислены составы киберэкстремистских преступлений в порядке убывания по количеству зарегистрированных деяний рассматриваемой категории: ст. 282, п. «д» ч. 2, ч. 3 ст. 207.3, п. «в» ч. 2 и ч. 4 ст. 354.1, ст. 148, ч. 3 ст. 212, ч. 2 ст. 119 УК РФ. За период с января 2020 по январь 2025 гг. ни одного преступления не зарегистрировано по следующим составам преступлений: ст. 136, 141, 142, 142.1, ч. 3 ст. 239 УК РФ.

Полагаем, что в целях всестороннего анализа киберэкстремистской преступности необходимо рассмотреть вопрос о том, какие информационно-телекоммуникационные технологии и для достижения каких целей наиболее часто используются при совершении рассматриваемых преступлений. В указанных целях нами был осуществлен анализ судебной практики по всем определенным в первом параграфе составам преступлений (111 судебных решений), в ходе которого удалось выявить наиболее часто используемые экстремистами ИТТ¹.

Как нами было отмечено ранее, киберэкстремистские преступления, не связанные с деятельностью экстремистских сообществ и организаций, наиболее часто характеризуются осуществлением публичных призывов к экстремистской деятельности и разжиганием ненависти или вражды, равно унижением человеческого достоинства. Для осуществления подобной деятельности киберэкстремисты активно используют возможности ИТТ, позволяющие наиболее быстро распространять экстремистские материалы среди неограниченного круга лиц, а также привлекать тем самым новых последователей. Согласно материалам судебной практики, в указанных целях наиболее часто используются социальные сети «ВКонтакте» (41,4%), «Одноклассники» (21,6%), «Instagram» и «Facebook» (по 22,5% и 11,7% приговоров соответственно), иные социальные сети – 2,8% (рисунок 5)².

¹ Ильиных Н. А. Роль информационно-телекоммуникационных технологий в совершении экстремистских преступлений в Российской Федерации, анализ судебной практики // Мир Закона. 2023. № 1-2. С. 32-39.

² Здесь и далее по тексту при упоминании данной организации: «Facebook/Instagram – проект «Meta Platforms Inc.», деятельность которой в России запрещена решением Тверского районного суда г. Москвы от 21 марта 2022 г. № 02-2473/2022 по основаниям осуществления экстремистской деятельности».

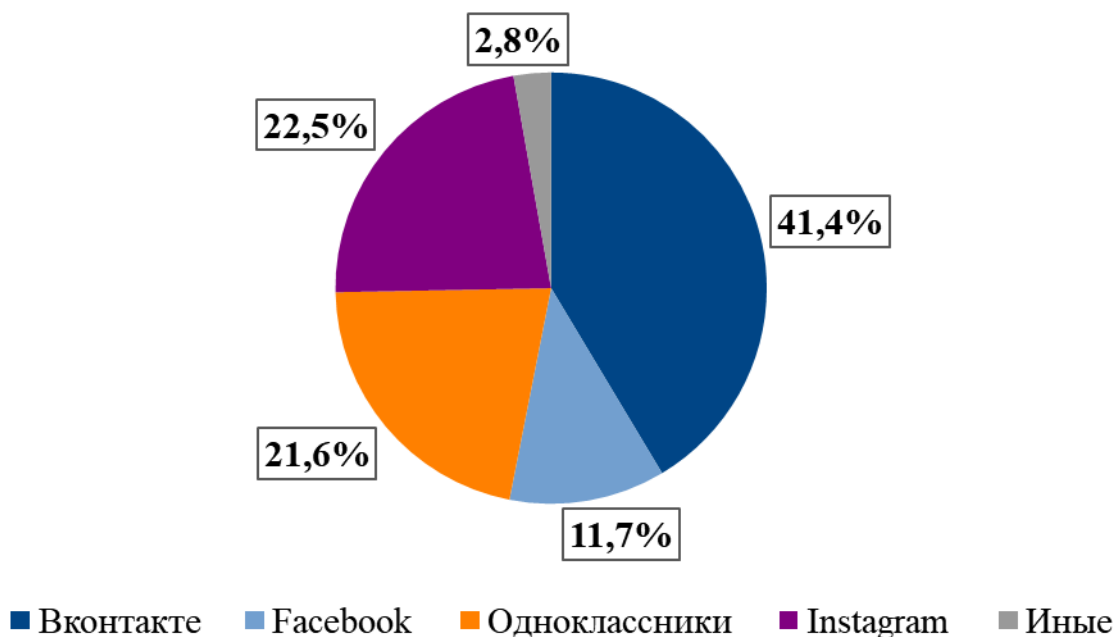


Рисунок 5 – Социальные сети, наиболее часто используемые для распространения экстремистских материалов и привлечения новых последователей согласно материалам судебной практики 2020-2024 гг.

На наш взгляд, приоритет в использовании преступниками для указанных целей именно отечественных социальных сетей в первую очередь обусловлен их наибольшей популярностью среди граждан России. Однако есть основания полагать, что доля зарубежных социальных сетей в распространении экстремистских материалов может быть несколько выше.

Во-первых, с момента запрета работы социальных сетей Facebook и Instagram деятельность правоохранительных органов по выявлению в них экстремистских материалов резко сократилась, следовательно, за последнее время снизилась и доля соответствующих обвинительных приговоров. Однако нельзя сказать, что граждане полностью перестали использовать данные соцсети. По состоянию на 2024 год, согласно отдельным исследованиям, Instagram входит в топ-5 самых популярных среди граждан социальных сетей¹.

¹ Как устроена аудитория социальных медиа / Mediascope. URL: <https://mediascope.net/news/2544317> (дата обращения: 07.02.2025).

Во-вторых, значительно проще установить личность пользователя, распространяющего экстремистские материалы именно в российских социальных сетях, что во многом обуславливает большое количество соответствующих обвинительных приговоров.

В-третьих, по результатам анкетирования практических сотрудников полиции установлено: свыше половины опрошенных (79,9%) указали на то, что сегодня большинство всех киберпреступлений совершается при помощи социальных сетей, находящихся в юрисдикции зарубежных стран.

Переходя к рассмотрению состояния организованного уголовного киберэкстремизма, отметим, что в течение исследуемого периода в целом большинство зарегистрированных преступлений экстремистской направленности, связанных с деятельностью экстремистских сообществ и организаций, совершались без использования ИТТ. Доля преступлений из данной категории с отметкой об использовании ИТТ значительно ниже аналогичного показателя для киберэкстремистских преступлений неорганизованного характера (рисунок 6) и составляет в среднем 23,12%.

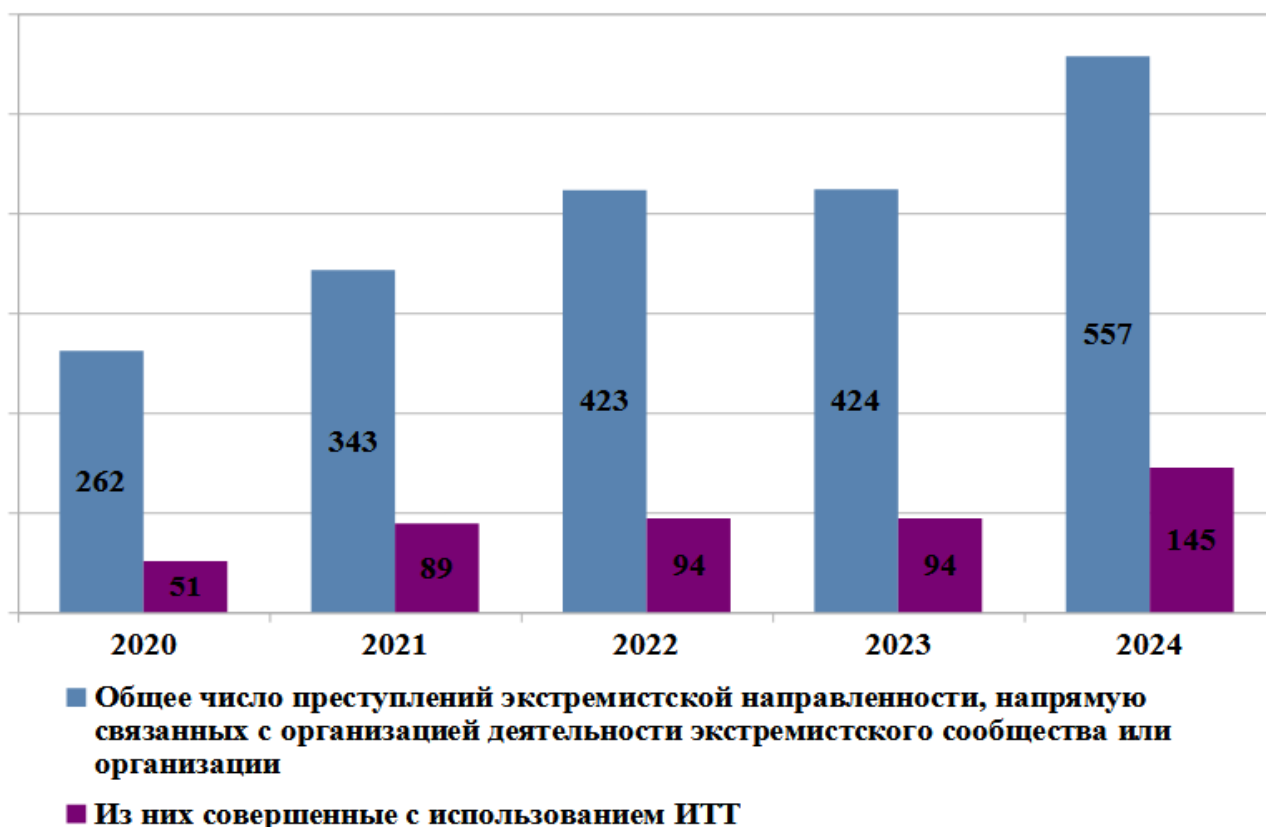


Рисунок 6 – Доля киберэкстремистских преступлений организованного характера

Вместе с тем полагаем, что ИТТ все же играют существенную роль в совершении киберэкстремистских преступлений организованного характера. Наиболее часто в данной категории регистрируются преступления, связанные с участием в деятельности общественного или религиозного объединения либо иной организации, в отношении которых судом принято вступившее в законную силу решение о ликвидации или запрете деятельности в связи с осуществлением экстремистской деятельности (ч. 2 ст. 282.2 УК РФ), а также аналогичные деяния в составе экстремистского сообщества (ч. 2 ст. 282.1 УК РФ). В среднем доля указанных киберэкстремистских преступлений в структуре организованного киберэкстремизма за последние 5 лет составила 69,9%. Безусловно, нельзя не отметить повышенную общественную опасность преступной деятельности, осуществляемой в составе какой-либо экстремистской организации или в сообществе. Однако указанная деятельность не всегда связана с принятием управленческих решений и зачастую ограничивается исполнением каких-либо поручений от непосредственных организаторов. В связи с этим особый интерес представляет та деятельность, которая связана с руководством организацией или сообществом, вербовкой новых членов, а также с осуществлением финансирования экстремизма (таблица 1).

Таблица 1 – Количество зарегистрированных преступлений экстремистской направленности, связанных с организацией деятельности экстремистских сообществ и организаций, совершенных с использованием ИТТ

Наименование нормы УК РФ	2020	2021	2022	2023	2024
ч. 1, 1.1, 3 ст. 282.1 УК РФ	3	10	5	4	9
ч. 1, 1.1, 3 ст. 282.2 УК РФ	12	38	23	21	20
ст. 282.3 УК РФ	5	5	11	17	37

Рассматривая вопрос о том, какие ИТТ наиболее часто используются для организации деятельности экстремистских сообществ и организаций, отметим, что в данном случае наибольшее значение имеют технологии, которые позволяют быстро устанавливать бесперебойные каналы связи. В ходе анализа материалов

судебной практики установлено, что в указанных целях экстремисты чаще всего использовали мессенджеры, а именно Telegram (40,6%) и WhatsApp (42,4%). При этом значительно реже в материалах судебных решений фигурировали уже ставшие традиционными технологии мобильной сотовой связи (15%) (рисунок 7).

На наш взгляд, популярность указанных мессенджеров обусловлена высокой степенью их анонимности по сравнению с обычными телефонными звонками или общением в социальных сетях. Она достигается благодаря эффективным методам шифрования информации: «Open Whisper Signal» у WhatsApp и «MTProto» у Telegram, которые значительно усложняют деанонимизацию пользователей и расшифровку их сообщений.

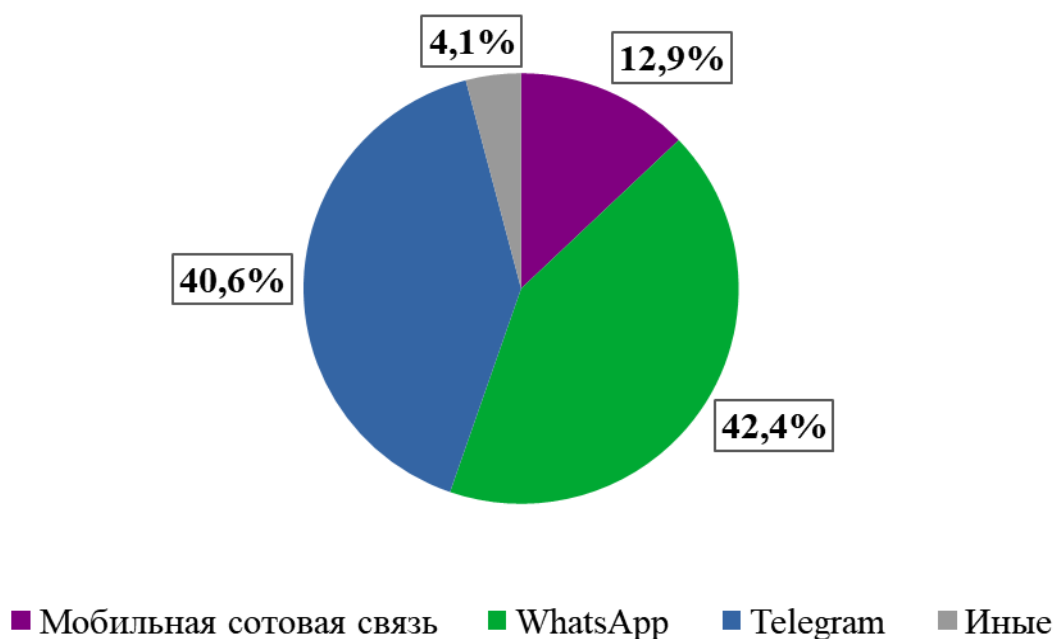


Рисунок 7 – ИТТ, используемые для связи участников экстремистских сообществ и организаций между собой, а также для вербовки новых участников и склонения к совершению преступлений экстремистской направленности

Еще одним немаловажным элементом организации деятельности экстремистских сообществ и организаций является привлечение финансирования. Примечательно, что современные возможности отдельных ИТТ способны не только облегчить процесс передачи денежных средств, но и сохранить при этом анонимность отправителя и получателя. В ходе анализа материалов судебной практики

установлено, что для финансирования экстремистской деятельности злоумышленники активно использовали банковские онлайн-переводы, а также транзакции в криптовалюте (рисунок 8).

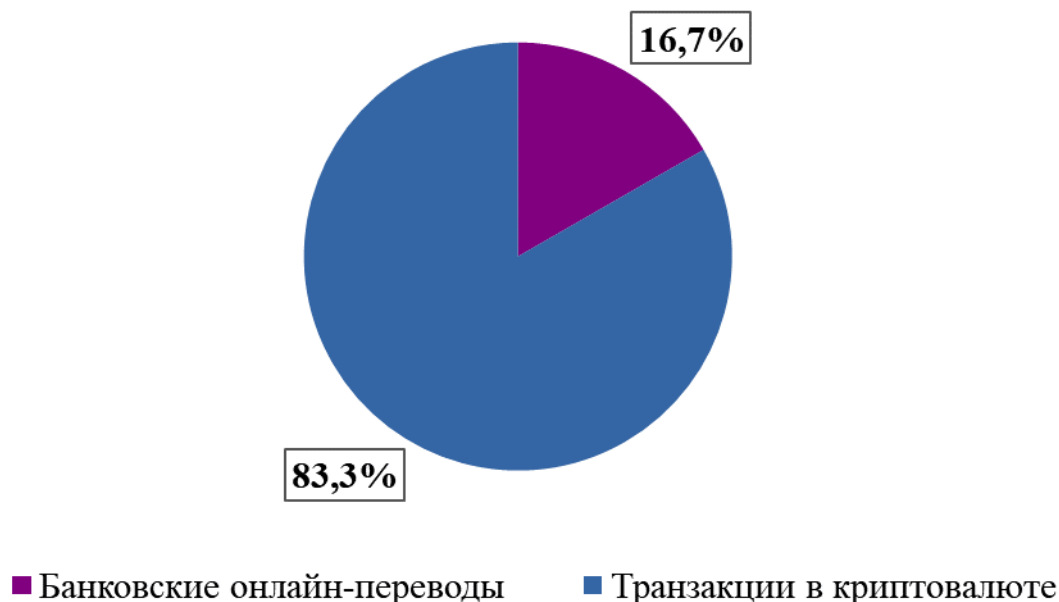


Рисунок 8 – ИТТ, используемые для финансирования экстремистской деятельности

В свою очередь, отметим тот факт, что, в отличие от банковских онлайн-переводов, операции с криптовалютой осуществляются при помощи такой формы технологии распределенных систем, как «блокчейн», особенности функционирования которой существенно снижают вероятность установления личностей отправителя и получателя криптовалют¹. Исследуя роль криптовалюты в финансировании экстремизма и терроризма, Т. В. Пинкевич и О. А. Зубалова в своем исследовании также справедливо отмечают, что ввиду высокой анонимности и низкого уровня обнаружения криптовалютных транзакций их использование создает благоприятные условия для совершения экстремистских и террористических пре-

¹ Андропова И. В., Гусаков Н. П., Завьялова Е. Б. Финансирование терроризма: новые вызовы для международной безопасности // Вестник международных организаций: образование, наука, новая экономика. 2020. № 1. С. 128.

ступлений в виртуальной среде¹. Полагаем, что в связи с этим значительная часть подобных фактов может оставаться скрытой от правоохранительных органов.

Далее рассмотрим вопрос об общем уровне латентности киберэкстремистских преступлений. По мнению исследователей, экстремистская преступность в целом характеризуется высоким уровнем латентности. Согласно результатам исследования А. В. Петрянина 96% осужденных за преступления экстремистской направленности в ходе социологического опроса признались, что ранее уже совершали указанные преступления, однако не привлекались к уголовной ответственности².

Полагаем, что высокий уровень латентности характерен в первую очередь для экстремистских преступлений, совершаемых с использованием ИТТ, поскольку именно ИТТ позволяют им совершать преступления дистанционно, скрывая свою личность и местоположение³. Например, технология VPN (Virtual Private Network) позволяет устанавливать защищенное соединение между устройством пользователя и интернетом. Она шифрует данные и маскирует пользовательский IP-адрес, скрывая тем самым местоположение пользователя. В результате использования киберэкстремистами подобных технологий снижается эффективность деятельности правоохранительных органов по установлению их личностей.

Считаем, что наиболее латентным является организованный криминальный киберэкстремизм, поскольку высокий уровень подготовки организаторов, а также непубличный характер их деятельности позволяют им наиболее эффективно использовать технические средства для сохранения анонимности и скрываться от правоохранительных органов. В свою очередь, киберэкстремистские преступле-

¹ Пинкевич Т. В., Зубалова О. А. Современное состояние экстремизма и терроризма в условиях развития цифровых технологий // Юристъ-Правоведъ. 2020. № 3. С. 67.

² Петрянин А. В. Концептуальные основы противодействия преступлениям экстремистской направленности: теоретико-прикладное исследование: монография. М.: Проспект, 2017. С. 213.

³ Ильиных Н. А. Отдельные факторы распространения экстремизма среди детей в информационно-телекоммуникационном пространстве // Правоохранительная деятельность органов внутренних дел в контексте современных научных исследований: мат-лы всерос. науч.-практ. конф. адъюнктов, аспирантов и соискателей. СПб.: Санкт-Петербургский университет МВД России, 2022. С. 231.

ния, не связанные с организацией деятельности экстремистских сообществ и организаций, как правило, совершаются без тщательной предварительной подготовки, в результате чего значительно чаще попадают в поле зрения правоохранительных органов.

Высокий уровень латентности обуславливается также активным использованием экстремистами иностранных социальных сетей, мессенджеров и других ИТТ, вследствие чего, чтобы установить личность и истинное местонахождение преступника, необходимо направлять запросы в правоохранительные органы иностранных государств, что в свою очередь в силу сложной внешнеполитической обстановки зачастую не представляется возможным.

Считаем, что тезис об активном использовании киберэкстремистами возможностей зарубежных ИТТ также косвенно подтверждается результатами проведенного нами опроса практических сотрудников, согласно которым 79,9% опрошенных полагают, что большинство указанных преступлений совершается с использованием зарубежных социальных сетей и мессенджеров¹.

Кроме того, считаем, что ввиду достаточно сложной специфики функционирования современных ИТТ у практических сотрудников нередко возникают проблемы, связанные с недостатком необходимых технических знаний и соответствующих средств для выявления и раскрытия киберэкстремистских преступлений. В ходе опроса три четверти сотрудников ЦПЭ отметили необходимость в разработке методических рекомендаций по использованию специальных технических средств для выявления экстремистских материалов и установления личности экстремиста в интернете².

Таким образом, киберэкстремистские преступления характеризуются высоким уровнем латентности ввиду особенностей функционирования отдельных ИТТ, сложностей обеспечения взаимодействия российских и зарубежных правоохранительных органов, а также в силу недостаточности существующей учебно-методической базы, позволяющей передать сотрудникам правоохранительных ор-

¹ См. Приложение 2.

² См. Приложение 1.

ганов необходимые знания о технических особенностях функционирования отдельных информационно-телекоммуникационных технологий, используемых для совершения преступлений экстремистской направленности.

Переходя к рассмотрению структуры киберэкстремистской преступности, следует сказать, что, как нами уже отмечалось, виды преступлений экстремистской направленности определяются через мотивы их совершения. Опираясь на материалы судебной практики (111 решений судов), удалось установить, что за период 2020–2024 гг. в большинстве случаев киберэкстремистские преступления совершались по политическим мотивам (44,9%). Как правило, данные противоправные действия выражались в форме публикаций или комментариев к ним в сообществах социальных сетей, содержащих призывы к совершению насильственных действий в отношении представителей органов государственной власти.

Например, согласно материалам приговора Сюзьинского районного суда Удмуртской Республики от 5 мая 2021 г. по делу № 1-56/2021, гражданин Ш. с помощью своего мобильного телефона, подключённого к интернету, действуя умышленно, осознавая публичный и антиобщественный характер своих действий, с целью воспрепятствования законной деятельности органов государственной власти и органов местного самоуправления и побуждения неограниченного круга пользователей интернета к совершению насильственных действий в отношении группы лиц, объединённых по признакам профессиональной социальной принадлежности – представители органов власти «чиновники», а также к нарушению прав и законных интересов последних, разместил на своей личной странице социальной сети «ВКонтакте» изображение и текстовую запись экстремистского содержания. Гражданин Ш. также неоднократно оставлял аналогичные текстовые комментарии в сообществе данной социальной сети «Типичный Ижевск»¹.

Доля киберэкстремистских преступлений, связанных с деятельностью запрещённых религиозных течений, составила 26,1%. Информационно-телекоммуникационные технологии наиболее часто использовались преступни-

¹ Приговор Сюзьинского районного суда Удмуртской Республики от 5 мая 2021 г. по делу № 1-56/2021. Доступ из справ.-правовой системы «ГАРАНТ».

ками для проведения онлайн-встреч, а также для осуществления вербовки новых последователей. Например, согласно материалам приговора Ленинского районного суда г. Ростова-на-Дону Ростовской области от 25 января 2021 г. № 1-41/2021 гражданка П. посредством сети Интернет организовывала онлайн-конференции, в ходе которых изучались статьи из книги «Священное писание – Перевод нового мира», включенной 5 июля 2018 г. под № 4488 в федеральный список экстремистских материалов Министерства юстиции Российской Федерации¹.

По сравнению с преступлениями экстремистской направленности, совершенными по иным мотивам, для осуществления указанных действий по религиозным мотивам преступники наиболее часто использовали средства мобильной сотовой связи. Данная технология преимущественно использовалась злоумышленниками для установления контакта и последующей вербовки потенциальных последователей. Так, согласно приговору Волжского районного суда г. Саратова Саратовской области от 25 августа 2021 г. представитель запрещенного религиозного объединения по телефону связывался с потенциальными последователями. В ходе разговоров он рассказывал об особенностях религиозного течения, а именно о «выходах на три, десять, сорок дней и четыре месяца», о необходимости осуществлять «труд», выходить на пути Аллаха, как осуществлять «ташкиль» и т. д.²

В 16,2% случаев преступники использовали ИТТ для совершения действий, направленных на разжигание расовой и национальной ненависти. Объективная сторона данных преступлений наиболее часто выражалась в размещении в интернете призывов к насильственным действиям в отношении представителей отдельной расы или национальности. Типичным примером данных преступлений являются действия гражданина М., который согласно материалам приговора Новочебоксарского городского суда Чувашской Республики – Чувашии от 21 сентября 2020 г. № 1-136/2020 разместил на своей личной странице в социальной сети «ВКонтакте» следующий текст: «Евреи ХАБАД-Любавичи захватили Власть в

¹ Приговор Ленинского районного суда г. Ростова-на-Дону Ростовской области от 25 января 2021 г. по делу № 1-41/2021. Доступ из справ.-правовой системы «ГАРАНТ».

² Приговор Волжского районного суда г. Саратова Саратовской области от 25 августа 2021 г. по делу № 1-202/2021. Доступ из справ.-правовой системы «ГАРАНТ».

наших странах!!! Украинцы убивайте не друг друга а Жидов. Бей Жидовскую мразь!!!», который содержит совокупность психологических и лингвистических признаков побуждения неограниченного круга лиц к агрессивным, насильственным действиям в отношении евреев, их физическому уничтожению, т.е. к осуществлению экстремистской деятельности¹.

Проявления идеологического экстремизма в киберпространстве (12,8%) преимущественно характеризовались совершением преступлений, предусмотренных ст. 354.1 УК РФ «Реабилитация нацизма». Информационно-телекоммуникационные технологии наиболее активно применялись для распространения деструктивных идей среди неопределенного круга лиц. Например, как следует из материалов приговора Красноярского краевого суда от 14 октября 2022 г. по делу № 2-40/2022, гражданин С. решил публично выразить свое отрицание фактов, установленных приговором Международного военного трибунала для суда и наказания главных военных преступников европейских стран «оси», и одобрение преступлений, установленных указанным приговором, путем публичного распространения соответствующих сведений в виде личного размещения своих текстовых комментариев в сети Интернет в различных сообществах социальной сети «ВКонтакте», доступных для просмотра и восприятия неограниченным кругом лиц².

Достаточно актуальной на сегодняшний день остается проблема распространения такой формы идеологического экстремизма, как пропаганда идей организации «АУЕ» (сокращение обычно расшифровывается как «Арестантский уклад един» или «Арестантское уголовное единство»)³. Специфика указанного общественного объединения заключается главным образом в пропаганде системы ценностей и норм поведения, тождественных по смыслу криминальной идеологии

¹ Приговор Новочебоксарского городского суда Чувашской Республики – Чувашии от 21 сентября 2020 г. по делу № 1-136/2020. Доступ из справ.-правовой системы «ГАРАНТ».

² Приговор Красноярского краевого суда от 14 октября 2022 г. по делу № 2-40/2022. Доступ из справ.-правовой системы «ГАРАНТ».

³ Здесь и далее по тексту при упоминании данной организации: «Деятельность организации запрещена Решением Верховного Суда Российской Федерации от 17 августа 2020 г. по делу № АКПИ20–514с по основаниям осуществления экстремистской деятельности».

русской организованной преступности («воровским понятиям»). Негативные проявления данной идеологии наиболее часто встречаются в местах лишения свободы. Однако для распространения идей указанной субкультуры злоумышленники наиболее активно используют и возможности ИТТ. Киберэкстремисты создают различные тематические сообщества, в которых публикуются материалы, направленные на романтизацию арестантской жизни. В качестве целевой аудитории подобных групп выступают преимущественно несовершеннолетние лица.

Так, например, в 2020 г. Останкинский районный суд признал запрещенным сообщество в социальной сети «ВКонтакте» под названием «Бог спасет, братва поможет». В материалах дела отмечается, что количество несовершеннолетних подписчиков составило 1967. Для распространения экстремистской и криминальной идеологии, вовлечения в свои ряды новых участников и сторонников движением активно использовались возможности сети Интернет. На сайтах участников «АУЕ» пропагандировались воровские и тюремные своды правил (так называемые понятия) и неукоснительное соблюдение «воровского кодекса», криминальные традиции, насилие как средство достижения цели, иные материалы, наносящие вред здоровью несовершеннолетних¹. Примечательно, что по состоянию на 13 марта 2025 г. сообщество с указанным названием и по тому же адресу ссылки продолжало функционировать. На главной странице сообщества отсутствует прямое упоминание движения «АУЕ», однако имеются многочисленные факты публикаций изображений оружия, употребления табачной и алкогольной продукции, а также иных атрибутов романтизации нелегальной деятельности.

Характеризуя структуру киберэкстремистской преступности, необходимо отметить, что, как и в случае с преступлениями экстремистской направленности, совершаемыми без использования ИТТ, не всегда можно однозначно определить их видовую принадлежность. В качестве примера можно привести материалы приговора Ленинского районного суда г. Кемерово Кемеровской области от 16 ноября 2020 г. № 1-265/2020. Гражданин Я. на своих личных страницах в соци-

¹ Решение Останкинского районного суда г. Москвы от 30 ноября 2020 г. по делу № 2а-556/2020. Доступ из справ.-правовой системы «ГАРАНТ».

альных сетях «ВКонтакте» и «Одноклассники» регулярно публиковал экстремистские материалы, содержащие призывы к насилию в отношении одновременно как представителей власти, так и группы лиц, выделенной по признаку национальности (евреи)¹.

Установленные в ходе анализа судебной практики значения показателей, характеризующих структуру киберэкстремистских преступлений, во многом сопоставимы с мнением сотрудников ЦПЭ, которым был задан вопрос относительно того, какой мотив совершения преступлений экстремистской направленности, по их мнению, сегодня является преобладающим (таблица 2)².

Таблица 2 – Сравнение результатов анализа судебной практики и анкетирования сотрудников ЦПЭ относительно структуры киберэкстремистских преступлений, выделенной по мотивационному признаку

Мотив	Результаты анализа судебной практики	Результаты анкетирования сотрудников ЦПЭ
Политический	44,9%	37,5%
Религиозный	26,1%	25%
Националистический	16,2%	28,2%
Идеологический	12,8%	9,3%

Рассматривая тенденции киберэкстремистской преступности, отметим, что сегодня все большую актуальность приобретает проблема, обусловленная ростом числа фактов распространения в киберпространстве недостоверных и дискредитирующих сведений о Вооруженных Силах Российской Федерации.

Например, вскоре после начала проведения специальной военной операции на Украине в 2022 г. в интернете появилась запись, представленная как факт атаки гражданских объектов Украины с помощью российских установок «Град». Одна-

¹ Приговор Ленинского районного суда г. Кемерово Кемеровской области от 16 ноября 2020 г по делу № 1-265/2020. Доступ из справ.-правовой системы «ГАРАНТ».

² См. Приложение 1.

ко стало известно, что данное видео было снято годом ранее в ходе военных манёвров России и было опубликовано 27 апреля 2021 г.¹

Недостоверными также являются активно распространяемые в информационно-телекоммуникационном пространстве видеоматериалы об осуществлении ВС РФ массированного обстрела города Мариуполя в феврале 2022 г.²

Вышеуказанный список можно продолжать еще очень долго. В рамках настоящего исследования представляет наибольший интерес тот факт, что, как отмечает в своем исследовании А. М. Абдулатипов, распространение подобных недостоверных сведений происходит преимущественно с использованием ИТТ³.

О массовости рассматриваемого явления свидетельствуют результаты исследования Н. Ш. Козаева и Н. А. Табаковой, которые также отмечают особую роль социальных сетей как основного источника фейков⁴. В ходе анкетирования граждан нами установлено, что 35,3% опрошенных встречаются с фейковыми новостями в мессенджерах, социальных сетях, на веб-сайтах минимум 1 раз в неделю; 37,6% – минимум 1 раз в месяц; 20,1% – за все время 1 раз; 7% опрошенных лиц ни разу не сталкивались с подобными сведениями⁵.

Согласно статистическим данным в 2022 г. выявлено 76 преступлений, предусмотренных п. «д» ч. 2, ч. 3 ст. 207.3 УК РФ. В 2023 г. данный показатель увеличился и составил уже 84 факта. В 2024 г. количество зарегистрированных деяний по данной статье также составило 84.

¹ См.: МО РФ заявило о нарастании количества фейков по ситуации на Украине. URL: <https://iz.ru/1297404/2022-02-26/mo-rf-zaiavilo-o-narastanii-kolichestva-feikov-po-situacii-naukraine> (дата обращения: 10.09.2023).

² См.: «Обстрел» Мариуполя Вооруженными Силами России оказался фейком. URL: <https://iz.ru/1296705/2022-02-25/obstrel-mariupolia-vooruzhennymi-silami-rossii-okazalsia-feikom> (дата обращения: 28.03.2022).

³ 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 // Юридический вестник Дагестанского государственного университета. 2022. № 2. С. 121-126.

⁴ Козаев Н. Ш., Табакова Н. А. Особенности уголовной ответственности за публичное распространение заведомо ложной информации об использовании Вооруженных Сил Российской Федерации, исполнении государственными органами Российской Федерации своих полномочий (ст. 207.3 УК РФ) // Общество и право. 2022. № 2. С. 48-51.

⁵ См. Приложение 4.

Рост количества зарегистрированных киберэкстремистских преступлений, связанных с распространением недостоверной информации, прослеживается и в отношении деяний, предусмотренных ст. 280.3 УК РФ: в 2023 г. – 28, в 2024 г. – 32.

Полагаем, что совокупность вышеуказанных фактов свидетельствует о такой тенденции киберэкстремистской преступности, как усиление роли фейков в деструктивном информационно-психологическом воздействии на население.

Полагаем, что еще одной современной тенденцией киберэкстремистской преступности является усиление роли зарубежных стран в подготовке и совершении преступлений экстремистской направленности в России. Как отметил в своем выступлении Президент РФ В. В. Путин, информационно-психологическое давление против нашей страны осуществлялось всегда, однако с началом СВО данный процесс усилился¹.

Сегодня множество исследователей также отмечают главенствующую роль зарубежных социальных сетей и СМИ в процессе распространения и создания экстремистских материалов. Как справедливо отмечает в своем исследовании А. Г. Кибальник, информационная кампания против России и ее Вооруженных Сил – это «война за умы людей, их настроения и волю». Автор утверждает, что представители отдельных зарубежных государств используют экстремистский контент, в частности фейки, для внедрения в массовое сознание населения идеи «преступности» действий ВС РФ на Украине и, как следствие, формирования пессимистических или даже экстремистских убеждений в российском обществе². Такой же позиции в своем исследовании придерживаются О. Е. Воронова и А. С. Трушин, отмечая ключевую роль представителей зарубежных стран в под-

¹ См.: Путин назвал западные страны «империей лжи» после введения новых санкций // РБК. URL: <https://www.rbc.ru/politics/28/02/2022/621cbe6b9a794770558ada7f> (дата обращения: 16.11.2023.)

² Кибальник А. Г. Уголовная ответственность за публичное распространение фейков об использовании Вооруженных Сил РФ. Как применять новую статью УК // Уголовный процесс. 2022. № 5. С. 63.

готовке и распространении экстремистского контента¹. Аналогичную точку зрения высказало также большинство опрошенных сотрудников ЦПЭ².

Таким образом, результаты исследования показали, что использование ИТТ играет значительную роль в совершении преступлений экстремистской направленности. Установлено, что около 60% всех данных преступлений совершается с использованием возможностей ИТТ.

В группе составов преступлений, не связанных с деятельностью экстремистских сообществ и организаций, доля зарегистрированных киберэкстремистских преступлений в среднем достигает 87,3%. Наиболее часто при совершении указанных деяний экстремисты используют возможности социальных сетей и мессенджеров.

Активно используются возможности ИТТ и для деятельности экстремистских сообществ и организаций. В среднем 18,7% всех данных преступлений имеют отметку об использовании ИТТ. Для связи между собой, а также для вербовки новых членов организаторы наиболее активно используют мессенджеры, для осуществления финансирования экстремистской деятельности – банковские онлайн-переводы и криптовалюту.

Полагаем, что значительная часть совершаемых киберэкстремистских преступлений являются латентными. Данный факт может быть обусловлен целым рядом причин, среди которых: использование экстремистами технологий, позволяющих сохранять анонимность, а также социальных сетей, мессенджеров, отдельных веб-сайтов, находящихся в юрисдикции зарубежных стран; высокий уровень подготовки и непубличный характер деятельности организаторов экстремистских сообществ и организаций, а также лиц, осуществляющих финансирование их деятельности; специфика функционирования отдельных технических средств, которая зачастую вызывает у практических сотрудников трудности, свя-

¹ Воронова О. Е., Трушин А. С. Современные информационные войны: стратегии, типы, методы, приемы. М.: Аспект Пресс, 2021. С. 46.

² См. Приложение 1.

занные с недостатком необходимых знаний, что в свою очередь снижает эффективность их деятельности по выявлению киберэкстремистских преступлений.

Характеризуя структуру криминального киберэкстремизма, отметим, что в ней преобладают преступления, совершаемые по политическим мотивам (около 44,9%). Около 26,1% киберэкстремистских преступлений сегодня совершается по мотивам религиозной ненависти и вражды. По идеологическим мотивам, а также по мотивам национальной ненависти и вражды с использованием ИТТ в среднем совершается 12,8% и 16,2% преступлений соответственно.

В ходе исследования нами также определена тенденция к усилению роли недостоверной информации в деструктивном информационно-психологическом воздействии на население.

§ 3. Криминологическая характеристика личностей киберэкстремистов и их влияние на формирование экстремистских воззрений у населения

Необходимость изучения криминологической характеристики преступника обусловлена стремлением понять все важные с юридической точки зрения обстоятельства неправомерного поведения для разработки эффективных мер предупреждения. Как справедливо отмечает Ю. М. Антонян, изучение личности преступника представляет собой одну из ключевых задач на пути к эффективному противодействию преступным проявлениям¹.

Обратимся к мнениям исследователей относительно определения понятия личности преступника.

М. П. Клейменов определяет личность преступника как совокупность социально значимых свойств, определяющих виновное совершение преступления, меру социальной патологии в человеке².

По мнению А. И. Долговой, личность преступника характеризуется следующими групповыми признаками: социально-демографические; уголовно-правовые;

¹ Антонян Ю. М., Тимошина Е. М. Причины преступности в России: монография. М.: ВНИИ МВД России, 2013. 348 с.

² Клейменов М. П. Криминология: учебник. М.: Норма, 2009. С. 89.

социальные проявления в разных сферах жизнедеятельности или социальные связи и нравственно-психологические характеристики. Аналогичный подход к определению личности преступника демонстрируют такие ученые-криминологи, как Ю. М. Антонян, П. С. Дагель, Н. С. Лейкина, А. Б. Сахаров и др.¹

Изучению личности экстремиста посвящено множество научных работ. Данный вопрос, в частности, рассматривали Ю. М. Антонян, А. В. Ростокинский, Я. И. Гишинский, И. Ю. Сундиев, В. В. Аванесян, Е. Н. Юрасова, Ю. Т. Касперович, М. Д. Давитадзе, В. И. Шиян, Л. А. Айвар, И. Л. Трунов и др.²

Среди наиболее общих характеристик личности экстремиста принято выделять его стремление к открытому противопоставлению себя другим людям или группам людей, объединенных по определенному признаку, а также стремление к радикальному, зачастую насильственному достижению своих целей. Как справедливо отмечает в своем исследовании А. В. Петрянин, одной из главных отличительных черт личности экстремиста является его стремление противопоставить себя другим людям, которые не разделяют его убеждений³.

Однако полагаем, что криминологическая характеристика киберэкстремистов в значительной мере отличается от характеристики лиц, которые совершают экстремистские преступления без использования ИТТ. Указанная гипотеза в первую очередь основана на особенностях функционирования наиболее распространенных ИТТ, которые характеризуются тем, что у экстремиста при воздействии на пользователей фактически отсутствует возможность непосредственного физического контакта с потенциальной жертвой. Большинство экстремистов, которые осуществляют свою деятельность в киберпространстве, по-прежнему стремятся противопоставить себя лицам, которые не разделяют их убеждений. Однако данное противостояние возможно только в киберпространстве. Киберэкстремисты

¹ Криминология: учебник / под общ. ред. А. И. Долговой. 3-е изд., перераб. и доп. М.: Норма, 2008. С. 330.

² Экстремизм и его причины: монография / Ю. М. Антонян, А. В. Ростокинский, Я. И. Гишинский [и др.]; под ред. Ю. М. Антоняна. М.: Логос, 2020. 312 с.

³ Петрянин А. В. Концептуальные основы противодействия преступлениям экстремистской направленности: теоретико-прикладное исследование: монография. М.: Проспект, 2017. С. 221.

в большинстве случаев могут осуществлять только информационно-психологическое воздействие на других лиц.

При определении криминологической характеристики личностей киберэкстремистов считаем необходимым отдельно рассматривать личностные особенности представителей организованного уголовного киберэкстремизма и лиц, чьи деяния не связаны с каким-либо экстремистским сообществом или организацией. Полагаем, что характеристика личности киберэкстремиста, целенаправленно действующего в интересах организованного экстремистского объединения (в роли как участника, так и руководителя), значительно отличается от характеристики лица, которое действует единолично.

При рассмотрении криминологической характеристики личности киберэкстремиста, деяния которого не связаны с деятельностью какого-либо экстремистского сообщества или организации, нами преимущественно будут использованы сведения относительно лиц, совершивших преступления, предусмотренные ч. 2 ст. 280 УК РФ (Публичные призывы к экстремистской деятельности, совершенные с использованием средств массовой информации либо информационно-телекоммуникационных сетей, в том числе сети «Интернет»), поскольку данное преступление является наиболее часто совершаемым среди рассматриваемых киберэкстремистов. Удельный вес преступлений, зарегистрированных по данной статье, в общей совокупности всех киберэкстремистских деяний, не связанных с деятельностью экстремистских сообществ или организаций, в 2024 году составил 56,5%. Также объективная сторона данного состава преступления не предполагает участие (или организацию) в деятельности экстремистских сообществ и организаций, а значит, сведения о данных лицах в полной мере удовлетворяют целям настоящего исследования и позволяют охарактеризовать наиболее важные криминологические особенности их личности.

Начнем с рассмотрения социально-демографических признаков, которые являются неотъемлемой частью криминологической характеристики личности преступника.

Большинство киберэкстремистов рассматриваемой группы на момент совершения преступления были в возрасте от 30 до 49 лет (66,8%)¹. В 23,4% случаев указанные преступления совершили лица в возрасте 18–29 лет. Весьма незначительной (4%) является доля несовершеннолетних.

Указанное обстоятельство является весьма специфичным и выделяющимся на фоне распространенного мнения о том, что большинство преступлений экстремистской направленности в киберпространстве совершается молодыми людьми в возрасте до 24–25 лет. Согласно результатам проведенного нами социологического опроса, на вопрос: «Какой средний возраст лиц, совершающих преступления экстремистской направленности с использованием информационно-телекоммуникационных технологий?» – 60,4% практических сотрудников полиции ответили, что в большинстве случаев киберэкстремистские преступления совершают лица в возрасте от 18 до 25 лет².

Вместе с тем полагаем, что сегодня все же прослеживается тенденция к уменьшению количества рассматриваемых деяний, совершенных лицами в возрасте 18–29 лет. В своей работе Д. Н. Еремин отмечает, что по состоянию на 2011 г. доля молодых людей, совершивших преступления экстремистской направленности с использованием ИТТ, составляла 70%³. В исследовании И. В. Букова содержится информация о том, что в 2018 г. данный показатель составлял 57%⁴. Согласно статистическим сведениям в 2021 г. удельный вес молодых людей рассматриваемого возраста в структуре лиц, совершивших киберэкстремистские преступления рассматриваемой группы, составил уже 42%. В 2022 г. данный показатель составил 35,9%; в 2023 – 20,4%; в 2024 – 22,6%.

Учитывая тенденцию к стабильному увеличению среднего возраста лиц из рассматриваемой группы, можно сделать вывод о том, что вышеуказанные пре-

¹ Здесь и далее по тексту параграфа использованы официальные статистические данные ГИАЦ МВД России.

² См. Приложение 2.

³ Еремин Д. Н. Применение дерматоглифических исследований в решении следственных задач при расследовании преступлений, связанных с экстремизмом // Вестник Балтийского федерального университета им. И. Канта. 2011. № 9. С. 138-142.

⁴ Буков И. В. Криминалистическая характеристика личности преступника экстремиста в Интернете // Вестник науки. 2019. № 1. С. 57-60.

ступления совершают люди, родившиеся примерно в один и тот же временной промежуток (в 70–90-х гг. XX века). На наш взгляд, указанный факт свидетельствует о необходимости более подробно рассмотреть комплекс детерминирующих факторов, которые были актуальны в данный период и привели к формированию экстремистских взглядов и убеждений у рассматриваемой категории граждан. Данная проблематика будет рассмотрена нами позднее, в рамках параграфа, посвященного предпосылкам уголовного киберэкстремизма.

Перейдем к рассмотрению такой социально-демографической характеристики, как пол преступника. В ходе исследования установлено, что в 2024 г. наиболее часто киберэкстремистские преступления совершали мужчины (в 93,4% случаев). Данный показатель остается неизменным на протяжении последних лет. Примечательно, что доля женщин значительно ниже (около 6–7%) в сравнении с показателями, характеризующими долю женской преступности в общей массе совершаемых в Российской Федерации преступлений (около 15–16%). Полагаем, что данный факт обусловлен традиционным для нашего общества мнением, согласно которому женщина, как правило, не воспринимается в качестве воинственной фигуры, способной призывать к радикальным и (или) насильственным действиям.

Рассматривая уровень образования киберэкстремистов, деяния которых не связаны с экстремистским сообществом или организацией, отметим, что рассматриваемые лица чаще всего имеют среднее профессиональное (40,8%) или среднее общее образование (23,1%). В то же время значительной является и доля преступников с высшим образованием (21,1%). Достаточный уровень образования вполне позволяет киберэкстремистам грамотно формулировать свою идеологическую позицию и пользоваться различными возможностями ИТТ (например, написать привлекающую внимание публикацию, содержащую призывы к экстремизму, в социальных сетях).

Еще одной немаловажной социально-демографической характеристикой личности является род занятий. Установлено, что рассматриваемые киберэкстремисты чаще всего являются трудоспособными людьми, но без постоянного места

работы (42,3%) или работниками промышленного сектора (34,3%). Данный факт, по нашему мнению, может свидетельствовать о том, что данные лица могут быть не удовлетворены своим финансово-материальным положением и (или) условиями труда.

Далее рассмотрим уголовно-правовую характеристику личности киберэкстремиста, деяния которого не связаны с деятельностью экстремистских сообществ или организаций. Характеризуя сами преступления, совершаемые рассматриваемыми лицами, отметим, что в большинстве случаев они обладают средней степенью тяжести. В качестве объектов их преступных посягательств могут выступать: основы конституционного строя и безопасности государства; общественная безопасность и общественный порядок; конституционные права и свободы человека и гражданина; жизнь и здоровье личности (в случае, если речь идет об угрозах убийством или причинением тяжкого вреда здоровью, демонстрируемых посредством ИТТ).

Чаще всего деяния рассматриваемых лиц выражаются в систематическом распространении путем размещения на своих личных страницах в социальных сетях и мессенджерах информации, содержащей: публичные призывы к экстремистской деятельности; оскорбления и иные негативные высказывания, выражающие ненависть в отношении какой-либо социальной группы, объединенной по политическому, религиозному, национальному, расовому или иному признаку. Также данные киберэкстремисты иногда размещают указанную информацию не на своей личной странице, а в комментариях под общедоступными и не имеющими отношения к экстремизму публикациями других пользователей или сообществ.

В ходе исследования нами также установлен следующий ряд особенностей уголовно-правовой характеристики лиц рассматриваемой группы:

1. В большинстве случаев они совершают преступления в одиночку. Как отмечает в своем исследовании Н. А. Андреев, до 99% преступлений, предусмотр-

ренных ст. 280 УК РФ, совершается единолично¹. Указанный тезис также подтверждается и данными судебной статистики. В 2024 г. из числа осужденных по ч. 2 ст. 280 УК РФ не было ни одного, кто совершил бы указанное преступление в составе группы.

2. Довольно часто рассматриваемые лица совершают киберэкстремистские преступления исключительно от своего имени, из своих личных побуждений, не упоминая при этом идеи какого-либо экстремистского сообщества или организации. Данный вывод основан на результатах проведенного нами анализа материалов 54 приговоров по ч. 2 ст. 280 и ч. 2 ст. 282 УК РФ за 2023–2024 гг. В тексте большинства материалов (39) отсутствует упоминание о том, что действия подсудимого имеют отношение к распространению идеологии какого-либо конкретного экстремистского сообщества. Также в ходе проведенного нами анкетирования 56,25% сотрудников ЦПЭ согласились с мнением о том, что киберэкстремистские преступления чаще всего совершаются лицами, не относящими себя к экстремистской организации, действующими без инструкций и сугубо из своих личных побуждений².

3. Чаще всего рассматриваемые киберэкстремисты не были ранее судимы. В 2024 г. на момент совершения преступления лишь 8,6% лиц имели не снятые и не погашенные на момент судебного рассмотрения судимости. Однако нельзя с полной уверенностью утверждать, что указанные лица до этого не совершали киберэкстремистские преступления. Как нами уже отмечалось ранее, криминальный киберэкстремизм характеризуется высоким уровнем латентности.

Переходя к рассмотрению нравственно-психологической характеристики личности киберэкстремиста, деяния которого не связаны с деятельностью экстремистских сообществ или организаций, отметим, что основу данной характеристики

¹ Андреев Н. А. Криминологическая характеристика личности преступника, совершающего преступления экстремистской направленности в сети Интернет // Вестник Краснодарского университета МВД России. 2023. № 1. С. 35.

² См. Приложение 1.

личности любого преступника составляет ее сфера мотивации, поскольку она опредмечивает потребности личности и стимулирует ее криминальное поведение¹.

На наш взгляд, ключевой нравственно-психологической характеристикой для всех киберэкстремистов рассматриваемой группы является их стремление сподвигнуть других людей на совершение преступлений экстремистской направленности, не предпринимая активных действий самостоятельно. Такая возможность во многом обуславливается опосредованным характером их общения с лицами, на которых они оказывают деструктивное информационно-психологическое воздействие. В свою очередь особенности функционирования наиболее распространенных ИТТ характеризуются тем, что у киберэкстремиста есть возможность оказывать деструктивное информационно-психологическое воздействие на пользователей исключительно в киберпространстве, без непосредственного общения. При этом зачастую основной «целью» киберэкстремистов является молодежь как наиболее физически активная, внушаемая и импульсивная часть общества².

Как нами уже отмечалось ранее, сегодня все чаще преступления экстремистской направленности с использованием ИТТ совершают люди в возрасте 30–49 лет, однако в качестве объекта своего деструктивного информационно-психологического воздействия они чаще всего избирают молодых людей, преимущественно в возрасте до 24–25 лет, с целью побудить именно их к совершению преступлений экстремистской направленности уже за пределами киберпространства. О том, что именно молодые люди до 24–25 лет являются основным объектом информационно-психологического воздействия в киберпространстве, свидетельствуют результаты многочисленных научных работ. Например, З. З. Маздогова в своем исследовании особое внимание уделяет проблеме возрос-

¹ Антонян Ю. М., Голубев В. П., Кудряков Ю. Н. Личность корыстного преступника. Томск: Изд-во Том. ун-та, 1989. С. 52-53.

² Ильиных Н. А. Интернет как средство массовой манипуляции молодежью в экстремистских кругах // Актуальные проблемы профилактики преступлений: мат-лы междунар. науч.-практ. семинара. Омск: Омская академия МВД России, 2023. С. 18-21.

шей активности экстремистов в вовлечении в свою деятельность молодежи¹. Как справедливо отмечают в своей работе Д. Д. Мухтаров и Х. Л. Кушхов, в силу неустоявшихся жизненных ориентиров и подверженности манипуляциям со стороны лиц старшего поколения молодежь становится приоритетной целью для экстремистов².

Указанный тезис подтверждается и результатами проведенного нами анкетирования практических сотрудников. При ответе на вопрос: «На какую возрастную категорию лиц чаще всего направлено деструктивное воздействие (кого вовлекают в экстремистскую деятельность)?» – 88,7% опрошенных указали на возрастную категорию лиц до 24–25 лет³.

В свою очередь полагаем, что стремление киберэкстремистов сподвигнуть других людей на совершение преступлений экстремистского характера может свидетельствовать о манипулятивном характере их личности. Главной целью рассматриваемых киберэкстремистов является способствование приобретению другими людьми радикальных взглядов и убеждений с целью побудить их (преимущественно молодежь) совершить экстремистские действия за пределами киберпространства. Таким образом, киберэкстремисты при помощи ИТТ часто стремятся дистанцироваться от личного участия в совершении экстремистским преступлений в «реальном мире», однако, желая наступления определенных негативных последствий, они путем деструктивного информационно-психологического воздействия активно вовлекают других лиц в совершение преступлений экстремистской направленности уже без использования ИТТ⁴.

¹ Маздогова З. З. Предупреждение вовлечения молодежи в террористические и экстремистские организации // Проблемы экономики и юридической практики. 2016. № 5. С. 227-229.

² Мухтаров Д. Д., Кушхов Х. Л. Технологии вовлечения молодежи в экстремистскую деятельность: новые вызовы и пути противодействия // Журнал прикладных исследований. 2022. № 3. С. 72-74.

³ См. Приложение 2.

⁴ Бабурин В. В., Ильиных Н. А. Криминологическая характеристика личности киберэкстремиста, деяния которого не связаны с организацией экстремистского сообщества или организации // Психопедагогика в правоохранительных органах. 2025. № 2. С. 234-240.

Помимо определенных наиболее общих личностных характеристик, большое количество совершаемых киберэкстремистских преступлений неорганизованного характера позволяет сделать предположение о наличии внутри рассматриваемой группы киберэкстремистов отличных друг от друга подгрупп лиц, что обуславливает целесообразность выделения дополнительной их классификации.

На сегодняшний день в доктрине весьма досконально проработаны и обоснованы классификации личностей экстремистов. Например, Р. С. Тамаев выделяет две группы экстремистов: экстремист, преимущественно осуществляющий свою преступную деятельность в регионах, где имеют место ложно понимаемые идеи «суверенитета» республик в составе Российской Федерации, борьбы за национальную «независимость», с высоким уровнем насильственной преступности (Чечня, Ингушетия, Дагестан и т.д.); экстремист, совершающий соответствующие преступления преимущественно в других российских регионах, как правило, крупных мегаполисах, финансовых и промышленных центрах¹.

В своем исследовании Р. М. Узденов определяет следующие типы экстремистов: а) идейно-самостоятельный тип – личность, осознанно и целенаправленно вступившая на путь экстремизма, самостоятельно осмысливающая и анализирующая существующее положение вещей и желающая это положение изменить; б) зависимый тип («экстремист за компанию») – личность, чья социальная позиция формируется главным образом за счет активного внешнего воздействия досуговой микросреды, СМИ и других подобных раздражителей².

Обоснованно представлена классификация экстремистов также в работе А. В. Петрянина. В зависимости от мотивации и роли автор выделяет следующие виды экстремистов: экстремист-лидер, экстремист-исполнитель, экстремист-мститель, экстремист-альтруист³.

¹ Тамаев Р. С. Организация правоохранительной деятельности в сфере противодействия экстремизму: автореф. дис. ... д-ра юрид. наук. М., 2010. С. 27.

² Узденов Р. М. Экстремизм: криминологические и уголовно-правовые проблемы противодействия: автореф. дис. ... канд. юрид. наук. М., 2008. С. 9.

³ Петрянин А. В. Концептуальные основы противодействия преступлениям экстремистской направленности: теоретико-прикладное исследование: монография. М.: Проспект, 2017. С. 218.

Полагаем, что вышеприведенные категории могут быть применены и для типизации киберэкстремистов, чьи деяния не связаны с деятельностью экстремистских сообществ и организаций. Однако данные основания классификации не учитывают особенности совершения преступлений именно в киберпространстве. Полагаем, что рассматриваемую группу киберэкстремистов целесообразно подразделять в зависимости от их отношения к сохранению анонимности на 2 подкатегории: «неосмотрительные» и «осторожные».

Первая, наиболее часто выявляемая и многочисленная подкатегория (по результатам анализа материалов судебной практики составляют около 80% среди всех киберэкстремистов, чьи деяния не связаны с деятельностью экстремистских сообществ и организаций) – «неосмотрительные» киберэкстремисты. Данные лица совершают преступления, особенно не задумываясь о сохранении своей анонимности и последствиях. Чаще всего ввиду недостаточного уровня грамотности в области функционирования ИТТ, принимая анонимность в киберпространстве за константу, рассматриваемые киберэкстремисты, не предпринимая достаточных действий для сокрытия своей личности, опрометчиво полагают, что установить их личность будет невозможно.

В качестве примера можно привести действия гражданина И., который, согласно материалам судебного решения, зарегистрировался в социальной сети «ВКонтакте» с использованием своего личного номера телефона (чего уже более чем достаточно для установления личности владельца страницы). При этом гражданин И. во время регистрации указал имя пользователя «Ivan Ivanov» (отличающееся от его настоящего имени и фамилии), опрометчиво полагая, что таким образом он сможет полностью скрыть свою личность¹.

Помимо недостатка специальных знаний по сохранению своей анонимности в киберпространстве, киберэкстремисты из рассматриваемой группы часто очень внушаемые, вследствие чего нередко могут действовать импульсивно, под воздействием сиюминутно возникших чувств (например, на фоне просмотра какого-

¹ Приговор Кумторкалинского районного суда Республики Дагестан от 15 августа 2023 г. по делу № 1-102/2023. Доступ из справ.-правовой системы «ГАРАНТ».

либо экстремистского видеоматериала со сценами жестокости и насилия, способными моментально вызывать негативные эмоции у зрителя). В свою очередь возможности ИТТ создают благоприятные условия для моментального «выражения» своих внезапно возникших эмоций в форме высказываний экстремистского содержания, например, в комментариях к публикации в крупном новостном сообществе в социальной сети.

Сегодня время от момента возникновения умысла до непосредственного совершения преступления экстремистской направленности в киберпространстве ограничивается лишь секундами, затраченными на набор текста в телефоне. В таком случае исключается вероятность, что потенциальный преступник может еще раз обдумать свои намерения и отказаться от совершения преступления. Ярким примером здесь могут служить положения приговора Сармановского районного суда Республики Татарстан от 28 июня 2023 г., согласно которым подсудимый так описывает свои действия в момент совершения преступления: «Ну и сам, не контролируя свои эмоции, используя свою персональную страницу «ВКонтакте», выложил свои комментарии, и так получилось, что выразился слишком грубо, призывая к насилию...»¹.

Ситуация здесь усугубляется тем, что, как показывают результаты исследований, посвященных изучению личности экстремиста, данные лица часто совершают преступления экстремистской направленности в состоянии алкогольного или наркотического опьянения². В свою очередь опьянение может служить катализатором импульсивных действий.

Полагаем, что данным лицам могут быть присущи такие признаки психологического экстремиста, как нарушение личности, психопатия, невротические расстройства. Нередко рассматриваемых киберэкстремистов можно отнести к случайному типу личности, т.е. человек не обладает ярко выраженными и стабильными экстремистскими убеждениями, но под воздействием определенных обстоя-

¹ Приговор Сармановского районного суда Республики Татарстан от 28 июня 2023 г. по делу № 1-46/2023. Доступ из справ.-правовой системы «ГАРАНТ».

² Тамбиев С. А. Криминологическая характеристика личности экстремиста // Журнал прикладных исследований. 2022. № 2. С. 58.

тельств (например, групповой динамики, влияния окружения) может прийти к экстремистским действиям¹.

Далее оценим влияние «неосмотрительных» киберэкстремистов на формирование экстремистских воззрений у населения, определив ряд ключевых позиций:

1) как правило, деятельность рассматриваемых лиц достаточно быстро пресекается за счет возможности оперативно установить их личность;

2) данные киберэкстремисты при осуществлении, например, публичных призывов к экстремистской деятельности редко аргументируют свою «позицию», ограничиваясь исключительно оскорблениями и призывами. В свою очередь, сообщения подобного содержания значительно реже находят отклик у других пользователей и едва ли способны сформировать у них устойчивые экстремистские воззрения;

3) в результате изучения материалов судебной практики удалось установить, что в большинстве случаев круг интересов данной категории киберэкстремистов к каким-либо событиям ограничивается географией населенного пункта или региона, где они проживают. Как правило, их действия выражаются в распространении информации экстремистского содержания в сообществах социальных сетей и мессенджеров, в которых состоят преимущественно местные жители конкретного региона или населенного пункта. Подобные сообщества зачастую обладают сравнительно небольшой аудиторией, а события, освещаемые и обсуждаемые в них, в большинстве случаев касаются исключительно какого-то конкретного населенного пункта или региона, что делает их более актуальными и насущными для местных жителей, но гораздо менее интересными для пользователей, проживающих в другой местности. В результате потенциальный круг лиц, на которых действия рассматриваемой категории киберэкстремистов могут оказывать негативное информационно-психологическое воздействие, как правило, ограничивается пользователями, проживающими в одной местности.

¹ Юзиханова Э. Г., Корсикова Н. А. Криминологический анализ экстремизма в молодежной среде на современном этапе развития общества // Правопорядок: история, теория, практика. 2024. № 4. С. 168.

Таким образом, оценивая влияние неосмотрительных киберэкстремистов на формирование экстремистских воззрений у населения, отметим, что их негативное информационно-психологическое воздействие на общество достаточно опасно. Однако в целом их деятельность представляется наименее целенаправленной и эффективной в сравнении с действиями киберэкстремистов других категорий.

Переходя к рассмотрению такой подкатегории, как «осторожные» киберэкстремисты, деяния которых не связаны с деятельностью экстремистских сообществ или организаций, отметим, что сегодня достаточно сложно оценить их реальное количество. Лица рассматриваемой группы отличаются значительно более ответственным подходом к сохранению своей анонимности. Как правило, к моменту, когда правоохранительным органам все же удастся установить его личность, он уже успевает совершить целый ряд киберэкстремистских преступлений, оказав негативное информационно-психологическое воздействие на множество пользователей.

Ярким примером, характеризующим киберэкстремистов рассматриваемой группы, могут служить материалы приговора Сулейман-Стальского районного суда Республики Дагестан от 14 ноября 2022 г.¹ Следствием было доказано, что гражданин Х. до момента его задержания успел совершить 10 эпизодов киберэкстремистского преступления, предусмотренных ч. 2 ст. 280 УК РФ, при этом действовал весьма осторожно. Для сохранения своей анонимности подсудимый создал по меньшей мере 8 разных аккаунтов в социальной сети «ВКонтакте». В результате с момента совершения первого до последнего доказанного эпизода преступления прошло около 2 лет, в течение которых гражданин Х. беспрепятственно осуществлял экстремистскую деятельность, последовательно распространяя материалы экстремистского содержания как на личной странице каждого из его аккаунтов, так и в комментариях к публикациям в различных сообществах социальной сети.

¹ Приговор Сулейман-Стальского районного суда Республики Дагестан от 14 ноября 2022 г. по делу № 1-87/2022. Доступ из справ.-правовой системы «ГАРАНТ».

Продолжая рассматривать криминологическую характеристику «осторожных» киберэкстремистов, следует отметить, что киберпространство само по себе обуславливает определенные психологические особенности взаимодействия между людьми. Данный факт непосредственно сказывается на внутреннем отношении киберэкстремиста к тем действиям, которые он совершает. В своем исследовании К. С. Есаулова среди прочих отличительных черт интернет-коммуникации выделяет психологическую раскрепощенность и стремление к нетипичному, ненормативному поведению. Описывая такое явление, как «социальная смелость», автор приходит к обоснованным выводам о том, что в ходе общения в киберпространстве «человек презентует себя с другой стороны, чем в условиях реальной социальной жизни, можно сказать, что примеряет на себя роли, проигрывает сценарии, которые не может реализовать вне сети. Мнимая раскрепощенность, некоторая безответственность приводит к тому, что человек может проявлять и чаще всего и проявляет свободу мыслей и нетипичных поступков...»¹.

Таким образом, можно сделать вывод о том, что рассматриваемые киберэкстремисты нередко могут вести «двойную» жизнь. В киберпространстве под вымышленным именем, например, в социальной сети, они активно осуществляют экстремистскую деятельность, в то же время никак ее не проявляя в реальном мире. Примером здесь могут послужить сведения, содержащиеся в приговоре Миасского городского суда Челябинской области от 19 мая 2023 г.² Из показаний супруги подсудимого следует, что даже она не знала о том, что ее муж размещал на своей странице «ВКонтакте» публикации экстремистского содержания. О том, что экстремистские действия подсудимого ограничивались лишь киберпространством, свидетельствует и тот факт, что по месту работы он характеризовался исключительно положительно, активно участвовал в спортивной и общественной жизни, не судим, на учете у нарколога не состоял, проживал с семьей.

¹ Есаулова К. С. К определению социальной смелости: в реальной жизни и интернет-коммуникации // Вестник РГГУ. Серия «Психология. Педагогика. Образование». 2016. № 2. С. 54.

² Приговор Миасского городского суда Челябинской области от 19 мая 2023 г. по делу № 1-278/2023. Доступ из справ.-правовой системы «ГАРАНТ».

Учитывая все вышеуказанные характеристики, оценим уровень влияния действий «осторожных» киберэкстремистов на формирование экстремистских воззрений у населения:

1) противоправная деятельность рассматриваемых лиц может быть достаточно длительной. С учетом осторожности их действий правоохранительным органам бывает весьма затруднительно установить личность такого киберэкстремиста. В свою очередь, чем дольше данные лица осуществляют свою деятельность, тем больше потенциальное число пользователей, у которых они могут сформировать экстремистские воззрения;

2) лица из рассматриваемой группы киберэкстремистов, как правило, неизвестны широкому кругу общественности. Скрываясь под масками разных аккаунтов в киберпространстве, крайне сложно обрести известность. Таким образом, в подавляющем большинстве случаев данные лица не способны оказывать негативное информационно-психологическое воздействие одномоментно на общество в целом или на значительную его часть. Тем не менее данные киберэкстремисты своими действиями стремятся охватить как можно больше пользователей;

3) в части, касающейся желания охватить своим негативным информационно-психологическим воздействием как можно большее количество пользователей, действия рассматриваемых лиц имеют общие черты с деятельностью организаторов экстремистских сообществ или организаций. Тем не менее они все же не являются организаторами. У рассматриваемых киберэкстремистов, как правило, нет лидерских качеств. Более того, у них отсутствует само желание руководить и организовывать деятельность других людей. Данные киберэкстремисты преследуют цель лишь подстрекать к совершению экстремистских преступлений других людей, не желая при этом непосредственно возглавлять и организовывать их деятельность;

4) от «неосмотрительных» киберэкстремистов лиц рассматриваемой подкатегории отличает также последовательность действий. В большинстве случаев они осуществляют свою деятельность на систематической основе. Для того, чтобы донести свои идеи до как можно более многочисленной аудитории, рассмат-

риваемые лица могут создавать собственные сообщества в социальных сетях, мессенджерах, на отдельных интернет-сайтах и т.д. Например, рассмотренный нами ранее приговор в отношении гражданина Х. содержит информацию о том, что он создал по меньшей мере два публичных сообщества («Воинствующий Атеист» и «Лезгейстан») в социальной сети «ВКонтакте».

Таким образом, действия «осторожных» киберэкстремистов способны оказывать значительное влияние на формирование экстремистских воззрений у населения. Наличие определенных знаний по сохранению своей анонимности в киберпространстве позволяет им достаточно длительное время оставаться вне поля зрения правоохранительных органов. Данный факт в совокупности с систематичностью их деятельности позволяет утверждать о том, что влияние данных киберэкстремистов на формирование у населения экстремистских воззрений достаточно велико и весьма опасно, поскольку носит более устойчивый и целенаправленный характер.

Переходя к изучению вопроса о личностных характеристиках представителей организованного уголовного киберэкстремизма, в первую очередь следует отметить, что данная преступность сегодня все чаще носит преимущественно транснациональный характер¹. Как справедливо отмечают в своем исследовании В. В. Меркуев и О. В. Боброва, сегодня в указанных процессах растет роль экстремистских организаций, курируемых зарубежными странами².

Полагаем, что современная организованная киберэкстремистская преступность все больше приобретает черты транснациональной организованной преступности (ТОП). В своем исследовании И. М. Клейменов определяет ТОП как явление, которое существует в «глобальном пространстве и представляет собой организованную преступную деятельность, связанную с перемещением потоков

¹ Ильиных Н. А. Отдельные аспекты характеристики личности лица, осуществляющего публичные призывы к экстремистской деятельности в Интернете // Актуальные проблемы борьбы с преступностью: вопросы теории и практики: мат-лы XXVI междунар. науч.-практ. конф. Красноярск: Сибирский юридический институт МВД России, 2023. С. 135.

² Боброва О. В., Меркуев В. В. Радикальные религиозные организации угроза национальной безопасности и средства противодействия им // Обозреватель. 2022. № 10. С. 106-126.

информации, денег, физических объектов, людей и других средств через государственные границы»¹.

Автор также отмечает, что уже в 2014 г. стала усиливаться политическая мотивация в деятельности ТОП. На тот период особо актуальной была проблема, связанная с деятельностью международной террористической организации «Исламское государство Ирака и Леванта» (ИГИЛ)². В данной организации было два основных лидера: Абу Хафс аль-Хашими аль-Кураши и Абу Фатима аль-Джахейши, которые преследовали свои цели, продиктованные их религиозными убеждениями. Однако, как справедливо отмечает в своем исследовании Ю. А. Михалёв, сама террористическая организация ИГИЛ была лишь одним из инструментов внешней политики других государств, который они использовали для внесения смуты и разжигания конфликтов в странах Ближнего Востока в целях установления «марионеточного» политического режима и доступа к углеводородным ресурсам³.

В связи с этим полагаем, что можно говорить об экстремистской направленности не только непосредственных лидеров ИГИЛ в лице Абу Хафс аль-Хашими аль-Кураши и Абу Фатима аль-Джахейши, но и отдельных государств, которые активно поддерживают (в первую очередь финансово) соответствующие региональные радикальные движения. При этом безусловным видится превосходство по степени организованности государственных структур над какой-либо иной формой объединения людей. Тем не менее рассмотрение целых государств как субъектов киберэкстремистской деятельности преимущественно является предметом изучения политологии, но не криминологии. В рамках настоящего исследования наибольший интерес все же представляет криминологическая характеристика личности киберэкстремистов, действующих в составе организован-

¹ Клейменов И. М. Сравнительная криминология: криминализация, преступность, уголовная политика в условиях глобализации: автореф. дис. ... д-ра юрид. наук. Омск, 2015. С. 11.

² Здесь и далее по тексту при упоминании данной организации: «Деятельность организации запрещена Решением Верховного Суда Российской Федерации от 29 декабря 2014 г. № АКПИ 14-1424С по основаниям осуществления террористической и экстремистской деятельности».

³ Михалёв Ю. А. «Исламское государство» в политике США // Вестник Московского государственного лингвистического университета. Общественные науки. 2018. № 2. С. 92.

ных экстремистских сообществ и организаций. Однако необходимо учитывать, что сегодня за ними нередко могут стоять государственные структуры зарубежных стран, а также аффилированные ими коммерческие организации.

Представителей организованного уголовного киберэкстремизма отличает целеустремленность их намерения участвовать в скоординированной экстремистской деятельности. Такие лица однозначно осознают свою принадлежность к экстремистскому сообществу или организации, дают согласие на участие в нём и выполняют любые по характеру, но обязательно причинно обусловленные членством действия. В своем исследовании З. М. Бешукова утверждает: «Членство в экстремистском сообществе выражается в даче лицом согласия (как показывает судебная практика, в большинстве своем оно устное); принятии на себя определенных обязательств...»¹. Как справедливо отмечает С. А. Пичугин, «обязательным условием уголовной ответственности за создание экстремистского сообщества, руководство им (его частью или входящими в такое сообщество структурными подразделениями) или участие в нем является осознание лицом общих целей функционирования такого сообщества, его части или структурного подразделения – подготовки либо совершения преступлений экстремистской направленности – и своей принадлежности к нему»².

Данные лица в полной мере осознают всю общественную опасность своей деятельности и часто действуют скрытно. Например, в приговоре Ленинского районного суда г. Махачкалы Республики Дагестан от 22 ноября 2021 г. содержится следующая информация: «Всем участникам религиозного объединения «...», деятельность которого возобновил ФИО16 А.Н, а именно: ему, ФИО21, гражданину З., ФИО89, ФИО20, Свидетелю № 4, Свидетелю № 2, Свидетелю № 5, Свидетелю № 1, Свидетелю № 3 и ФИО2 было известно, что данная идеология запрещена в Российской Федерации, поскольку считается антиконституцион-

¹ Бешукова З. М. Участие в экстремистском сообществе: некоторые вопросы законодательного регулирования и правоприменения // Полицейская деятельность. 2016. № 5. С. 499.

² Пичугин С. А. Организация экстремистского сообщества по российскому уголовному законодательству: нормативная регламентация и практика применения // Вестник Владимирского юридического института. 2022. № 4. С. 89.

ной и экстремистской, поэтому они на тот период вели себя очень скрытно и в свой круг общения лишних людей не подпускали. С ФИО8 они обсуждали религиозные вопросы в ходе переписки в мессенджере «WhatsApp», и у них имелась группа, куда входили он и указанные выше им лица»¹.

О преимущественно скрытном характере действий представителей организованного уголовного киберэкстремизма косвенно свидетельствует и тот факт, что рассматриваемые лица нередко выступают в роли главных инициаторов создания экстремистских материалов, однако они не распространяют их лично, что также позволяет им оставаться вне поля зрения правоохранительных органов. Как справедливо отмечает в своем исследовании М. В. Ульянов, непосредственные авторы экстремистских материалов и лица, инициирующие их вброс в киберпространство, часто не устанавливаются².

Вместе с тем общей характеристикой в поведении рассматриваемых киберэкстремистов является их высокая восприимчивость к достижениям научно-технического прогресса, активное использование его результатов в экстремистских целях (например, активное использование цифровых инструментов коммуникации в информационно-телекоммуникационном пространстве)³. Данный факт свидетельствует о способности представителей организованного уголовного киберэкстремизма более умело скрывать свою личность в киберпространстве. Полагаем, что благодаря данному обстоятельству в большинстве случаев личность участников экстремистских сообществ и организаций удастся определить только в связи с их деятельностью за пределами киберпространства. По данным за 2024 г. из 311 зарегистрированных по ст. 282.2 УК РФ преступлений лишь 81 было совершено с использованием ИТТ.

¹ Приговор Ленинского районного суда г. Махачкалы Республики Дагестан от 22 ноября 2021 г. по делу № 1-717/2021. Доступ из справ.-правовой системы «ГАРАНТ».

² Ульянов М. В. Миграционные процессы в системе детерминант экстремистской преступности: монография. М.: Юрлитинформ, 2019. С. 32.

³ Давыдов В. О. Экстремизм 2.0: криминалистически значимые аспекты организованного преступного формирования экстремистской направленности // Философия права. 2023. № 4. С. 124.

Далее рассмотрим особенности социально-демографической характеристики представителей организованного криминального киберэкстремизма. Для указанных целей нами преимущественно были использованы статистические сведения о лицах, совершивших преступления, предусмотренные ч. 1 ст. 282.1 и ч. 1, 3 ст. 282.2 УК РФ.

Чаще всего указанные преступления совершают мужчины в возрасте от 30 до 49 лет (56,5%).

В подавляющем большинстве киберэкстремисты рассматриваемой группы имеют постоянное место работы. Доля безработных в общей совокупности данных лиц в 2024 стремится к нулю. Вместе с тем значительной является доля тех, кто занят трудом, однако не имеет постоянного источника дохода и не трудоустроен официально (27,1%).

Характеризуя уровень образования, отметим, что киберэкстремисты, занимающиеся организационной деятельностью, как правило, наиболее подготовлены. О данном факте свидетельствуют статистические данные, характеризующие долю данных лиц с высшим образованием. Данный показатель у рассматриваемых лиц составляет 52,4% против 21,1% у киберэкстремистов, деяния которых не связаны с организационной деятельностью.

Считаем, что более высокий уровень образования позволяет сделать предположение о наличии у рассматриваемых лиц специальных знаний по наиболее эффективному деструктивному информационно-психологическому воздействию на пользователей. Например, как отмечает в своем исследовании А. Б. Юнусова, одним из эффективных приемов психологического воздействия, используемых в радикальных движениях, является эксплуатация образа женщины, чтобы заявить о невинном и ненасильственном характере своей деятельности. Как нами уже отмечалось ранее, данный прием сегодня активно используется киберэкстремистами. Например, представители запрещенной в Российской Федерации организации «Легион «Свобода России» регулярно размещают в киберпространстве информацию о женщинах, которые непосредственно участвуют в деятельности

их движения или оказывают им активное содействие¹. Например, одна из таких публикаций содержала в себе информацию о встрече участников движения с британским лингвистом Джейд Селеной МакГлинн, пропагандирующей идеи русофобии и применения насилия в отношении граждан России.

Далее выделим ключевые элементы уголовно-правовой характеристики личности киберэкстремистов, действующих в интересах организованного экстремистского объединения. Преступления, совершаемые рассматриваемыми лицами, определяются как тяжкие. В качестве объекта преступных посягательств в большинстве случаев выступают основы конституционного строя и безопасности государства.

Нередко представителями экстремистских сообществ и организаций могут быть публичные личности, в том числе обладающие служебным положением. Примером здесь может служить деятельность депутата городской Думы г. Томска, которая одновременно являлась координатором экстремистской организации «Штабы Навального»²³.

Помимо непосредственно экстремистских мотивов совершения преступлений, среди данных лиц нередко имеет место корыстный мотив, что справедливо отмечает в своем исследовании, например, С. А. Пичугин⁴.

В большинстве случаев представители организованного криминального киберэкстремизма ранее не были судимы. Чаще всего никакая другая противоправная деятельность, помимо экстремистской, у данных лиц не проявляется. Исклю-

¹ Здесь и далее по тексту при упоминании данной организации: «Деятельность организации запрещена решением Верховного Суда Российской Федерации от 16 марта 2023 г. № АКПИ23-101С по основаниям осуществления террористической и экстремистской деятельности».

² Здесь и далее по тексту при упоминании данной организации: «Деятельность организации запрещена решением Московского городского суда от 9 июня 2021 г. № 3а-1573/2021 по основаниям осуществления экстремистской деятельности».

³ Суд приговорил экс-главу штаба Навального в Томске к девяти годам / РБК. URL: <https://www.rbc.ru/politics/29/12/2023/658e914d9a7947516efa674c> (дата обращения: 12.01.2025).

⁴ Пичугин С. А. Организация экстремистского сообщества по российскому уголовному законодательству: нормативная регламентация и практика применения // Вестник Владимирского юридического института. 2022. № 4. С. 90.

чение здесь составляют экстремисты, действующие в местах лишения свободы, которые значительно реже используют в своих целях возможности ИТТ.

Далее обозначим особенности нравственно-психологической характеристики киберэкстремистов-организаторов как наиболее отличительных в сравнении с другими участниками экстремистских сообществ и организаций. Данным лицам в полной мере присущи общие черты лидеров преступных сообществ или организаций. Изучению личности преступников-организаторов посвящено множество криминологических исследований, основные положения которых совершенно справедливо применимы для определения личностных особенностей киберэкстремистов рассматриваемой группы.

В большинстве случаев факт занятия человеком лидерской позиции в любом преступном сообществе или организации обусловлен наличием у него выдающихся (как минимум на фоне остальных участников) интеллектуальных, управленческих и физических качеств. Как нами уже отмечалось ранее, именно на организатора возлагается обязанность по привлечению новых членов, поддержанию дисциплины и т.д. Для лидеров экстремистских сообществ или организаций также одной из ключевых является задача по повышению узнаваемости их объединения и основных идей в обществе. Такую деятельность в некотором смысле можно сравнить с продвижением товарного бренда. Как справедливо отмечают в своем исследовании Н. И. Верченко и Е. Ю. Чубриков, «современная организованная преступность – это бизнес, в котором у организатора должны быть соответствующие способности: коммуникабельность, предприимчивость, независимость мышления, высокий интеллект и т. д.»¹.

Важно отметить систематичность и последовательность деятельности представителей организованного криминального киберэкстремизма в киберпространстве. Данный факт выражается в регулярном распространении противо-

¹ Чубриков Е. Ю. Личность организованного преступника и детерминанты организованного преступного поведения // Развитие уголовно-исполнительной системы: организационные, правовые и экономические аспекты: сб. мат-лов междунар. науч.-практ. конф. в рамках международного юридического форума «Право и экономика: национальный опыт и стратегии развития». Новосибирск, Новокузнецк: Новосибирский государственный университет экономики и управления; Кузбасский институт ФСИН России, 2021. С. 172-176.

правного контента от лица различных экстремистских сообществ или организаций с использованием всех доступных ИТТ. Например, лица, обеспечивающие пропагандистскую деятельность запрещенной организации «Полк Азов», регулярно публикуют одни и те же экстремистские материалы сразу на нескольких доступных площадках, добиваясь тем самым наибольшего охвата аудитории¹.

Справедливым будет отметить высокое качество контента, создаваемого экстремистскими организациями, с точки зрения его внешней привлекательности. Данные материалы, как правило, содержат красочные иллюстрации, музыкальное сопровождение и профессионально смонтированный видеоряд. В результате откровенно деструктивные и противоправные материалы «оборачиваются» в красивую оболочку, привлекающую внимание пользователей. В свою очередь, тот факт, что экстремистские сообщества и организации способны создавать внешне привлекательные материалы, высокого качества, может свидетельствовать о высоком уровне подготовленности в данной области самих участников и (или) их умении привлекать к данной работе высококлассных специалистов соответствующего профиля.

Оценивая влияние действий киберэкстремистов, действующих в интересах организованного экстремистского объединения, на формирование радикальных воззрений в обществе, полагаем, что оно является наиболее опасным по сравнению с киберэкстремистами из ранее рассмотренных нами групп.

Безусловно, любая организованная преступная деятельность обладает большей общественной опасностью в сравнении с аналогичной неорганизованной, и киберэкстремистская преступность не является здесь исключением. Повышенное влияние на формирование экстремистских воззрений, помимо прочего, достигается за счет способностей данных лиц организовывать свою противоправную деятельность в киберпространстве на систематичной основе, а также за счет умения привлекать финансирование и специалистов по созданию и распро-

¹ Здесь и далее по тексту при упоминании данной организации: «Деятельность организации запрещена решением Верховного Суда Российской Федерации от 2 августа 2022 г. № АКПИ22-411С по основаниям осуществления террористической и экстремистской деятельности».

странению в киберпространстве привлекающих внимание широкого круга пользователей материалов. Данный факт, с учетом обозначенной нами существенной организаторской роли иностранных государств, позволяет сделать вывод о том, что деятельность рассматриваемых лиц сегодня обладает беспрецедентной степенью организованности. В результате негативное информационно-психологическое воздействие на население оказывается постоянно, на профессиональной основе и с использованием практически всех существующих ИТТ.

Оценивая последствия такого воздействия, можно сделать вывод о том, что его объектом может стать практически любой гражданин, использующий ИТТ. Безусловно, приобретение экстремистских взглядов и убеждений отдельным человеком станет крайне негативным последствием для общества и может явиться причиной совершения преступлений экстремистской направленности в будущем. Вместе с тем чаще всего отдельный человек не имеет возможности транслировать приобретенные убеждения на большую аудиторию. В результате такой человек либо может стать членом экстремистской организации или сообщества, либо будет самостоятельно распространять свои новые взгляды. Во всех случаях степень влияния уже его действий на формирование экстремистских воззрений и населения будет по меньшей мере сопоставима по степени опасности с действиями неорганизованных киберэкстремистов.

Значительно опаснее представляется ситуация, при которой идеи экстремистского сообщества или организации в киберпространстве начинает распространять какая-либо популярная среди населения персона. При этом не имеет принципиального значения, действительно ли данная личность является носителем тех экстремистских воззрений, которые она транслирует на свою аудиторию, или же здесь имеет место исключительно корыстный интерес. Гораздо важнее здесь тот факт, что, обладая популярностью и авторитетом среди широкого круга населения, такие лица выступают фактически в роли лидеров мнений. Они не просто транслируют экстремистские идеи на большую аудиторию, но и вызывают у нее гораздо больше доверия. В результате становится сложно переоценить

негативный эффект, оказываемый на формирование экстремистских воззрений у населения.

Таким образом, в рамках настоящего параграфа нами определена характеристика личностей киберэкстремистов, а также оценено их влияние на формирование экстремистских взглядов и убеждений у населения.

Киберэкстремистами, деяния которых не связаны с деятельностью экстремистских сообществ и организаций, являются, как правило, трудоспособные мужчины в возрасте от 30 до 49 лет со средним профессиональным образованием, не имеющие постоянного места работы либо трудящиеся в промышленном секторе. Рассматриваемые лица чаще всего действуют исключительно от своего имени, из своих личных побуждений, не упоминая какое-либо экстремистское сообщество или организацию. Как правило, на момент привлечения к уголовной ответственности данные лица не имеют судимости, однако ранее уже неоднократно совершали аналогичные преступления, оставаясь вне поля зрения правоохранительных органов.

Общей для данной группы киберэкстремистов особенностью нравственно-психологической характеристики является их нежелание самостоятельно предпринимать активные преступные действия за пределами киберпространства. Вместо этого они стремятся побудить других лиц (преимущественно молодых людей в возрасте до 25 лет) к совершению преступлений экстремистской направленности в реальном мире.

Учитывая многочисленность группы киберэкстремистов, деяния которых не связаны с деятельностью экстремистских сообществ и организаций, нами предложено их дополнительно разделить в зависимости от степени «открытости» действий и отношения к сохранению анонимности на 2 подгруппы: «неосмотрительные» и «осторожные».

Неосмотрительных киберэкстремистов отличает их безразличное либо наивное отношение к сохранению своей анонимности в киберпространстве. Данные лица, как правило, легко внушаемы, они обладают достаточно узким кругозором, а также склонны к импульсивным и необдуманным действиям.

Уровень влияния данных лиц на формирование экстремистских воззрений у населения оценивается нами как низкий, поскольку их противоправная деятельность, как правило, весьма непродолжительна, плохо спланирована и не систематична. В свою очередь, приемы негативного информационно-психологического воздействия, используемые неосмотрительными киберэкстремистами, представляются наименее эффективными.

К подкатегории «осторожные» нами отнесены киберэкстремисты, которые в первую очередь обладают некоторыми знаниями по сокрытию своей личности в информационно-телекоммуникационном пространстве. По отношению к данным лицам негативные психологические особенности коммуникации в киберпространстве, такие как психологическая раскрепощенность, безответственность, а также стремление к ненормативному поведению, нередко служат катализатором для проявления их экстремистских воззрений. «Осторожные» киберэкстремисты могут вести «двойную» жизнь, выступая в киберпространстве в роли активиста, однако никак не проявляя своих экстремистских взглядов и убеждений в реальном мире.

Влияние данных лиц на формирование экстремистских воззрений у населения представляется более существенным, в отличие от действий неосмотрительных киберэкстремистов. За счет возможности долгое время скрывать свою личность противоправная деятельность данных лиц может быть весьма продолжительной. Кроме того, у «осторожных» киберэкстремистов прослеживается стремление к последовательности и систематичности негативного информационно-психологического воздействия. Несмотря на то, что данные лица, как правило, неизвестны широкому кругу общественности, они всячески стремятся своими действиями охватить как можно больше пользователей.

Давая криминологическую характеристику личностей представителей организованного уголовного киберэкстремизма, необходимо учитывать тот факт, что сегодня такие лица нередко действуют в интересах отдельных зарубежных стран. Как правило, ими являются трудоспособные мужчины в возрасте 30–49 лет, которые часто имеют высшее образование и специальные знания по наиболее эффек-

тивному использованию возможностей современных ИТТ для сохранения своей анонимности и привлечения финансирования.

Также следует отметить факт наличия у организаторов специальных знаний по наиболее эффективному деструктивному информационно-психологическому воздействию на пользователей. Указанные навыки выражаются в их умении самостоятельно (либо при помощи привлеченных специалистов) создавать и распространять внешне привлекательные экстремистские материалы, захватывающие внимание большого количества пользователей.

Влияние представителей организованного криминального киберэкстремизма на формирование у населения экстремистских взглядов и убеждений является наиболее существенным и опасным. Практически любой гражданин регулярно может наблюдать экстремистские материалы, массово создаваемые и распространяемые в киберпространстве на профессиональной основе. Наиболее опасной представляется ситуация, при которой идеи экстремистского сообщества или организации в киберпространстве начинают транслировать популярные среди больших групп населения личности. Используя свой авторитет и доверие среди населения, они гораздо более эффективно формируют экстремистские воззрения у населения. В результате сложно переоценить тот негативный эффект на формирование экстремистских воззрений среди населения, который оказывают киберэкстремисты, действующие в интересах организованного экстремистского объединения.

Таким образом, определив основные элементы криминологической характеристики киберэкстремистской преступности, перейдем к рассмотрению комплекса детерминирующих ее факторов, а также мер по их предупреждению.

ГЛАВА 2. ПРЕДПОСЫЛКИ УГОЛОВНОГО КИБЕРЭКСТРЕМИЗМА И ЕГО ПРЕДУПРЕЖДЕНИЕ В РОССИЙСКОЙ ФЕДЕРАЦИИ

§ 1. Объективные и субъективные предпосылки совершения преступлений экстремистской направленности, посредством использования информационно-телекоммуникационных технологий¹

Переходя к рассмотрению причинного комплекса совершения преступлений экстремистской направленности с использованием ИТТ, полагаем, что распространение киберэкстремистской преступности в Российской Федерации обусловлено рядом объективных и субъективных предпосылок. Как справедливо отмечает профессор Н. Ф. Кузнецова, деление предпосылок на объективные и субъективные позволяет выявить возможность воздействия внешних факторов на человеческое поведение и влияние внутренних, личностных особенностей индивида на его поступки². В свою очередь, применительно к нашему исследованию объективные предпосылки нами были дополнительно подразделены на внешние (т.е. связанные с непосредственным участием представителей отдельных зарубежных стран) и внутренние (без непосредственного участия представителей отдельных зарубежных стран).

Начиная рассматривать внешние объективные предпосылки, отметим, что, как мы уже говорили, в киберпространстве деструктивное информационно-психологическое воздействие на граждан оказывается преимущественно путем распространения деструктивного контента в социальных сетях, мессенджерах, на отдельных веб-сайтах. Сегодня мировое медиапространство практически полностью контролируется крупнейшими транснациональными корпорациями, которые в свою очередь находятся под юрисдикцией зарубежных стран. Как отмечают в своем исследовании Н. А. Васильев и С. Н. Комиссаров, уже по состоянию на

¹ Основные выводы данного параграфа отражены в публикации автора: Ильиных Н. А. Предпосылки киберэкстремистских преступлений и отдельные меры их предупреждения // Вестник Дальневосточного юридического института МВД России имени И. Ф. Шилова. 2025. № 3. С. 58-66.

² Кузнецова Н. Ф. Проблемы криминологической детерминации. М.: Изд-во Моск. ун-та, 1984. С. 52.

2021 г. из 5 миллиардов пользователей социальных сетей по всему миру 3 миллиарда имели аккаунты в социальной сети Facebook, которая в свою очередь принадлежит организации Meta¹. Вышеуказанная организация также владеет социальной сетью Instagram и мессенджером WhatsApp.

Об опасности информационно-психологического воздействия с участием зарубежных стран и его способности выступать в качестве объективной предпосылки совершения преступлений экстремистской направленности в первую очередь свидетельствует тот факт, что деструктивный контент на подобных информационных порталах не только не блокируется, но и активно продвигается, а его распространение в сообществах и между пользователями никак не ограничивается. Ярким примером здесь может служить заявление пресс-секретаря компании Meta Platforms Inc Энди Стоуна от 11 марта 2022 г., в котором он публично заявил, что компания снимает в своих социальных сетях запрет на размещение в разных странах информации, которая содержит призывы к насилию против российских граждан, в том числе военнослужащих². Данный факт, в частности, и послужил поводом для признания компании Meta экстремистской и запрета ее деятельности на территории Российской Федерации.

Однако даже несмотря на то, что сегодня в России доступ к части данных информационных ресурсов заблокирован, при помощи ряда технологий, таких как VPN, Проxy, Тор и др., для отдельных пользователей не составляет особого труда обойти такие блокировки и получить доступ к любым ресурсам, после чего полученная ими там информация может моментально продолжить свое распространение уже на отечественных информационных площадках. В результате распространяемые на заблокированных в РФ иностранных информационных ресурсах экстремистские материалы часто становятся доступными и для отечественных пользователей. Полагаем, что данный факт в совокупности с высокой вовле-

¹ Васильев Н. А., Комиссаров С. Н. Социальные сети. формирование нового социального мира // Гуманитарий Юга России. 2021. № 4. С. 43-60.

² Суд признал Meta экстремистской организацией и запретил в России Facebook и Instagram // Российская газета. URL: <https://rg.ru/2022/03/21/reg-cfo/sud-zapretit-v-rossii-instagram-i-facebook-za-ekstremistskuiu-deiatelnost.html> (дата обращения: 25.12.2023).

ченностью населения в использование ИТТ выступает в качестве предпосылки формирования у части граждан экстремистских взглядов и убеждений.

Исследуя вопрос о внешних объективных предпосылках распространения криминального киберэкстремизма в России, нельзя не сказать об активной организационной и координационной роли ряда зарубежных государств в указанном процессе. Рассматриваемое внешнее воздействие в первую очередь выражается в предоставлении для организаторов экстремистских сообществ информационных площадок с множеством пользователей для распространения их идеологии. Сегодня на таких популярных информационных ресурсах, как Youtube или запрещенные на территории Российской Федерации социальные сети Facebook, Instagram и др., вполне успешно функционируют аккаунты запрещенных движений, среди которых «Правый сектор»¹, «Полк Азов» и др. Как отмечают в своем исследовании А. В. Ананьев и Е. В. Ананьева, деятельность подобных организаций представителями отдельных государств активно поддерживается и финансово².

Необходимо отметить, что сегодня представители отдельных государств могут эффективно использовать возможности ИТТ и для непосредственной организации стихийных массовых беспорядков путем разжигания экстремистских настроений в отдельных регионах или группах населения Российской Федерации. Ярким примером здесь является ряд произошедших в конце октября 2023 г. массовых беспорядков на Северном Кавказе. Наиболее масштабной стала протестная акция в аэропорту г. Махачкалы 29–30 октября 2023 г. Беспорядки носили явный антисемитский характер. Участники протестов установили контроль над аэропортом и угрожали физической расправой над прибывшими самолетом из Израиля еврейскими беженцами, при этом игнорируя требования сотрудников полиции о прекращении указанных действий и оказывая им физическое сопротивление. Учитывая распространение массовых беспорядков, представителями

¹ Здесь и далее по тексту при упоминании данной организации: «Деятельность организации запрещена решением Верховного Суда РФ от 17 декабря 2014 г. № АКПИ14–1292с по основаниям осуществления террористической и экстремистской деятельности».

² Ананьев А. В., Ананьева Е. В. Страна управляемого неонацизма // Перспективы. 2022. № 2. С. 46.

различных официальных ведомств отмечалась высокая степень организованности данной акции, а также главенствующая роль в указанных процессах представителей иностранных государств¹.

Наиболее важен для настоящего исследования тот факт, что все призывы к экстремистским действиям и координация действий участников осуществлялись при помощи ИТТ². В частности, с момента начала боевых действий между Израилем и Палестиной осенью 2023 г. в Telegram-канале «Утро Дагестан» систематически публиковалась информация негативного содержания в отношении евреев, а также публичные призывы к ограничению их прав по признаку национальной принадлежности. Тем самым организаторы рассматриваемого сообщества в мессенджере, воспользовавшись внешнеполитической ситуацией, разжигали антисемитские настроения среди преимущественно исламского населения Республики Дагестан. Непосредственно в день начала беспорядков в Telegram-канале была опубликована информация с точным временем прибытия самолета с еврейскими беженцами, а также данные о количестве пассажиров. Указанная информация сопровождалась призывами к исламскому населению Дагестана о недопущении (в том числе с применением насилия) прибытия еврейский беженцев на территорию республики. Непосредственно во время событий в аэропорту путем публикации соответствующих сообщений в вышеуказанном Telegram-канале активно осуществлялась координация действий участников беспорядков. Таким образом, целенаправленное, организованное использование возможностей ИТТ во многом способствовало эффективной организации массовых беспорядков.

Немаловажным здесь является тот факт, что благодаря скорости передачи сведений в киберпространстве информация из Telegram-канала «Утро Дагестан» была быстро распространена и на других информационных платформах, в том числе на личных страницах отдельных популярных пользователей. Например,

¹ Путин назвал беспорядки в Махачкале событием, а не тенденцией // РБК. URL: <https://www.rbc.ru/rbcfreenews/6544f1519a794794e21391bd> (дата обращения: 25.12.2023).

² Беспорядки в Махачкале организованы через социальные сети // Известия. URL: <https://iz.ru/1597736/alena-nefedova/ne-dobivaias-rezultatov-na-pole-boia-khotiat-raskolot-nas-iznutri> (дата обращения: 25.12.2023).

один из достаточно известных блогеров (по состоянию на конец октября 2023 г. имел около 33,5 тысяч подписчиков в своем Telegram-канале) в дни беспорядков опубликовал изображение со словами «Мы против еврейских беженцев», а также сообщения с призывами ограничивать права евреев. Во втором сообщении он осудил администраторов отеля «Фламинго» в Хасавюрте, в котором якобы располагались израильтяне. Блогер заявил, что их всех необходимо выселить, иначе «гостиница превратится в пепел»¹. Вскоре данная информация была удалена, а блогер выступил с осуждением действий участников беспорядков, однако к моменту удаления вышеуказанных сообщений их посмотрели свыше 55,5 тыс. человек. Указанное число является достаточно большим, оно сопоставимо с общим количеством подписчиков Telegram-канала «Утро Дагестан» (около 62 тыс. пользователей по состоянию на октябрь 2023 г.). Таким образом, можно утверждать, что экстремистский контент, целенаправленно публикуемый на одном или нескольких курируемых экстремистскими организациями информационных площадках, может быть очень быстро распространен обычными пользователями и блогерами среди неограниченного круга лиц.

Помимо прочего, считаем необходимым отдельно рассмотреть роль внешнего воздействия в распространении экстремистских недостоверных сведений среди населения. Как нами уже отмечалось ранее, сегодня негативное информационно-психологическое воздействие на граждан РФ активно оказывается в целях вызвать у населения чувства тревоги, страха, беспокойства и незащищенности со стороны государства.

Масштабность фальсификаций, а также скорость их распространения в киберпространстве свидетельствуют об организованном характере подготовки вбросов указанных материалов. Ярким примером здесь является фейк о совершении российскими военными массовых убийств мирных жителей в городе Буча Киевской области. Данная масштабная дезинформация за несколько часов была рас-

¹ Блогера Хасбика за антисемитизм и призывы к беспорядкам проверит Генпрокуратура // РБК. URL: <https://lenta.ru/news/2023/10/31/blogera-hasbika-za-antisemitizm-i-prizyvy-k-besporiyadkam-proverit-genprokuratura/> (дата обращения: 25.12.2023).

пространена под видом достоверного факта на информационных порталах самых крупных зарубежных СМИ, таких как BBC, CNN, FoxNews и др. Также быстро указанный фейк был распространен во всех крупных социальных сетях и мессенджерах, создав общественный резонанс.

В свою очередь, наличие в киберпространстве подобных масштабных и качественно сфабрикованных материалов, а также активное их продвижение на зарубежных информационных ресурсах приводит к тому, что данные сведения получают свое распространение и среди отечественных пользователей. В результате анализа судебных приговоров по ст. 207.3 УК РФ установлено, что в тексте 7 из 22 приговоров за 2023–2024 гг. фигурировал фейк о событиях в городе Буча. Осужденные за вышеуказанные деяния, ознакомившись на различных информационных площадках с указанными материалами и поверив в их достоверность, начали распространять экстремистские материалы на своих личных страницах в социальных сетях, группах, пересылать в чаты мессенджеров, а также комментировать аналогичные записи других пользователей.

Например, согласно материалам одного из приговоров по делу о распространении вышеуказанных недостоверных сведений, «гражданка С., желая создать у пользователей сети Интернет убеждение о соответствии действительности своей ложной информации, с целью придания ей достоверности, разместила три видеозаписи с изображением городской местности и людей в военном обмундировании с предметами в руках, схожими с огнестрельным оружием, которые ведут людей со связанными за спинами руками, а в последующем расстреливают их. Данную публикацию просмотрели 52 пользователя социальной сети «ВКонтакте», у которых в результате преступных действий гражданки С. могло создаться убеждение в том, что опубликованное ею заведомо ложное сообщение является достоверным и соответствующим действительности». Как следует из материалов судебного решения, к вышеуказанному числу следует прибавить еще 82 человека, которые просмотрели аналогичную публикацию гражданки С., опубликованную

ранее¹. Итого действия лишь одного человека могли привести к формированию экстремистских взглядов и убеждений у 134 пользователей.

Таким образом, нами рассмотрена внешняя объективная предпосылка совершения киберэкстремистских преступлений, отличительной особенностью которой является непосредственное участие в них представителей отдельных зарубежных стран или аффилированных ими коммерческих организаций.

Переходя к рассмотрению внутренних объективных предпосылок, отметим, что для целей настоящего исследования под ними понимается комплекс факторов, которые существуют без явного и целенаправленного участия представителей отдельных зарубежных стран.

В рамках первого параграфа нами было определено такое негативное явление, как имплицитное деструктивное информационно-психологическое воздействие на человека в киберпространстве. Как нами уже отмечалось, под ИДИПВ следует понимать такие формы негативного информационно-психологического воздействия, которые напрямую не запрещены действующим законодательством. Отличительной чертой данного воздействия является его неявный характер. Полагаем, что именно оно сегодня выступает в качестве внутренней объективной предпосылки совершения киберэкстремистских преступлений и проявляется в различных формах, особенности которых нами будут рассмотрены далее.

Одной из форм ИДИПВ является скрытая пропаганда деструктивных ценностей, проявляющаяся через безобидные на первый взгляд фильмы, видеоигры, музыкальные клипы, книги и т.д., где все или часть событий и персонажей являются художественным вымыслом. В подобном контенте может закладываться скрытая пропаганда насилия в отношении определенных групп людей или иные деструктивные идеи, которые в свою очередь могут выступить в качестве возможной предпосылки приобретения пользователем экстремистских взглядов и убеждений.

¹ Приговор Свердловского районного суда г. Иркутска Иркутской области от 22 мая 2023 г. по делу № 1-597/2023. Доступ из справ.-правовой системы «ГАРАНТ».

В особенности опасен данный вид информационно-психологического воздействия в отношении детей и подростков. В силу возраста у них еще не сформирована устойчивая психика и может отсутствовать достаточный уровень критического отношения к просматриваемому контенту. Как справедливо отмечает в своем исследовании А. Ю. Шаханская, для детей в определенной мере важны идеально-позитивные как художественные, так и реальные модели поведения. На экране отрицательные примеры героев могут оставаться без оценочных комментариев, что со стороны выглядит как одобрение. Персонажа, нарушающего общепринятые правила, никто не наказывает. В итоге у ребенка закрепляется представление о допустимости подобных форм поведения, расшатываются эталоны хорошего и плохого поступка, допустимого и неприемлемого поведения.

Ярким примером опасности данной формы ИДИПВ и его способности выступать в качестве предпосылки могут свидетельствовать события, связанные с набравшим в 2023 г. популярность деструктивным движением под названием «ЧВК Рёдан»¹. На сегодняшний день указанное движение официально не признано экстремистским, однако оно носит ярко выраженный деструктивный характер. Данный факт, в частности, отмечается в исследовании профессора С. Ю. Чимарова². Мы разделяем позицию исследователя о том, что необходимо уделять больше внимания проявлениям как конкретно данного движения в частности, так и подобных ему деструктивных течений в целом.

В группе социальной сети «ВКонтакте» под названием «ЧВК Рёдан», организаторы которой позиционируют его как официальное сообщество указанного движения, прямо сказано о том, что их основной аудиторией являются любители аниме (от японского «анимэ сён» – японский анимационный стиль, который отличается от других анимационных стилей своей уникальной стилизацией персонажей, мира и сюжета), которыми по большей части являются подростки.

¹ Молодежная субкультура ЧВК «Редан» захлестнула Россию: что это такое и зачем подростки снимают на видео драки в ТЦ // Комсомольская правда. URL: <https://www.kp.ru/daily/27470/4726359/> (дата обращения: 18.12.2023).

² Чимаров С. Ю. Проблемный аспект ЧВК «Рёдан» и предметное поле правоохранительной деятельности ОВД России в формате молодежного дискурса // Международный журнал гуманитарных и естественных наук. 2023. № 3-3. С. 97-98.

Результаты проведенного нами контент-анализа публикаций указанного сообщества свидетельствуют о проявлении пользователями высокого интереса к тематике сообщества, в частности к специфической символике данного движения¹. На странице группы регулярно публикуются фотографии молодых людей с татуировками или одеждой, на которых изображен белый паук с цифрой «4». Цифра «4» в данном случае обозначает номер члена группировки по имени Хисока Мороу из японского комикса-аниме «Охотник × Охотник», которому и поклоняются члены группировки ЧВК «Рёдан». По характеру данный персонаж является негативным, скрытным, а его намерения являются неясными. Согласно сюжету данного аниме все члены группировки с номерами «4» являются антагонистами, что связано с традиционным японским убеждением о негативном значении самой цифры «4», произношение которой на японском языке созвучно со словом «смерть».

В результате анализа содержания комментариев к публикациям рассматриваемого нами сообщества в социальной сети установлено, что среди них содержится много оскорблений, нецензурной лексики, а также крайне негативных высказываний, нередко сопровождающихся угрозами применения насилия, в адрес тех подростков, которые высказывают свое скептическое мнение относительно символики или других ценностей сообщества «ЧВК Рёдан». При этом организаторы сообщества часто либо напрямую поддерживают подобные оскорбления, либо не препятствуют их размещению в комментариях к своим публикациям, поощряя тем самым негативное поведение подростков.

Таким образом, можно утверждать, что скрытая пропаганда в киберпространстве деструктивных ценностей, проявляющаяся через безобидные на первый взгляд фильмы, видеоигры, книги и т.д., нередко служит предпосылкой формирования экстремистских взглядов и убеждений. Более того, как видно из

¹ Ильиных Н. А. Имплицитное информационно-деструктивное воздействие как условие формирования экстремистских взглядов и убеждений // Актуальные проблемы борьбы с преступностью: вопросы теории и практики: мат-лы XXVII междунар. науч.-практ. конф. В 2 ч. Красноярск: Сибирский юридический институт МВД России, 2024. Ч. 2. С. 19-22.

рассмотренного нами примера, данное явление может провоцировать молодежные субкультурные конфликты¹.

Перейдем к рассмотрению второй формы имплицитного деструктивного информационно-психологического воздействия на человека. Полагаем, что сегодня существенное негативное воздействие на общественное сознание оказывают повсеместно распространяемые в социальных сетях и мессенджерах новостные публикации относительно совершения преступлений и (или) административных правонарушений с прямым указанием на принадлежность виновника к той или иной социальной группе, объединенной по политическим, религиозным, национальным или идеологическим признакам. В подобных публикациях в зависимости от убеждений, поддерживаемых большинством пользователей сообществ или исходя из их национальности, акцентируется внимание на том, что преступление или административное правонарушение совершил представитель другой национальности или социальной группы, разделяющий иные взгляды. При этом зачастую новости о том, что аналогичные деяния совершил представитель титульной нации или человек, являющийся носителем общепринятых среди большинства пользователей взглядов, не публикуются либо размещаются без указания на принадлежность виновника к той, или иной социальной группе, объединенной по политическим, религиозным, национальным или идеологическим признакам. Например, в одном из своих заявлений глава Чеченской Республики Р. А. Кадыров обратил внимание на данную проблему и прокомментировал ее следующими словами: «СМИ ведут себя так, будто есть только две категории граждан: кавказец и человек без национальности»².

Еще большую актуальность проблема приобретает в контексте проводимой государством миграционной политики, направленной, с одной стороны, на

¹ Ростокинский А. В. Преступления экстремистской направленности как проявления субкультурных конфликтов молодежных объединений: уголовно-правовые и криминологические проблемы: дис. ... д-ра юрид. наук. М., 2011. С. 15.

² Кадыров раскритиковал СМИ и Симоньян за освещение драки в Новой Москве // РБК. URL: <https://www.rbc.ru/politics/06/11/2021/6186ac0b9a7947b2c2e4ea59> (дата обращения: 31.01.2024).

«восполнение численности населения, в том числе повышение уровня занятых и экономически активного населения», с другой – на обеспечение соответствующего государственного контроля и «защиту прав и свобод гражданина, материальных и духовных ценностей государства»¹. Полагаем, что в результате систематического распространения подобных публикаций в обществе может сформироваться ошибочное представление об определенной социальной группе как наиболее криминогенной. Складывающаяся ситуация не только не способствует гармонизации общественных отношений, необходимой для успешной реализации миграционной политики государства, но и активно содействует распространению экстремистских взглядов и убеждений среди отдельных групп населения.

В целях выявления уровня восприимчивости населения к данной форме имплицитного информационно-деструктивного воздействия нами было проанализировано 40 подобных публикаций в 10 крупных новостных сообществах соцсети «ВКонтакте» и мессенджере «Telegram»². В рамках исследования были рассмотрены публикации в следующих новостных сообществах с количеством участников по состоянию на 1 февраля 2024 г. свыше 50 тысяч: «Топор – Хранилище» («ВКонтакте» – 4 млн 500 тыс. подписчиков); «Прямой репортаж» («Telegram» – 4 млн 76 тыс. подписчиков); «Плохие новости» («ВКонтакте» – 1 млн 600 тыс. подписчиков); «Москвач. Новости Москвы» (1 млн 300 тыс. подписчиков); «ВПШ» («Telegram» – 1 млн 100 тыс. подписчиков); «Лентач» («Telegram» – 327 тыс. подписчиков); «Инцидент Омск» («ВКонтакте» – 324 тыс. подписчиков); «Smesto события – Новости» («ВКонтакте» – 205 тыс. подписчиков); «КБ 18+» («ВКонтакте» – 134 тыс. подписчиков); «Московский комсомолец: главное сегодня» («Telegram» – 60 тыс. подписчиков); «Чёткая Грань I SxE» («ВКонтакте» – 59 тыс. подписчиков).

¹ Юзиханова Э. Г. Организация профилактики правонарушений в сфере миграции // Вестник Тюменского института повышения квалификации сотрудников МВД России. 2021. № 2. С. 39-40.

² См. Приложение 3.

В результате анализа 1000 выбранных в случайном порядке комментариев к опубликованным в данных сообществах публикациям установлено, что свыше трети из них (34,9%) содержали крайне негативные высказывания исключительно в адрес той или иной социальной группы, к которой принадлежит виновник. Считаем, что данный показатель является достаточно большим, особенно учитывая, что 22,9% комментариев вовсе не имели отношения к опубликованной новости¹. Таким образом, полагаем, что результаты проведенного нами контент-анализа свидетельствуют о том, что подобные публикации активно способствуют формированию среди населения экстремистских взглядов и убеждений и могут выступать в качестве объективной предпосылки.

Таким образом, нами определена внешняя объективная предпосылка уголовного киберэкстремизма, которая выражается в непосредственном участии в совершении и организации киберэкстремистских преступлений представителей отдельных зарубежных стран, а также внутренняя предпосылка, которые выражается в двух формах имплицитного деструктивного информационно-психологического воздействия.

Переходя к рассмотрению субъективных предпосылок криминального киберэкстремизма, также начнем с внешних. Здесь рассмотрим факторы, которые способствовали формированию экстремистских взглядов и убеждений среди той категории населения, представители которой сегодня наиболее часто совершают киберэкстремистские преступления. Как нами уже отмечалось ранее, средний возраст большинства киберэкстремистов сегодня около 30 лет. Учитывая, что наиболее активно процессы социализации человека и формирования его основных убеждений протекают в период обучения в старшей школе, в вузе (или ССУЗе), наибольший интерес в рамках настоящего исследования представляет комплекс негативных факторов, воздействовавших на рассматриваемую категорию граждан в период, когда они были в возрасте от 14 до 24 лет. Данный период практически совпадает с периодом формирования государственности в Российской Федерации после распада СССР, сопровождавшегося глобальными изменениями ценностных

¹ См. Приложение 3.

ориентиров общества. Кроме того, именно в указанный момент в нашей стране получили наиболее активное распространение информационно-телекоммуникационные технологии. Считаем, что указанные факты взаимосвязаны, и их следует рассматривать комплексно в качестве предпосылок для совершения киберэкстремистских преступлений гражданами, которые выросли в указанное время.

Отнесение данных предпосылок к категории внешних объективных обусловлено активным участием отдельных зарубежных стран в политических процессах, происходивших в период после распада СССР, деятельность которых во многом способствовала изменению ценностных ориентиров российского общества в 1990-е годы.

Понятие ценностных ориентаций часто определяют как совокупность установок личности на определенные ценности материальной и духовной культуры общества¹. В свою очередь, различными исследователями отмечается, что после распада СССР произошли коренные изменения в духовной и экономической сферах жизни российского общества. Например, как справедливо утверждает в своей работе А. М. Цыбулька, в указанный период была стерта историческая общность людей как единого советского народа и, как следствие, претерпела изменение общая ценностная основа бытия². На смену советской идеологии практически моментно пришла идеология либерализма, распространяемая при активном участии представителей западных государств. В частности, директор лондонского Института экономических проблем Ральф Харрисон открыто называл «нашими людьми» правительство при Президенте России Б. Н. Ельцине (1991–1999 гг.)³.

Однако для быстрой смены системы ценностей необходимо было производить систематическое информационно-идеологическое воздействие на население страны с целью убеждения населения в привлекательности идей западного либе-

¹ Елишев С. О. Изучение понятий «Ценность», «Ценностные ориентации» в междисциплинарном аспекте // Ценности и смыслы. 2011. № 2. С. 91.

² Цыбулька А. М. Изменение ценностных основ в условиях глобальных вызовов человечеству // Ученые записки Санкт-Петербургского имени В. Б. Бобкова филиала Российской таможенной академии. 2022. № 2. С. 68-71.

³ Дуглас Р. Яд для России // Завтра. 2010. № 19. С. 2.

рализма, европейского и американского образа жизни и пропаганды дружелюбности указанных стран. Полагаем, что указанное систематическое информационно-психологическое воздействие наиболее активно оказывалось через кинофильмы, музыку, книги и т.д. Как справедливо в своем исследовании отмечают Е. П. Казбан и С. С. Степанова, в числе факторов, определяющих смыслы и ценности как продукты духовно-практического освоения действительности, одну из ключевых ролей играет искусство¹.

Для того чтобы достичь наибольшего охвата аудитории, в рассматриваемый период в России начали вести активную работу крупнейшие западные медиахолдинги с целью повсеместной трансляции в информационном поле контента зарубежного производства (фильмы, сериалы, музыка, книги и т.д.). Согласно данным исследования Ю. В. Маркиной, по состоянию на 2018 г., помимо прочих, одна только немецкая медиакорпорация Bertelsmann (входит в число 6 крупнейших мировых медиахолдингов, наряду с Time Warner, Vivendi, News Corporation Walt Disney Co, и Viacom.), помимо телеканалов в Германии, Франции, Бельгии, Испании и др., владела 25% российского «Первого канала» и 7,5% долей в отечественной «Национальной Медиа Группе», в состав которой входят телеканал «Рен-ТВ», газета «Известия» и телекомпания «Петербург»².

В результате на несколько десятилетий западная массовая культура стала в российском обществе преобладающей. Например, среди всех фильмов, выходивших в прокат в отечественных кинотеатрах с 1990 по 1999 гг., в десятку лучших, по мнению зрителей, вошел только один российский³. В связи с этим закономерен факт, что та категория населения, чей период взросления и социализации пришелся на рассматриваемый временной промежуток, активно перенимала ценности западного либерализма.

¹ Казбан Е. П., Степанова С. С. Либерализм в ценностной системе российского общества // PolitBook. 2019. № 1. С. 182.

² Маркина Ю. В. Мировые транснациональные медиакорпорации как сегмент глобализации информационной деятельности // Вопросы журналистики, педагогики, языкознания. 2018. № 3. С. 486.

³ Лучшие фильмы 1990-х годов // Кинопоиск. URL: <https://www.kinopoisk.ru/lists/movies/year--1990-1999> (дата обращения: 05.04.2025).

Однако если в большинстве западных стран идеи либерализма развивались последовательно на протяжении нескольких столетий, без внешнего вмешательства, и были тесно связаны с сильным правовым государством, то в Российской Федерации ситуация сложилась кардинально иначе. Переоценка ценностей советского общества происходила резко и при активном участии бывших противников СССР, которые были заинтересованы в извлечении собственной выгоды, а не в создании свободного российского общества. В результате одна из ключевых ценностей либерализма – свобода личности (в первую очередь свобода от контроля со стороны государства) – на фоне общей слабости институционализации российской государственной власти и неоднозначной социальной политики стала ошибочно восприниматься в нашем обществе как вседозволенность и безнаказанность. Вплоть до настоящего времени исследователями отмечается кризис ценностной системы российского общества, обусловленный восприятием либерализма как вольницы без ответственности¹.

В свою очередь, ценности можно трактовать как обобщенные представления людей относительно наиболее значимых целей и норм поведения, которые определяют приоритеты в восприятии действительности, задают ориентацию их действиям и поступкам во всех сферах жизни². В контексте формирования предпосылок уголовного киберэкстремизма убежденность населения во вседозволенности своих высказываний ярко проявилась и в информационно-телекоммуникационном пространстве. Рассматривая психологические особенности коммуникации между людьми в киберпространстве, К. С. Есаулова отмечает, что интернет очень часто в общественном сознании воспринимается как «пространство свободы»³.

¹ Казбан Е. П., Степанова С. С. Либерализм в ценностной системе российского общества // PolitBook. 2019. № 1. С. 189.

² Засыпкина Л. Р. Политические процессы в России конца XX века как объект социокультурного анализа // Историческая и социально-образовательная мысль. 2017. Т. 9, № 3-1. С. 50-55.

³ Есаулова К. С. К определению социальной смелости: в реальной жизни и интернет-коммуникации // Вестник РГГУ. Серия «Психология. Педагогика. Образование». 2016. № 2. С. 55.

С момента активного распространения интернета в России на продолжительное время глобальная сеть стала популярным местом для распространения самых разных деструктивных идей, нередко напрямую сопряженных с экстремизмом, как в случае с рассмотренной нами ранее онлайн-игрой «Большая игра: Сломай Систему», принадлежавшей экстремистской организации «Северное братство». В свою очередь, слабый контроль за информационно-телекоммуникационным пространством со стороны государственных органов в совокупности с убежденностью пользователей во вседозволенности своих действий прочно укоренили в обществе мнение о том, что в киберпространстве можно безнаказанно распространять контент любого содержания, в том числе и экстремистского, что, на наш взгляд, безусловно может выступать в качестве предпосылки совершения киберэкстремистских преступлений.

Далее рассмотрим внутренние, то есть не обусловленные прямым участием представителей зарубежных стран субъективные предпосылки совершения киберэкстремистских преступлений. К таковым, на наш взгляд, в первую очередь следует отнести высокий уровень восприимчивости населения к публикуемому в киберпространстве деструктивному контенту. Восприимчивость пользователей к подобной информации может выступать в качестве предпосылки приобретения ими в том числе и экстремистских убеждений.

Полагаем, что сегодня граждане в целом очень часто доверяют сомнительному контенту, размещаемому в киберпространстве. Данный факт подтверждается активной вовлеченностью населения в приобретение некачественных товаров и услуг, продаваемых и активно рекламируемых онлайн. Достаточно часто граждане становятся жертвами различных онлайн-финансовых пирамид и иных финансовых мошенничеств. Ситуация здесь во многом усугубляется отмечаемой Е. В. Никульченковой проблемой, связанной с общей недостаточной, а порой и низкой компьютерной грамотностью пользователей¹.

¹ Никульченкова Е. В. Причинностные факторы киберпреступности // Правоприменение в публичном и частном праве: мат-лы междунар. науч. конф. Омск: Омский государственный университет им. Ф.М. Достоевского, 2024. С. 121.

Считаем, что одной из ключевых проблем здесь является то, что в информационно-телекоммуникационном пространстве можно создать идеальный (и в то же время сложно проверяемый на соответствие действительности) образ для своего товара или услуги благодаря красочному описанию, сопровождаемому привлекательными изображениями и видео. Для злоумышленников не составляет особого труда создать при помощи ИТТ фальшивые положительные отзывы «довольных покупателей», тем самым еще больше подкрепив доверие пользователей. Более того, современные возможности ИТТ предоставляют практически неограниченные возможности для рекламы на различных площадках. В результате пользователи очень часто воспринимают данную информацию как достоверную.

Ярким примером подобного массового доверия граждан может послужить ситуация, связанная с деятельностью финансовой пирамиды «Finiko». Создатели мошеннической схемы активно использовали возможности ИТТ для привлечения вкладчиков. Недостоверная информация о высокой прибыли для клиентов массово распространялась во множестве сообществ социальных сетей и в группах мессенджеров. На своем официальном канале видеохостинга «Youtube» злоумышленники регулярно публиковали «познавательные» видео, в которых пользователей убеждали в честности руководителей финансовой пирамиды и безопасности вкладов¹. Все подобные видеоролики и рекламные размещения сопровождались большим количеством комментариев «довольных клиентов», создавая эффект иллюзорной массовости, еще больше подкрепляя тем самым доверие потенциальных вкладчиков. В то же время на тех немногочисленных пользователей, кто высказывал сомнения в честности схемы, моментально обрушивался поток оскорблений и обвинений в некомпетентности. В конечном счете в результате деятельности данной компании было обмануто свыше 165 тыс. вкладчиков на сумму до 7 млрд рублей².

¹ Подробнее про программу AT35 – автомобиль за 35% от стоимости // Finiko. URL: <https://www.youtube.com/watch?v=ZtonloYiVEw> (дата обращения: 15.02.2025).

² Евтушенко И. И. Мошенничества с цифровыми правами: вопросы квалификации // Ученые записки Крымского федерального университета имени В. И. Вернадского. Юридические науки. 2022. № 1. С. 134.

В целях определения уровня доверия населения экстремистскому контенту, публикуемому в киберпространстве, рассмотрим, как сегодня пользователями воспринимаются сфальсифицированные новости, которые зачастую публикуются в целях формирования экстремистских взглядов и убеждений. Согласно проведенному нами опросу сотрудников ЦПЭ на вопрос: «Как Вы оцениваете уровень критического отношения населения к недостоверным сведениям, публикуемым из неофициальных источников?» – 62,5% опрошенных ответили, что большинство населения легко внушаемо, граждане информацию не перепроверяют. С мнением о том, что пользователи редко перепроверяют информацию, согласились 25% респондентов. Лишь 12,5% опрошенных ответили, что население скорее не внушаемо, и пользователи часто перепроверяют информацию через различные источники¹.

Нами также был проведен контент-анализ комментариев и реакций пользователей социальных сетей и мессенджеров к фейковым новостям². В результате анализа выбранных нами в случайном порядке 1000 комментариев к 15 фейковым новостным публикациям установлено, что смысловое содержание 53,5% комментариев свидетельствует о восприятии пользователями информации как достоверной. Около 20% комментариев не имели отношения к опубликованной новости. Лишь 26,2% комментариев свидетельствовали о том, что пользователи не доверяют опубликованной новости³.

Значительно выше оказались аналогичные показатели по результатам анализа реакций (в большинстве мессенджеров и социальных сетей можно оценить публикацию различными условными обозначениями, отражающими отношение пользователя к публикации) пользователей на вышеуказанные публикации. Всего было проанализировано 54 тыс. реакций, 78,3% из которых подтверждают восприятие информации как достоверной, 21,7% свидетельствуют о недоверии к новости либо не имеют отношения к ней⁴.

¹ См. Приложение 1.

² Под реакциями понимаются условные обозначения, располагающиеся непосредственно под публикацией, при помощи которых пользователи могут оценить контент.

³ См. Приложение 3.

⁴ См. Приложение 3.

Таким образом, опираясь на мнение большинства опрошенных нами практических сотрудников, занимающихся противодействием экстремизму, а также на результаты проведенного контент-анализа, полагаем, что значительная часть отечественных пользователей крайне восприимчива к различным формам деструктивного контента, в том числе и непосредственно экстремистского, распространяемого в информационно-телекоммуникационном пространстве. Данный факт, в свою очередь, может выступать в качестве предпосылки формирования экстремистских убеждений и совершения отдельными лицами киберэкстремистских преступлений.

Продолжая рассматривать субъективные предпосылки, считаем необходимым изучить вопрос об осведомленности граждан о том, какие преступления экстремистской направленности существуют и в каких формах сегодня проявляется экстремизм.

В результате проведенного нами опроса 853 жителей Омской области в возрасте от 18 лет установлено, что подавляющее большинство респондентов не осведомлены о том, что из себя представляет экстремистская деятельность. В частности, на вопрос: «Какие действия признаются экстремизмом?» — из 4 предложенных вариантов ответов верный выбрали только 28,2% респондентов, при этом 32,1% затруднились ответить¹. Около 86,6% опрошенных практических сотрудников также отмечают низкую осведомленность граждан относительно того, какие деяния по действующему законодательству признаются преступлениями экстремистской направленности².

В своем диссертационном исследовании П. А. Глущенко, говоря об осведомленности граждан относительно угроз и последствий финансирования экстремистской и террористической деятельности, также приходит к выводу о достаточно низком уровне правовой грамотности населения в этих вопросах³. Без-

¹ См. Приложение 4.

² См. Приложение 2.

³ Глущенко П. А. Криминологические основы противодействия финансированию экстремистской и террористической деятельности: дис. ... канд. юрид. наук. Краснодар, 2025. С. 56.

условно, здесь следует в очередной раз отметить сложную структуру современного российского законодательства об экстремизме. В. В. Лунеев совершенно справедливо высказывается по этому поводу: «Даже специалисту очень трудно разобраться в законотворчестве об экстремизме, а ведь законы предназначены для обычных граждан и не очень грамотных сотрудников системы уголовной юстиции»¹.

Вместе с тем непростые формулировки законов хотя и могут требовать дополнительного внимания со стороны законодателя, однако сами по себе не являются основанием для освобождения от ответственности и необходимости для граждан знать эти нормы. В свою очередь, как справедливо отмечает в своем исследовании А. И. Петров, низкий уровень правовой грамотности может являться причиной совершения преступлений². Таким образом, полагаем, что существующий сегодня достаточно низкий уровень осведомленности населения относительно сущности экстремизма, а также форм его проявления может выступать в качестве субъективной предпосылки киберэкстремистской преступности.

Таким образом, в рамках исследования нами определен ряд объективных и субъективных предпосылок совершения киберэкстремистских преступлений. Полагаем, что их целесообразно разделять на внешние (те, которые непосредственно связаны с участием представителей зарубежных стран) и внутренние (обусловленные процессами, протекающими без непосредственного участия в них представителей зарубежных государств).

К внешним объективным предпосылкам нами отнесено непосредственное участие представителей зарубежных государств в совершении киберэкстремистских преступлений, которое выражается: в организации массовых экстремистских акций посредством использования ИТТ; в фабрикации и вбросе в киберпространство недостоверных сведений экстремистского содержания; в поддержке крупных

¹ Лунеев В. В. Российский экстремизм: политика и реалии // Всероссийский криминологический журнал. 2009. № 3. С. 24.

² Петров А. И. Деятельность прокуратуры по правовому просвещению как средство профилактики правонарушений и преступлений // Oeconomia et Jus. 2018. № 3. С. 48-62.

информационных площадок, на которых активно распространяются экстремистские материалы.

В качестве внутренней объективной предпосылки выступает имплицитное информационно-деструктивное воздействие на личность, которые выражается в следующих формах:

- а) пропаганда деструктивных ценностей в фильмах, видеоиграх, книгах и т.д.;
- б) формирование негативного отношения к какой-либо социальной группе, объединенной по политическим, религиозным, национальным или идеологическим признакам, путем распространения в киберпространстве сведений относительно совершения правонарушений с прямым указанием на представителя группы как виновного.

Внешней субъективной предпосылкой выступает восприятие значительной частью населения России идеологии либерализма как вседозволенности на фоне проводимых после распада СССР при активном участии недружественных стран реформ, совпавшее с началом широкого распространения в стране в 90-х гг. XX в. информационно-телекоммуникационных технологий, что в совокупности с недостаточным контролем со стороны правоохранительных органов за киберпространством способствовало формированию в российском обществе чувства безнаказанности за распространение экстремистских материалов при помощи ИТТ.

Внутренними субъективными предпосылками совершения киберэкстремистских преступлений являются:

- а) высокая восприимчивость населения к экстремистским материалам, распространяемым в информационно-телекоммуникационном пространстве;
- б) низкий уровень осведомленности граждан о формах проявления экстремизма и ответственности за совершение деяний экстремистской направленности.

§ 2. Обеспечение информационно-психологической безопасности граждан как мера нивелирования деструктивного информационно-психологического воздействия и предупреждения киберэкстремистских преступлений

В рамках настоящего исследования считаем необходимым отдельно рассмотреть вопрос о том, каким образом нивелировать негативный эффект от деструктивного информационно-психологического воздействия на российское общество, оказываемого в результате совершения киберэкстремистских преступлений. Ключевыми здесь должны выступать меры, направленные на обеспечение отдельных элементов информационно-психологической безопасности личности, которые в свою очередь способны выступить в качестве мер по устранению предпосылок совершения киберэкстремистских преступлений. Меры противодействия криминальному киберэкстремизму, которые будут предложены в рамках данного параграфа, направлены преимущественно на устранение внутренних объективных и субъективных предпосылок, определенных нами в рамках предыдущего раздела исследования.

В первую очередь определимся с тем, что сегодня понимается под информационно-психологической безопасностью личности. Исходя из текста подп. 4 п. 25 Указа Президента РФ от 2 июля 2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации» можно однозначно утверждать лишь о том, что обеспечение информационно-психологической безопасности личности является одной из приоритетных задач обеспечения национальной безопасности. Тем не менее имеющаяся в данном нормативно-правовом акте формулировка не раскрывает содержательную составляющую рассматриваемого нами понятия, поэтому обратимся к мнениям исследователей.

В рамках своей работы Г. В. Грачев под информационно-психологической безопасностью личности предлагает понимать «состояние защищенности ее основных интересов, которые состоят в реализации конституционных прав и свобод, в обеспечении личной безопасности, в повышении качества и уровня жизни, в физическом, духовном и интеллектуальном развитии, от угроз, вызываемых ин-

формационным воздействием на психику человека разнообразными социальными субъектами и информационной средой общества»¹.

В своем исследовании К. Д. Рыдченко определяет информационно-психологическую безопасность личности как «основанное на балансе интересов личности, общества и государства состояние защищенности индивидуальной психики и общественного сознания от осуществляемого при обороте вредоносной информации негативного психологического воздействия»².

В результате нами сделан вывод о том, что обеспечение информационно-психологической безопасности должно представлять собой комплекс мер, направленных на сохранение состояния защищенности психики личности и общественного сознания от достаточно широкого спектра деструктивного информационного воздействия. Тем не менее наиболее важным элементом сохранения информационно-психологической безопасности является комплекс мер, направленных на ее обеспечение, в части, касающейся устранения именно тех факторов, которые могут способствовать совершению преступлений экстремистской направленности.

В п. 12 и подп. «д» п. 21 Указа Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» указывается, что информационно-психологическое воздействие в первую очередь подразумевает под собой действия, направленные на изменение ценностных ориентиров российского общества с целью дестабилизировать внутривнутриполитическую и социальную ситуации в стране³. Таким образом, законодатель акцентирует особое внимание на необходимость обеспечения информационно-психологической безопасности личности в части, касающейся недопущения распространения информации именно экстремистского содержания.

¹ Грачев Г. В. Информационно-психологическая безопасность личности: теория и технология психологической защиты: автореф. дис. ... д-ра психол. наук. М., 2000. С. 20.

² Рыдченко К. Д. Административно-правовое обеспечение информационно-психологической безопасности органами внутренних дел Российской Федерации: автореф. дис. ... канд. юрид. наук. Воронеж, 2011. С. 10.

³ Об утверждении Доктрины информационной безопасности Российской Федерации: Указ Президента РФ от 5 декабря 2016 г. № 646. Доступ из справ.-правовой системы «КонсультантПлюс».

В указанных целях в первую очередь необходимо определить возможные источники, через которые деструктивная информация может доходить до большей части населения.

На данный момент все больше граждан в качестве источника актуальных новостей предпочитают новостные сообщества в мессенджерах и социальных сетях. Согласно официальным статистическим данным ВЦИОМ сегодня новостные сообщества возглавляют рейтинг самых популярных подписок в мессенджерах и социальных сетях. В среднем около 77% пользователей регулярно просматривают новости из вышеуказанных источников¹. Среднесуточный охват новостных сообществ сегодня составляет примерно 16% всего населения страны. При этом, как отмечается в отдельных социологических исследованиях, в моменты, когда органами государственной власти принимались важные в масштабах всей страны решения, среднесуточный охват новостных сообществ социальных сетей и мессенджеров достигал около 25% всего населения страны².

Данный формат распространения информации позволяет пользователям быстро, удобно и концентрированно узнавать об актуальных новостях, ввиду чего он и пользуется популярностью. Важно учитывать, что в новостных сообществах преимущественно распространяется именно общественно значимая информация, под которой согласно положениям п. 2 ч. 1 ст. 15.3 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее – Федеральный закон об информации) понимается та информация, недостоверное распространение которой «создает угрозу причинения вреда жизни и (или) здоровью граждан, имуществу, угрозу массового нарушения общественного порядка и (или) общественной безопасности либо угрозу создания помех функционированию или прекращения функционирования

¹ Социальные сети и мессенджеры: вовлеченность и предпочтения // ВЦИОМ. URL: <https://wciom.ru/analytical-reviews/analiticheskii-obzor/socialnye-seti-i-messendzhery-vovlechennosti-i-predpochtenija> (дата обращения: 25.01.2025).

² Аудитория интернета в 2022 году // Mediascope. URL: https://mediascope.net/upload/iblock/3d8/qrlyhud7t7dxyzw1rhtzvg3rwk8deg7uk/2022_%D0%98%D0%9D%D0%A2%D0%95%D0%A0%D0%9D%D0%95%D0%A2.pdf (дата обращения: 07.02.2023).

объектов жизнеобеспечения, транспортной или социальной инфраструктуры, кредитных организаций, объектов энергетики, промышленности или связи»¹.

Важность данной информации и вызывает наибольший интерес среди большинства пользователей. Содержание новостных публикаций зачастую провоцирует обсуждение пользователей в комментариях, среди которых нередко могут распространяться экстремистские материалы. Особенно опасной представляется ситуация, при которой в данных сообществах распространяется информация сомнительного происхождения, специально направленная на привлечение внимания аудитории и провоцирующая «эмоциональные» обсуждения среди пользователей. Вместе с тем сам формат распространения общественно значимой информации в социальных сетях и мессенджерах создает условия для вышеуказанных негативных явлений, что обусловлено особенностями механизма создания и администрирования самих новостных сообществ в социальных сетях и мессенджерах.

На сегодняшний день крупнейшие социальные сети и мессенджеры предоставляют возможность любому зарегистрированному пользователю стать владельцем или администратором (по умолчанию это один и тот же пользователь) неограниченного количества сообществ². Более того, администратор имеет возможность сохранять при этом свою анонимность. Таким образом, любой человек, в том числе не имеющий соответствующего профильного образования в сфере журналистской деятельности либо иной специальной подготовки, оборудования, соответствующей лицензии и т.д., может освещать какие-либо события от лица созданного им новостного сообщества на общих с любыми другими пользователями основаниями.

¹ Об информации, информационных технологиях и о защите информации: федеральный закон от 27 июля 2006 г. № 149-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

² Фактически владелец сообщества может делегировать другому пользователю управление сообществом (возможность публикации материалов, добавления и удаления участников и т.д.), наделив его правами администратора. Однако поскольку данное действие не снимает никакой ответственности с непосредственного владельца, то для целей настоящего исследования понятия администратора и владельца новостного сообщества в социальной сети или мессенджере будут использованы в качестве синонимов.

Рассматривая вопрос о порядке администрирования и размещения публикаций в новостных сообществах социальных сетей и мессенджеров, считаем необходимым отметить, что само существование данных сообществ зачастую обусловлено исключительно стремлением их владельцев к получению денежной выгоды. Администраторы могут за вознаграждение размещать различные рекламные публикации. Возможность зарабатывать предоставляют непосредственно сами социальные сети и мессенджеры. Например, по заявлению создателя мессенджера «Telegram» П. В. Дурова, администраторы телеграм-каналов будут иметь возможность получать денежные выплаты за показ рекламы напрямую от представителей платформы¹.

На наш взгляд, данный факт во многом обуславливает такую негативную черту отдельных новостных сообществ социальных сетей и мессенджеров, как отсутствие у их администраторов прямой заинтересованности в размещении достоверного и качественного материала. Вместо этого на первый план выходит стремление привлечь как можно большую аудиторию с целью получения материальной выгоды². Указанный подход не только не способствует опубликованию тщательно проверенных и качественных материалов, но и наоборот, побуждает их размещать как можно более провокационный контент, который вызовет резонанс среди пользователей, заставит их подписаться на сообщество и распространить информацию среди своих знакомых. В своем исследовании О. И. Ляховенко отмечает существование значительного количества телеграм-каналов, в которых размещаемые материалы носят тенденциозный характер, преобладает пересказ слухов и сплетен, умозрительные и конспирологические построения, ангажированные позиции³.

¹ Telegram начнет платить владельцам каналов за рекламу // РБК. URL: https://www.rbc.ru/technology_and_media/28/02/2024/65df2cf39a794735d2013709 (дата обращения: 21.03.2024)

² Ильиных Н. А. Новостные сообщества в социальных сетях и мессенджерах как источник распространения фейковой информации // Актуальные проблемы профилактики преступлений: тезисы докл. и сообщ. междунар. науч.-практ. семинара. Омск: Омская академия МВД России, 2024. С. 14.

³ Ляховенко О. И. Телеграм-каналы в системе экспертной и политической коммуникации в современной России // Galactica Media: Journal of Media Studies. 2022. № 1. С. 136.

Необходимо отметить, что сегодня существует высокая конкуренция между новостными сообществами. По состоянию на конец 2024 г. только в мессенджере «Telegram» зарегистрирована по меньшей мере 61 тыс. новостных сообществ, продающих рекламу¹. Данный факт побуждает администраторов сообществ раньше всех остальных публиковать информацию, которая вызовет интерес среди пользователей, при этом качество данных материалов, как правило, может не иметь особого значения. В свою очередь чем более провокационной будет сама новость, а также ее подача, тем больше внимания пользователей она привлечет и вызовет зачастую негативные обсуждения в комментариях, создавая условия для распространения экстремистского контента.

В связи с этим, учитывая высокий уровень восприимчивости населения к различной деструктивной информации, размещаемой в киберпространстве, а также значительную вовлеченность населения в просмотр контента в новостных сообществах социальных сетей и мессенджеров, полагаем, что в целях обеспечения информационно-психологической безопасности граждан необходимо усовершенствовать механизм государственного контроля за соблюдением порядка размещения общественно значимой информации в данных источниках. Для этого в первую очередь необходимо соответствующим образом адаптировать существующую нормативно-правовую базу.

На сегодняшний день вопрос о правовом статусе новостных сообществ в социальных сетях и мессенджерах остается нерешенным. Данные сообщества не являются средствами массовой информации. Согласно положениям ст. 8 Закона РФ от 27 декабря 1991 г. № 2124-1 «О средствах массовой информации» даже при подаче соответствующего заявления они не могут быть признаны средством массовой информации, ввиду того что они не являются самостоятельными

¹ Каталог Telegram-каналов и чатов Новости и СМИ // Сервис аналитики Telegram-каналов и чатов «TGStat». URL: <https://tgstat.ru/news> (дата обращения: 05.02.2025).

сайтами, а функционируют на базе существующих информационных ресурсов, в нашем случае – сайтов социальных сетей и мессенджеров¹.

В тексте Федерального закона об информации содержится ряд понятий, прав, обязанностей и запретов, регламентирующих порядок распространения информации в социальных сетях и мессенджерах, однако не в полной мере регулирующих рассматриваемый нами аспект. В ст. 10.4 Федерального закона об информации содержится понятие «владелец новостного агрегатора», под которым понимается «владелец сайта и (или) страницы сайта в сети «Интернет», и (или) информационной системы, и (или) программы для электронных вычислительных машин, которые используются для обработки и распространения новостной информации в сети «Интернет» на государственном языке Российской Федерации, государственных языках республик в составе Российской Федерации или иных языках народов Российской Федерации, на которых может распространяться реклама, направленная на привлечение внимания потребителей, находящихся на территории Российской Федерации, и доступ к которым в течение суток составляет более одного миллиона пользователей сети «Интернет».

Исходя из данной формулировки рассматриваемые нами сообщества не охватываются вышеуказанным понятием, поскольку непосредственным владельцем сайта и (или) страницы является именно социальная сеть или мессенджер, но не владелец новостного сообщества, функционирующего в их рамках. Более того, согласно ч. 10 ст. 10.4 новостной информацией признается только информация из официально зарегистрированных средств массовой информации. В свою очередь владельцы новостных сообществ могут публиковать информацию из любых иных источников. О том, что рассматриваемые нами сообщества не регламентируются данной правовой нормой, свидетельствует и тот факт, что по состоянию на февраль 2025 г. в соответствующем реестре Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (далее – Роскомнадзор) содержится лишь 6 новостных

¹ О средствах массовой информации: Закон РФ от 27 декабря 1991 г. № 2124-1. Доступ из справ.-правовой системы «КонсультантПлюс».

агрегаторов («Новости@mail.ru», «СМИ2», «Рамблер/новости», «Новости», «24СМИ»), которые не являются новостными сообществами в социальных сетях и мессенджерах.

Существующая на данный момент редакция ст. 10.6 Федерального закона об информации «Особенности распространения информации в социальных сетях» регламентирует деятельность непосредственно социальных сетей, таких как «ВКонтакте», «Одноклассники» и др., однако, за исключением отдельных положений, указанный порядок не распространяется на администраторов сообществ, созданных на базе данных социальных сетей. Закрепленный порядок признания ресурса социальной сетью, в случае если в течение суток его посещает более пятисот тысяч пользователей сети Интернет, находящихся на территории Российской Федерации, также не относится к новостным сообществам в социальных сетях и мессенджерах, о чем в том числе свидетельствует их отсутствие в действующем реестре социальных сетей Роскомнадзора.

Определенная правовая регламентация деятельности владельцев сообществ в социальных сетях и мессенджерах появилась сравнительно недавно¹. В положениях ст. 10.6 Федерального закона об информации был закреплен ряд обязанностей для лиц, объем аудитории персональных страниц которых составляет более десяти тысяч пользователей. Ключевым изменением стало закрепление обязанности данных лиц подавать сведения о себе в Роскомнадзор для ведения соответствующего реестра. Таким образом, был сделан важный шаг по деанонимизации большого количества каналов в социальных сетях и мессенджерах. Вместе с тем указанные изменения касаются преимущественно только одной обязанности по предоставлению контактных данных владельцев сообществ. В остальном для владельцев рассматриваемых сообществ в порядке распространения информации сегодня нет существенных отличий от рядовых пользователей.

¹ О внесении изменений в Федеральный закон «О связи» и отдельные законодательные акты Российской Федерации: федеральный закон от 8 августа 2024 г. № 303-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

Таким образом, на сегодняшний день в законодательстве не существует отдельного порядка распространения общественно значимой информации через новостные сообщества в социальных сетях и мессенджерах. Соответствующая ответственность за распространение перечисленных в ч. 1 ст. 15 Федерального закона об информации видов распространяемой с нарушением закона информации в отношении владельцев новостных сообществ в социальных сетях и мессенджерах наступает на общих для всех пользователей основаниях, предусмотренных административным и уголовным законодательством.

Таким образом, при большом количестве новостных каналов, их популярности среди населения, а также в связи с особенностями порядка их администрирования и недостаточностью правовой регламентации создаются условия для распространения экстремистских материалов среди большого числа пользователей. В связи с этим считаем, что в целях обеспечения информационно-психологической безопасности личности и общества необходимо принять ряд мер правового и организационного характера.

Полагаем, что целесообразно в рамках Федерального закона об информации регламентировать порядок функционирования новостных сообществ и порядок размещения в них информации¹. В указанных целях представляется необходимым внести изменения в действующую редакцию данного федерального закона, дополнив статью 10.6 частями 1.4 и 1.5, которые закрепили бы за владельцами новостных сообществ часть обязанностей, аналогичных тем, которые возложены сегодня на владельцев социальных сетей (п. 1–5 ч. 1 ст. 10.6).

Говоря о владельцах новостных сообществ в социальных сетях и мессенджерах, считаем нецелесообразным в тексте предлагаемых новых пунктов использовать существующее в законе определение данных лиц «владелец персональной страницы, объем аудитории которой составляет более десяти тысяч пользователей социальной сети...». Вместе с тем возможно дополнить его словами «и на которой систематически распространяется общественно значимая информация», подчеркнув особый статус таких страниц и их владельцев.

¹ См. Приложение 6.

Аналогично правильным считаем не обозначать в тексте предлагаемых пунктов отдельно владельцев новостных сообществ в мессенджерах, поскольку данные ИТТ по смыслу рассматриваемого закона охватываются понятием «социальные сети», о чем свидетельствует содержание реестра социальных сетей Роскомнадзора, в котором, например, присутствует мессенджер «Telegram».

Также считаем необходимым создать отдельный реестр новостных сообществ в социальных сетях в целях осуществления контроля со стороны Роскомнадзора, аналогично порядку, предусмотренному для владельцев персональных страниц, объем аудитории которых составляет более десяти тысяч пользователей, новостных агрегаторов, СМИ и социальных сетей. Полагаем, что указанная мера в значительной степени будет способствовать осуществлению эффективного контроля со стороны правоохранительных органов. В свою очередь 34,4% опрошенных нами сотрудников ЦПЭ относительно того, направление деятельности каких органов, организаций, подразделений, по их мнению, следует усилить в целях повышения эффективности предупреждения экстремизма, указали именно на государственные органы в сфере защиты информации¹.

Считаем, что предложенная мера не только будет эффективна для организации контроля за экстремистской информацией в социальных сетях и мессенджерах, но и одновременно позволит нивелировать определенную нами внутреннюю субъективную предпосылку уголовного киберэкстремизма, выражающуюся в высоком уровне восприимчивости населения к экстремистским материалам, распространяемым в киберпространстве.

Как нами уже отмечалось ранее, сегодня прослеживается тенденция усиления роли киберэкстремистских фейков в деструктивном информационно-психологическом воздействии на население. В связи с этим считаем, что работа по их разоблачению требует особого внимания в целях обеспечения информационно-психологической безопасности личности и общества. Как отмечает в своей работе С. Н. Фридинский, именно просветительская деятельность должна выступать одним из ключевых направлений

¹ См. Приложение 1.

предупреждения экстремистской деятельности¹. Аналогичную точку зрения высказывает также С. В. Криштопов, отмечая важную роль пропагандистской деятельности для профилактики экстремизма².

Ключевой проблемой здесь является то, что отдельные фейки могут быть достаточно тщательно подготовлены, и обычному пользователю тяжело определить их достоверность. В своем исследовании А. И. Коробеев и Д. В. Жмуров утверждают, что сегодня практически каждый второй гражданин признается, что не может отличить достоверную информацию от ложной³. Полагаем, что необходимо активизировать организованную работу по разоблачению недостоверных сведений. В указанных целях нами предлагается создание специализированных государственных информационных платформ, на которых систематически публиковались бы разоблачения фальшивых новостей и объяснения существующих форм проявления экстремизма и ответственности за их совершение. Данные платформы должны быть представлены в формате интернет-сайтов, а также сообществ (групп, каналов и т.д.) на базе популярных среди граждан социальных сетей, мессенджеров и видеохостингов.

Необходимо отметить, что сегодня в некоторых социальных сетях и мессенджерах уже существуют отдельные проекты, которые публикуют разоблачения (например, новостные сообщества «Война с фейками» и «АнтиФейк.Основа» в мессенджере «Telegram» или медиапроект «АнтиФейк» «Первого канала»). Тем не менее их деятельность не носит системного характера и является инициативой отдельных граждан или организаций. К тому же некоторые подобные проекты по сути представляют собой анонимные новостные сообщества в социальных сетях и мессенджерах (сообщества, группы, каналы и т.д., в которых невозможно устано-

¹ Фридинский С. Н. Противодействие экстремистской деятельности (экстремизму) в России (социально-правовое и криминологическое исследование): автореф. дис. ... д-ра юрид. наук. М., 2011. С. 10.

² Криштопов С. В. Уголовно-правовое противодействие преступлениям экстремистской направленности: автореф. дис. ... д-ра юрид. наук. М., 2022. С. 8.

³ Коробеев А. И., Жмуров Д. В. Кибервиктимология фейка: первичное досье // Вестник Томского государственного университета. 2021. № 471. С. 254.

вить их владельца), что не дает оснований полностью доверять публикуемой в них информации.

По этой причине необходимо, чтобы на предлагаемых нами информационных платформах просветительская работа велась от лица государственных органов. Тем самым государство здесь должно выступать в качестве гаранта качества и достоверности публикуемых материалов, что крайне важно в контексте противодействия фальсификации общественно значимой информации. С данным утверждением согласилось также большинство (84,8%) опрошенных жителей Омской области, указав на более высокий уровень доверия именно к той информации, которая публикуется от лица государственных органов. Поэтому считаем целесообразным создание соответствующих информационных платформ с обязательной отметкой, позволяющей идентифицировать их как официальный государственный источник.

Как нами уже отмечалось ранее, экстремистские сообщества и организации, распространяющие свои материалы в киберпространстве, сегодня уделяют особое внимание внешней привлекательности своего контента в целях привлечения и удержания внимания пользователей. Поэтому при организации работы соответствующих информационных платформ важно обеспечить создание не только достоверного, но и привлекательного контента, способного заинтересовать пользователей. Полагаем, что в указанных целях к данной работе крайне важно привлекать соответствующих специалистов в сфере журналистики, графического дизайна, видеомонтажа и т.д.

Полагаем, что данная мера значительно снизит негативный эффект, оказываемый на общество в результате массового распространения недостоверных сведений в киберпространстве, а также способствует повышению осведомленности населения относительно существующих сегодня форм проявления экстремизма и ответственности за совершение деяний экстремистской направленности.

Вместе с тем в контексте предупреждения распространения недостоверных новостных публикаций и противодействия их негативному эффекту на общество,

кроме просветительской работы среди населения, перспективной мерой также будет создание системы автоматизированной верификации новостных публикаций в информационно-телекоммуникационном пространстве (далее – САВНИ). Данная система позволит оперативно и лишь при незначительном участии человека определять степень достоверности любой новости в киберпространстве. С учетом современного уровня развития информационно-телекоммуникационных технологий представляется вполне возможным разработать соответствующее программное обеспечение (далее – ПО)¹.

На наш взгляд, в основе работы ПО целесообразно использовать технологии искусственного интеллекта, что в полной мере согласуется с положениями подп. 12 п. 57 Стратегии национальной безопасности о том, что необходимо совершенствовать средства и методы обеспечения информационной безопасности на основе применения передовых технологий, включая технологии искусственного интеллекта (далее – ИИ). Более того, необходимость в проведении научных исследований, направленных на разработку и применение технологий искусственного интеллекта при осуществлении мониторинга средств массовой информации и информационно-телекоммуникационных сетей, прямо указана в положениях Стратегии противодействия экстремизму в Российской Федерации.

Учитывая, что информация в новостных сообществах социальных сетей и мессенджерах редко дословно дублирует соответствующую новость, опубликованную в официальных СМИ или на информационном ресурсе какого-либо государственного органа, представляется невозможным просто сопоставить исходный текст новостной публикации. Необходимо, чтобы САВНИ была способна определить основную мысль исходных текстов и соотнести ее с имеющейся на порталах государственных органов и СМИ информацией.

¹ Программное обеспечение встроенных систем. Общие требования к разработке и документированию: государственный стандарт РФ ГОСТ Р 51904-2002 от 25 июня 2002 г. № 247-с. Доступ из справ.-правовой системы «КонсультантПлюс».

В указанных целях следует использовать технологии ИИ, которые могут осуществлять семантический (смысловой) анализ текста.

Сегодня для решения данных задач активно используются алгоритмы обработки естественного языка под общим названием NLP (от англ. «natural language processing» – «обработка естественного языка»), являющиеся технологией машинного обучения, которая предназначена для обработки, анализа и понимания человеческого языка¹. Об эффективности данной технологии и ее пригодности для решения поставленной задачи свидетельствует тот факт, что указанные алгоритмы сегодня уже активно внедряются для решения задач законотворческой деятельности². Исследователями активно обсуждаются возможности применения NLP и в правоприменительной деятельности. Например, в своем исследовании С. В. Немира рассматривает перспективы использования данной технологии в оценке достоверности заключений эксперта по уголовным делам³.

Для определения степени достоверности новостной информации указанная технология может быть использована для анализа содержания сверяемой информации, а также для ее сопоставления с данными, содержащимися на официальных информационных порталах государственных органов и СМИ. В результате САВНИ может предоставлять пользователю ответ, содержащий оценку содержания новостной публикации как потенциально достоверной или ложной.

На наш взгляд, ПО все же должно предоставлять именно оценочные ответы, без утверждения о безусловной истинности результатов своего анализа. Сегодня множество исследователей отмечают, что технологии ИИ могут иногда допускать ошибки. Например, при рассмотрении вопроса о возможности использования ИИ

¹ Aditya Jain, Gandhar Kulkarni, Vraj Shah: Natural Language Processing. International Journal of Computer Sciences and Engineering, Vol.6, Issue.1, pp.161-167 (2018)

² Власти ХМАО создадут нейросеть для написания законов // Ведомости. Страна. URL: <https://www.vedomosti.ru/strana/ural/news/2024/03/05/1023817-vlasti-hmao-sozdadut> (дата обращения: 04.04.2024).

³ Немира С. В. Искусственный интеллект в оценке достоверности заключения эксперта по уголовным делам. Постановка проблемы // Государственная служба и кадры. 2023. № 5. С. 250-254.

в судебной экспертизе А. И. Хмыз отмечает, что искусственный интеллект способен оперативно обрабатывать непосильный человеку постоянно увеличивающийся объем информации, однако результаты его применения следует подвергать оценке эксперта¹. Однако задача по анализу и сопоставлению новостной информации представляется гораздо менее сложной для ИИ, поскольку здесь, как правило, отсутствует труднообрабатываемая для машины специфическая терминология, присущая экспертной деятельности. Таким образом, вероятность допущения ошибки ИИ в результате анализа достоверности новостной информации значительно ниже, тем не менее нельзя полностью исключать такую возможность. В связи с этим следует предоставлять пользователю результаты работы ПО в виде оценочных суждений, без утверждения об абсолютной истинности проведенного искусственным интеллектом анализа.

Таким образом, нами предложен механизм автоматизированной верификации текстовой информации. Однако в киберпространстве контент может быть представлен в видео- или аудиоформате. Поэтому прежде всего его следует предварительно преобразовать в текст, который потом смогут обработать вышеописанные алгоритмы NLP. Для решения поставленной задачи также целесообразно использовать технологии ИИ, которые позволяют автоматически преобразовывать аудиозаписи в текстовый формат. Данные технологии сегодня часто называют ASR (от англ. «automatic speech recognition» – «автоматическое распознавание речи»)². Их применение позволяет распознавать и извлекать текст из аудиозаписи. В случае если новость представлена в формате видеозаписи, то САВНИ первоначально извлекает ее аудиодорожку, которая в последующем преобразовывается в текст алгоритмами ASR. В результате можно автоматически обрабатывать новостную информацию видео- и аудиоформата, чтобы приводить

¹ Хмыз А. И. Использование возможностей искусственного интеллекта в судебной экспертизе // Вестник экономической безопасности. 2022. № 5. С. 224-227.

² Валуйцева И. И., Филатов И. Е. Разработка программы ASR для распознавания вариантов русского языка // Полилингвильность и транскультурные практики. 2021. № 3. С. 145.

ее к единообразному виду – текстовому для последующей работы в целях ее сравнения с информацией на официальных новостных порталах органов государственной власти и СМИ.

В целях повышения эффективности работы САВНИ для определения достоверности новостей следует также подвергать автоматизированному анализу изображения, которыми нередко сопровождаются новостные публикации. Ввиду того, что для создания фейковых новостей зачастую используются давно опубликованные и не имеющие отношения к описываемому событию изображения, целесообразно определять, когда и в каком контексте впервые изображение было опубликовано. На сегодняшний день на базе популярных поисковых систем (Yandex, Google, Bing и др.) уже существуют соответствующие технологии, позволяющие осуществлять обратный поиск изображений в интернете (пользователь отправляет изображение, а в ответе получает информацию о дате, месте публикации, а также контексте, в котором оно было опубликовано). Использование данных технологий в САВНИ способствует существенному повышению эффективности работы всей системы.

В результате при объединении всех вышеописанных элементов образуется система автоматизированной верификации новостной информации, которая способна анализировать содержание новостных публикаций, представленных в любом формате (текст, аудио, видео, фото), и сверять их с информацией из официальных новостных порталов органов государственной власти и СМИ.

Далее важно определить направления применения САВНИ в контексте противодействия фейковым новостям. Выделим два наиболее перспективных направления использования САВНИ:

1. Автоматизированная верификация фейковых новостей в информационно-телекоммуникационном пространстве в целях повышения эффективности работы правоохранительных органов по выявлению, обработке и блокировке противоправного контента;

2. Использование системы любым пользователем в целях автоматизированной проверки достоверности любой новостной публикации в информационно-телекоммуникационном пространстве.

Говоря о целесообразности применения САВНИ непосредственно в правоохранительной деятельности, подчеркнем, что в ходе проведенного нами опроса 87,5% сотрудников ЦПЭ отметили, что сегодня в их деятельности актуальной является проблема, связанная с недостатком времени, сил и средств на выявление и обработку содержащегося в интернете экстремистского контента. При этом подавляющее большинство опрошенных сотрудников указали, что внедрение программного обеспечения, обеспечивающего автоматизацию анализа большого количества информации в интернете, способно значительно повысить эффективность их деятельности¹.

Таким образом, считаем, что применение САВНИ в деятельности правоохранительных органов будет иметь существенный положительный эффект в части, касающейся оперативного выявления, обработки и блокировки фейковых новостей в киберпространстве, что в свою очередь позволит своевременно пресекать их негативное информационно-психологическое воздействие на общество.

Несмотря на то, что правоохранительные органы должны играть ключевую роль в защите граждан от различных преступных посягательств, в криминологии значительное внимание уделяется также виктимологической профилактике как одному из важных направлений в предупреждения преступлений. Безусловно, человека, который просмотрел фейковую новость и воспринял ее как достоверную, нельзя назвать жертвой в классическом понимании этого термина. Однако можно с уверенностью утверждать, что при просмотре фальшивых новостей человек подвергается негативному информационно-психологическому воздействию, что может стать причиной приобретения им экстремистских взглядов и убеждений. В свою очередь любая фейковая новость не будет иметь никакого эффекта, если человек будет уверен в ее недостоверности. Поэтому

¹ См. Приложение 1.

крайне важно предоставить гражданам как можно больше инструментов для быстрой и удобной проверки достоверности новостных публикаций.

Сегодня в случае обнаружения пользователем новостной публикации, в достоверности которой он сомневается, ему необходимо самостоятельно ее перепроверять на различных информационных ресурсах. Результаты проведенного нами социологического опроса жителей Омской области свидетельствуют о том, что респонденты, а также люди из их близкого окружения далеко не всегда перепроверяют новостную информацию, публикуемую в социальных сетях и мессенджерах. Так, на вопрос: «Как часто Вы перепроверяете информацию, опубликованную в мессенджерах, социальных сетях, интернет-сайтах, иных источниках?» – 29,8% опрошенных ответили, что относятся к проверке безразлично. На аналогичную просьбу оценить, как часто люди из близкого окружения респондентов перепроверяют информацию, 37,8% указали на безразличное отношение их близких к проверке достоверности публикуемой в социальных сетях и мессенджерах информации¹.

Полагаем, что предоставление гражданам доступа к функционалу САВНИ позволит им быстро осуществить предварительную оценку степени достоверности новостных публикаций. Возможность в кратчайшие сроки и в автоматизированном режиме оценить достоверность той или иной новостной публикации может избавить граждан от достаточно трудоемкого процесса самостоятельного поиска информации из различных источников, что в свою очередь снизит долю людей, которые вовсе не перепроверяют новостную информацию.

Реализовать работу САВНИ для ее самостоятельного использования пользователями наиболее целесообразно на базе вышеописанных нами информационных платформ, посвященных разоблачению фейковых новостей. Для удобства использования гражданами ПО можно реализовать в формате ботов (от англ. bot (robot) – робот). Основным преимуществом данной реализации является то, что боты могут функционировать непосредственно в социальных сетях, мессендже-

¹ См. Приложение 4.

рах, на отдельных интернет-сайтах без необходимости установки дополнительного ПО непосредственно на устройство пользователя, делая САВНИ доступным для любого гражданина, имеющего выход в интернет.

Далее перейдем к мерам, направленным на устранение внутренней объективной предпосылки формирования экстремистских взглядов и убеждений среди населения. Как нами уже отмечалось, в качестве таковой выступает имплицитное информационно-деструктивное воздействие, которое выражается в распространении сведений относительно совершения преступлений и (или) административных правонарушений с прямым указанием на принадлежность виновника к той или иной социальной группе, объединенной по политическим, религиозным, национальным или идеологическим признакам. Полагаем, что для устранения последней предпосылки будет достаточно внести соответствующие изменения в законодательство, регламентирующее порядок распространения информации, а также обеспечить соответствующий государственный контроль.

Действующая редакция ст. 4 Закона о СМИ «Недопустимость злоупотребления свободой массовой информации» содержит запрет на распространение экстремистских материалов в средствах массовой информации, однако рассматриваемая нами форма ИДИПВ положениями данной статьи не охватывается. Полагаем, что необходимо дополнить текст указанной нормы следующим образом: *«...публично оправдывающих терроризм, других экстремистских материалов, материалов, содержащих сведения относительно совершения правонарушений с прямым указанием на принадлежность лица, его совершившего, к той или иной социальной группе, объединенной по политическим, религиозным, национальным или идеологическим признакам...»¹.*

Необходимо сказать, что в 2021 году в Государственную Думу уже вносился на рассмотрение проект федерального закона № 21931-8, предусматривавший внесение аналогичных изменений в данную статью². Однако тогда законопроект

¹ См. Приложение 6.

² О внесении изменения в статью 4 Федерального закона «О средствах массовой информации» // Система обеспечения законодательной деятельности. URL: <https://sozd.duma.gov.ru/bill/21931-8> (дата обращения: 15.02.2025).

был отклонен, законодатель сослался на то, что указанные действия не содержат признаков состава какого-либо преступления или правонарушения, назвав указание национальности или вероисповедания правонарушителя «обычным информированием». Считаем, что указанная аргументация сегодня представляется не вполне обоснованной. Запреты, установленные в ст. 4 Закона о СМИ, не всегда связаны с фактом совершения правонарушения. Ответственность наступает за сам факт нарушения установленных в данной статье запретов, о чем свидетельствуют положения ст. 13.15. КоАП РФ «Злоупотребление свободой массовой информации». Также считаем, что предлагаемые нами изменения способствуют соблюдению положений ст. 29 Конституции РФ, устанавливающей запрет на «пропаганду и агитацию, возбуждающие социальную, расовую, национальную или религиозную ненависть и вражду, а также на пропаганду социального, расового, национального, религиозного или языкового превосходства». Таким образом, учитывая результаты проведенного нами контент-анализа, свидетельствующие о «всплеске» среди пользователей экстремистских высказываний и негативной реакции в адрес представителей социальной группы, к которой принадлежит виновник, закрепление соответствующего запрета представляется необходимой и обоснованной мерой по обеспечению информационно-психологической безопасности личности.

Продолжая рассматривать проблему противодействия имплицитному информационно-деструктивному воздействию, перейдем к изучению вопроса о предупреждении распространения деструктивной идеологии через различные фильмы, видеоигры, книги и т.д. Данная информация сама по себе не является экстремистской, однако ее содержание при определенной интерпретации может оказывать серьезное деструктивное информационно-психологическое воздействие на человека, формируя в нем чувство неприязни к другим людям, побуждая к насилию или причинению вреда себе.

Как мы отмечали ранее, наиболее подвержены указанному деструктивному информационно-психологическому воздействию несовершеннолетние, а значит, и

комплекс соответствующих предупредительных мер должен быть адресован именно им.

На сегодняшний день Постановлением Правительства от 28 апреля 2023 г. № 1105-р принята Концепция информационной безопасности детей в Российской Федерации¹. Указанный документ содержит комплекс направлений по обеспечению соответствующих элементов информационно-психологической безопасности несовершеннолетних в киберпространстве. Считаем, что приоритетными направлениями в решении рассматриваемой нами проблемы должны выступать: взаимодействие с родительским сообществом; активизация работы по привлечению детей к участию в общероссийских общественно-государственных движениях детей и молодежи («Движение Первых», «Российское движение школьников» и др.), а также государственная поддержка информационной продукции для детей, способствующей формированию у них социально одобряемых ценностно-моральных ориентиров, нравственной и правовой культуры, гражданственности и патриотизма в соответствии с традиционными ценностями. Отметим, что необходимость работы по данным направлениям сегодня уже закреплена в нормативно-правовых актах, а соответствующая деятельность по ее реализации активно ведется. Тем не менее в указанной деятельности можно выделить несколько проблемных аспектов, затрудняющих реализацию названных положений.

Что же касается распространения информационной продукции среди детей, важно понимать, что дети сегодня чаще всего предпочитают смотреть непродолжительные видеоролики в социальных сетях («TikTok», «VK» и т.д.). Вместе с тем проблема с качеством контента для детей здесь по существу сходна с той, что присуща новостным сообществам в социальных сетях и мессенджерах. Основной целью для многих популярных среди детей блогеров является привлечение все большей аудитории для извлечения последующей финансовой

¹ Об утверждении концепции информационной безопасности детей в Российской Федерации: распоряжение Президента РФ от 28 апреля 2023 г. № 1105-р. Доступ из справ.-правовой системы «КонсультантПлюс».

прибыли. В подавляющем большинстве случаев производимый для детей контент сегодня имеет мало общего с формированием социально одобряемых ценностно-моральных ориентиров, а скорее даже наоборот, нередко носит деструктивный характер. С данным утверждением согласно подавляющее большинство опрошенных нами педагогических работников в сфере школьного образования (84,9%)¹.

На наш взгляд, для решения указанной проблемы необходимо совершенствовать работу по мониторингу качества контента, распространяемого популярными среди детей блогерами. Для этого следует привлекать к указанной деятельности соответствующие государственные органы и общественные организации.

Вместе с тем в целях обеспечения информационно-психологической безопасности подрастающего поколения необходимо совершенствовать работу по взаимодействию государства, педагогических работников и родителей. В своем исследовании Р. О. Кочергин указывает на важность такого взаимодействия в контексте противодействия экстремизму². В своем исследовании, посвященном предупреждению экстремистской преступности несовершеннолетних, Т. Г. Сироткина среди прочего предлагает создать в Федеральном агентстве по делам молодежи специальную службу правовой и социальной помощи для работы с несовершеннолетними лицами, склонными к экстремистским проявлениям. При этом большинство предлагаемых автором полномочий указанная служба должна выполнять во взаимодействии с педагогами и родителями³.

В Стратегии противодействия экстремизму в Российской Федерации сказано, что сегодня необходимо повышать уровень осведомленности руководителей и педагогических работников образовательных организаций в сфере противодействия экстремизму. В ходе опроса педагогических работников в сфере

¹ См. Приложение 5.

² Кочергин Р. О. Противодействие молодежному экстремизму: правовые и криминологические проблемы: дис. ... канд. юрид. наук. Ростов-н/Д, 2008. С. 9.

³ Сироткина Т. Г. Криминологическая характеристика и предупреждение экстремистской преступности несовершеннолетних: автореф. дис. ... канд. юрид. наук. М., 2024. С. 27.

школьного образования нами установлено, что большинство (77,4%) опрошенных указывают на проблему низкой осведомленности родителей о том, какой контент популярен среди их детей¹. Дети гораздо активнее вовлечены в просмотр информации и общение в киберпространстве, нежели их родители. Последние чаще всего не знают о том, какие деструктивные идеи сегодня популярны. Как отмечают сами учителя, они также не всегда успевают следить за всеми новыми молодежными течениями, в результате чего проведение соответствующих профилактических мероприятий с детьми на ранних этапах представляется невозможным.

На наш взгляд, соглашаясь с мнением Э. Г. Юзихановой и Н. А. Корсиковой, для преодоления данной проблемы, помимо прочих, необходимо предпринимать следующие меры²:

1) проведение профилактических бесед с родителями, учителями и другими лицами, влияющими на формирование мировоззрения молодежи, для предупреждения возможного влияния экстремистских идей на их воспитанников;

2) организация образовательных мероприятий, таких как конференции, семинары, круглые столы, посвященные проблемам экстремизма, его последствиям и способам борьбы с ним;

3) сотрудничество с различными организациями и общественными органами, направленными на поддержку молодежи, для предотвращения ее вовлечения в экстремистскую деятельность.

Также отметим особую важность деятельности по привлечению общественных и государственных организаций для мониторинга информационно-телекоммуникационного пространства на предмет возникновения новых деструктивных течений, популярных среди несовершеннолетних. Крайне важно обеспечивать оперативное доведение соответствующей информации до учителей,

¹ См. Приложение 5.

² Юзиханова Э. Г., Корсикова Н. А. Содержание деятельности органов внутренних дел России по противодействию экстремизму в молодежной среде // Правопорядок: история, теория, практика. 2025. № 1. С. 126.

которые в свою очередь должны проводить соответствующие профилактические беседы в рамках классных часов и родительских собраний.

Несмотря на их необходимость, все вышеуказанные меры носят преимущественно реакционный характер. В свою очередь, необходимо всегда стремиться предупреждать угрозу на как можно более раннем этапе. Считаем, что для эффективного предупреждения ИДИПВ сегодня необходимо особое внимание уделять созданию условий для воспитания у детей чувств неприязни к различному деструктивному контенту.

Как справедливо отмечает в своем исследовании Н. Л. Худякова, «основой воспитания в быстро меняющемся обществе могут быть только традиционные ценности, которые должны определять содержание системы целей воспитания»¹. На сегодняшний день документом, определяющим понятие традиционных российских ценностей, а также цели и задачи по их укреплению у подрастающего поколения, являются Основы государственной политики по сохранению и укреплению традиционных российских духовно-нравственных ценностей, утвержденные Указом Президента РФ от 9 ноября 2022 г. № 809². В данном документе прямо закреплена задача по «защите от внешнего деструктивного информационно-психологического воздействия, направленного на разрушение традиционных ценностей в России». На наш взгляд, в контексте настоящего исследования в целях противодействия ИДИПВ среди детей в первую очередь необходимо решить следующие закрепленные в Основах государственной политики взаимосвязанные задачи:

1) поддержка проектов, направленных на продвижение традиционных ценностей в информационной среде;

¹ Худякова Н. Л. Традиционные ценности как основа воспитания в современном быстроменяющемся обществе // Вестник ЧелГУ. 2023. № 4. С. 99.

² Об утверждении Основ государственной политики по сохранению и укреплению традиционных российских духовно-нравственных ценностей: Указ Президента РФ от 9 ноября 2022 г. № 809. Доступ из справ.-правовой системы «КонсультантПлюс».

2) реализация государственной информационной политики, направленной на усиление роли традиционных ценностей в массовом сознании и противодействие распространению деструктивной идеологии.

В целях реализации указанных задач Правительством РФ утверждаются соответствующие планы. Актуальным на данный момент является Распоряжение Правительства РФ от 1 июля 2024 г. № 1734-р «Об утверждении Плана мероприятий по реализации в 2024–2026 годах Основ государственной политики по сохранению и укреплению традиционных российских духовно-нравственных ценностей». Документ содержит перечень планируемых мероприятий (всероссийский конкурс «Послы Победы», всероссийская акция «Георгиевская лента», всероссийская акция «Свеча памяти» и др.). Безусловно, проведение указанных мероприятий является необходимой и эффективной мерой для сохранения и укрепления традиционных российских духовно-нравственных ценностей. Вместе с тем полагаем, что проведение только подобных мероприятий является недостаточным для продвижения традиционных ценностей среди детей в информационной среде. В большинстве случаев данные мероприятия проводятся в очном формате. Вместе с тем, как нами уже отмечалось ранее, сегодня дети значительную часть времени проводят именно в киберпространстве, следовательно, и соответствующие меры должны реализовываться преимущественно именно там. Кроме того, вышеуказанные масштабные мероприятия хотя и проводятся ежегодно, однако они все же не оказывают регулярного и систематического воздействия на подрастающее поколение. Иными словами, они не становятся тем контентом, который дети просматривают ежедневно.

На наш взгляд, для противодействия ИДИПВ в киберпространстве больше внимания необходимо уделять совершенствованию реализации такой меры, как «поддержка проектов, направленных на продвижение традиционных ценностей в сети «Интернет», средствах массовой информации и книжной индустрии». Данная мера, на наш взгляд, является эффективной, а ее дальнейшее совершенствование представляется весьма целесообразным.

Считаем, что следует создать больше условий для получения государственной поддержки новыми авторами социально полезного контента, способствующего воспитанию детей в духе традиционных российских ценностей. Сегодня господдержку могут получить только авторы, у которых минимум 10 000 подписчиков в социальной сети, мессенджере, видео-/аудиохостинге¹. Данное число является весьма существенным. Чтобы набрать такое количество подписчиков, новому автору потребуется немалое количество времени и денежных средств на рекламу. Складывающаяся в результате ситуация отнюдь не способствует массовому появлению в киберпространстве новых авторов. Следовательно, не увеличивается и объем контента, способствующего сохранению и укреплению традиционных российских ценностей.

Считаем, что необходимо предоставить возможность получать государственную поддержку новым авторам социально полезного контента. В результате получится «предоставить трибуну» большому количеству экспертов, которые не имеют возможности для самостоятельного продвижения своих каналов и (или) страниц в социальных сетях, мессенджерах, видео-/аудиохостингах. В свою очередь новыми авторами, претендующими на государственную поддержку, должны выступать ученые, педагоги и деятели искусства, т.е. люди, которые действительно могут донести до подрастающего поколения информацию, способствующую сохранению и укреплению традиционных российских ценностей. Указанная мера будет способствовать увеличению объема социально полезного контента для реализации задачи по усилению роли традиционных ценностей в сознании детей и формированию у них чувства неприязни к деструктивному контенту, распространяемому в киберпространстве.

В результате в рамках настоящего исследования нами определено, что в целях предупреждения киберэкстремистских преступлений, а также нивелирования их негативного информационно-психологического воздействия

¹ Молодежный контент. Требования к проекту // АНО «Институт развития интернета». URL: <https://xn--h1aax.xn--p1ai/contests/molodezhnyy-kontent-10-24> (дата обращения: 03.02.2025).

целесообразно предпринять ряд мер, направленных на обеспечение информационно-психологической безопасности граждан. Нами предлагается следующий комплекс предупредительных мер, способствующих устранению или минимизации негативного влияния определенных ранее внутренних объективных и субъективных предпосылок:

1. Публикуемая в новостных сообществах в социальных сетях и мессенджерах общественно значимая информация может вызывать у пользователей сильные негативные чувства, под воздействием которых в ходе обсуждения нередко распространяются сведения экстремистского содержания. Вместе с тем для владельцев рассматриваемых сообществ в целях их продвижения зачастую бывает выгодным не пресекать подобные «эмоциональные» обсуждения. Более того, в целях поддержания активности аудитории нередко специально публикуются новости сомнительного происхождения или со спорным содержанием. Учитывая огромную популярность среди населения формата получения новостной информации через социальные сети и мессенджеры, в целях предупреждения распространения экстремистской информации считаем необходимым дополнить статью 10.6 Федерального закона об информации частями 1.4 и 1.5, закрепив за владельцами новостных сообществ часть обязанностей, аналогичных тем, которые возложены сегодня на владельцев социальных сетей (п. 1–5 ч. 1 ст. 10.6 Федерального закона об информации). В целях обеспечения контроля предлагается создание реестра новостных сообществ в социальных сетях в порядке, аналогичном предусмотренному для владельцев персональных страниц, объем аудитории которых составляет более десяти тысяч пользователей, новостных агрегаторов, СМИ и социальных сетей.

2. Для совершенствования просветительской деятельности среди населения предлагается активизировать работу соответствующих информационных площадок в социальных сетях, мессенджерах и видеохостингах, с обязательной отметкой, позволяющей гарантировано идентифицировать их как официальные государственные. Важно обеспечить не только информативность публикуемого на

указанных ресурсах контента, но и его внешнюю привлекательность для пользователей.

Для снижения негативного эффекта от высокой восприимчивости населения к экстремистским материалам, распространяемым в киберпространстве, нами предложена концепция программного обеспечения, представляющего собой систему автоматизированной верификации новостной информации (САВНИ). В основу работы САВНИ может быть положена технология искусственного интеллекта в области обработки естественного языка (NLP), которая будет выполнять задачу по анализу содержания проверяемой информации и сопоставлять ее с данными, размещенными на официальных информационных порталах государственных органов и в СМИ¹. Указанную систему предлагается использовать по следующим направлениям:

а) пресечение распространения недостоверных сведений экстремистской направленности в киберпространстве путем внедрения САВНИ в деятельность правоохранительных органов для повышения эффективности их работы по выявлению, обработке и блокировке противоправного контента;

б) предоставление возможности гражданам самостоятельно, быстро и в удобной форме осуществлять предварительную оценку степени достоверности интересующих их новостных публикаций в информационно-телекоммуникационном пространстве.

В целях противодействия ИДИПВ как внутренней объективной предпосылке киберэкстремизма, выражающейся в распространении информации относительно совершения преступлений и (или) административных правонарушений с прямым указанием на принадлежность виновника к той или иной социальной группе, объединенной по политическим, религиозным, национальным или идеологическим признакам, предлагается внести изменения в действующую редакцию ст. 4 Закона о СМИ, закрепив соответствующий запрет и дополнив ее следующи-

¹ Ильиных Н. А. Использование информационных платформ и искусственного интеллекта в противодействии фейковым новостям как мера предупреждения киберэкстремизма // Научный вестник Омской академии МВД России. 2025. Т. 31, № 1. С. 37-43.

ми словами: «...публично оправдывающих терроризм, других экстремистских материалов, *материалов, содержащих сведения относительно совершения правонарушений с прямым указанием на принадлежность лица, его совершившего, к той или иной социальной группе, объединенной по политическим, религиозным, национальным или идеологическим признакам...*». При этом важно обеспечить соблюдение указанных положений и администраторами новостных сообществ в социальных сетях и мессенджерах.

Для предупреждения ИДИПВ на несовершеннолетних через пропаганду деструктивных ценностей в фильмах, видеоиграх, книгах и т.д. предлагается особое внимание уделять следующим перспективным направлениям по обеспечению информационно-психологической безопасности несовершеннолетних:

а) мониторинг содержания информации, распространяемой популярными среди несовершеннолетних блогерами, путем привлечения к указанной деятельности общественных организаций, родительского сообщества и педагогических работников при координационной роли правоохранительных органов в целях своевременного выявления деструктивных идей;

б) увеличение в киберпространстве объема социально полезных материалов, пропагандирующих традиционные российские духовно-нравственные ценности и усиливающих их роль в воспитании у детей чувства неприязни к различным деструктивным идеям;

в) взаимодействие государства, педагогических работников и родительского сообщества по вопросам просветительской деятельности относительно новых деструктивных течений, появляющихся в киберпространстве.

§ 3. Организационно-тактические и технические меры по предупреждению преступлений экстремистской направленности, совершаемых с использованием информационно-телекоммуникационных технологий¹

Как указывает Е. В. Никульченкова, дальнейшее развитие ИТТ и трансформация общества неизбежны. Поэтому государству необходимо выработать эффективные методы своевременного выявления и пресечения таких преступных деяний². В научном сообществе сегодня преобладает идея о том, что предупреждение киберпреступности должно представлять собой многоуровневую деятельность, поскольку, помимо масштабных и долговременных мер общесоциального характера, необходимыми являются разработка и принятие мер более узкого, конкретного характера, имеющих прикладное значение и рассчитанных на достижение цели повышения эффективности деятельности правоохранительных органов, занимающихся предупреждением киберпреступности³.

На наш взгляд, наиболее эффективными мерами борьбы с киберэкстремистскими преступлениями должны выступать технические меры, выражающиеся в разработке и внедрении в деятельность правоохранительных органов новых программных средств, предназначенных для выявления и предупреждения киберэкстремистских преступлений, а также меры организационно-тактического характера, направленные на обеспечение порядка использования вышеуказанных программных средств подразделениями, занимающимися противодействием экстремизму. Как справедливо отмечает И. В. Ботвин, «технологии, наряду с общепрофилактической работой, могут дать возможность сотрудникам правоохранитель-

¹ Основные выводы данного параграфа отражены в публикациях автора: Ильиных Н. А. Предпосылки киберэкстремистских преступлений и отдельные меры их предупреждения // Вестник Дальневосточного юридического института МВД России имени И.Ф. Шилова. 2025. № 3. С. 58-66; Ильиных Н. А. Перспективы применения технологии нейронных сетей в профилактике киберэкстремизма // Преимущество и новации в юридической науке: мат-лы междунар. науч. конф. адъюнктов, аспирантов и соискателей. Омск: Омская академия МВД России, 2023. Вып. 19. С. 47-49.

² Никульченкова Е. В. Некоторые криминологические аспекты противодействия киберпреступлениям в России // Правоприменение в публичном и частном праве: мат-лы Междунар. науч. конф. Омск: Омский государственный университет им. Ф.М. Достоевского, 2023. С. 199.

³ Аносов А. В. Специально-криминологическое предупреждение преступлений, совершаемых с использованием высоких технологий // Труды Академии управления МВД России. 2018. № 4. С. 93-97.

ных органов приумножить свой профессиональный уровень, повысить качество и эффективность деятельности по предупреждению преступлений, связанных с экстремизмом и основанных на экстремистских призывах»¹.

Предупредительные меры, которые будут предложены в рамках настоящего параграфа, направлены преимущественно на прогнозирование и своевременное пресечение готовящихся и на выявление уже совершенных киберэкстремистских преступлений, в том числе тех, в которых задействованы представители зарубежных стран (внешняя объективная предпосылка уголовного киберэкстремизма).

Как нами уже отмечалось ранее, одним из перспективных направлений предупреждения киберпреступлений является применение технологий ИИ. Более того, в подп. 5 п. 36 Стратегии противодействия экстремизму прямо указывается на необходимость проведения научных исследований, направленных на разработку технологий ИИ и их применение при осуществлении мониторинга киберпространства. На наш взгляд, ИИ в контексте противодействия уголовному киберэкстремизму и повышения эффективности деятельности соответствующих подразделений целесообразно использовать в следующих целях:

1) для автоматизации процесса идентификации экстремистского материала в киберпространстве. Соответствующие технологии ИИ (или их комплекс в рамках одного ПО) способны производить достаточно эффективный анализ информации любого формата (текста, аудио, изображения и видео);

2) для прогнозирования подготовки к массовым беспорядкам или иным видам организационной деятельности для совершения преступлений экстремистской направленности в определенной области или среди определенных групп пользователей.

Далее подробно рассмотрим, каким образом можно использовать технологии ИИ для достижения вышеуказанных целей. Крайне важно также определить порядок получения и использования результатов их работы для

¹ Ботвин И. В. Роль современных технологий в предупреждении экстремизма в молодежной среде // Актуальные проблемы борьбы с преступлениями и иными правонарушениями. 2023. № 23-2. С. 9.

предупреждения преступлений экстремистской направленности, совершаемых с использованием ИТТ.

Переходя к рассмотрению вопроса о применении технологий ИИ для автоматизации процесса идентификации экстремистского материала в киберпространстве, необходимо отметить, что указанная мера в первую очередь направлена на решение проблемы, связанной с нехваткой сил и средств на анализ большого количества фактов проявлений экстремизма в киберпространстве у сотрудников подразделений по противодействию экстремизму. В свою очередь 57,35% сотрудников ЦПЭ согласны с утверждением о том, что создание программы на основе искусственного интеллекта, обеспечивающей автоматизацию поиска и анализа информации в сети Интернет на предмет экстремизма, существенно повысит эффективность их деятельности. Около трети опрошенных (31,25%) отметили, что подобная программа позволит частично решать поставленные перед подразделением задачи по выявлению экстремистского контента¹. Таким образом, можно утверждать, что предлагаемая мера предупреждения будет востребована среди практических сотрудников.

Важно отметить, что отдельными исследователями ранее уже рассматривалась возможность применения технологий ИИ в подобных целях. Как отмечает в своем исследовании О. Б. Березина, «в контексте противодействия экстремизму наиболее эффективным представляется использование искусственного интеллекта для автоматизации процессов распознавания объектов, особенно в сфере лингвистики»². Аналогично о возможном применении технологий ИИ для обнаружения и идентификации экстремистского контента в своем исследовании утверждают В. В. Бычков и В. А. Прорвич³.

¹ См. Приложение 1.

² Березина О. Б. Искусственный интеллект и противодействие экстремизму // Актуальные вопросы образования. 2023. № 3. С. 213.

³ Бычков В. В., Прорвич В. А. Искусственный интеллект как средство противодействия преступлениям экстремистской направленности, совершаемым с использованием информационно-телекоммуникационных сетей, в том числе сети Интернет // Вестник Академии Следственного комитета Российской Федерации. 2020. № 4. С. 47-52.

Тем не менее на сегодняшний день в доктрине не выработано подробного научно обоснованного комплекса технологий, который целесообразно применять для автоматизированной идентификации экстремистского контента в киберпространстве. Также требует разрешения вопрос о работе данных технологий в качестве системы для решения поставленной задачи. Более того, нерешенными остаются следующие вопросы: в каком виде может быть представлено данное программное обеспечение? Каким образом программа должна получать доступ к анализируемым материалам? На какие государственные органы и негосударственные организации должна быть возложена обязанность по разработке, совершенствованию и поддержанию работоспособности предлагаемых программных средств?

Чтобы решить все вышеуказанные проблемы и ответить на поставленные вопросы, предложим собственный подробный алгоритм работы программного обеспечения, который может быть использован для автоматизации процесса идентификации экстремистского материала в информационно-телекоммуникационном пространстве.

Как нами уже отмечалось ранее, в большинстве случаев экстремистские материалы в киберпространстве выражаются в форме публичных призывов к осуществлению экстремистской деятельности; в виде публикаций, направленных на возбуждение ненависти либо вражды, а равно унижение человеческого достоинства. Актуальной также остается проблема, связанная с фактами публичной демонстрации нацистской атрибутики или символики, либо атрибутики или символики экстремистских организаций, либо иной атрибутики или символики, публичное демонстрирование которых запрещено.

Для идентификации таких экстремистских материалов целесообразно применять наиболее подходящие технологии ИИ. В данном случае наиболее подходящей технологией ИИ являются нейронные сети. Нейросетевые модели –

это инструменты машинного обучения, в которых компьютер учится выполнять определенную задачу, анализируя примеры обучения¹.

Как правило, информация, которая, например, содержит публичные призывы к осуществлению экстремистской деятельности, обладает рядом практически неизменных признаков, которые можно использовать для обучения нейросетевых моделей, способных автоматически идентифицировать такие материалы как экстремистские. В данном случае важно понимать, что для создания любой нейросетевой модели необходимо большое количество данных, по которым модель будет «учиться», чтобы в последующем «уметь» идентифицировать информацию. В доктрине уже определены соответствующие признаки, которыми обладает тот или иной вид экстремистской информации. Например, И. А. Анисимова, В. В. Ерахмилевич и Е. П. Веснина к числу признаков публичных призывов к экстремистской деятельности относят наличие в сообщении специальных лексических средств, к примеру, глаголов в повелительном наклонении («круши», «делай» и др.)². В случае с действиями, направленными на возбуждение ненависти или вражды, вполне можно определить наличие в сообщении негативных высказываний в отношении представителей какой-либо социальной группы, объединенной по политическим, идеологическим, национальным или религиозным признакам. Также не представляет особого труда подготовить набор обучающих данных для автоматического обнаружения на изображении нацистской символики или символики какой-либо экстремистской организации.

В данном случае перед предполагаемой нейросетевой моделью будет стоять лишь задача по бинарной классификации входных данных, чтобы отнести информацию к одной из двух категорий: экстремистская и неэкстремистская. В своем прототипе системы поиска и обнаружения экстремистских текстовых

¹ Иванько А. Ф., Иванько М. А., Сизова Ю. А. Нейронные сети: общие технологические характеристики // Научное обозрение. Технические науки. 2019. № 2. С. 18.

² Анисимова И. А., Ерахмилевич В. В., Веснина Е. П. Публичные призывы к осуществлению экстремистской и террористической деятельности как угроза безопасности // Гуманитарные, социально-экономические и общественные науки. 2023. № 6. С. 84-88.

сообщений в социальной сети «ВКонтакте» В. Э. Баумтрог, А. В. Еськов, Ю. А. Смирнов использовали предварительно обученную модель DeepPavlov/rubert-base-cased-sentence и получили хороший результат¹. Вместе с тем полагаем, что представленный авторами метод сегодня можно дополнить и обновить с учетом появления более продвинутых предобученных моделей. Общий алгоритм для классификации экстремистских текстов может быть следующим:

1. Сбор и подготовка данных. Для успешного обучения модели необходимо собрать достаточное количество размеченных данных. Следует использовать заранее подготовленные человеком тексты, которые явно классифицированы как экстремистские и неэкстремистские. Данные могут быть собраны из различных источников, таких как социальные сети, мессенджеры, отдельные веб-сайты. Важно обеспечить разнообразие источников и тематики для повышения обобщающей способности модели.

2. Предобработка текста. Необходимо унифицировать тексты:

- а) привести символы к нижнему регистру, удалить нечитаемые символы;
- б) заменить ссылки, телефоны и т.д. на специальные «токены»: <URL>, <PHONE>;

- в) преобразовать текст в числовой формат. Обычно для этого используются векторные представления слов (Embeddings), получаемые в результате обработки текстов такими современными моделями, как RuRoBERTa-large, mDeBERTa-v3, XLM-RoBERTa-large, bge-m3, e5-multilingual-large-instruct и др., чтобы усилить способность нейросетевой модели «понимать» содержание текстов.

3. Разделение данных. Собранные и обработанные данные необходимо разделить на тренировочную и тестовую выборки. Зачастую принято использовать соотношение 80/20, где 80% данных идет на обучение модели, а 20% – на ее тестирование.

¹ Баумтрог В. Э., Еськов А. В., Смирнов Ю. А. Прототип системы поиска и обнаружения экстремистских сообщений в социальной сети ВКонтакте // Полицейская деятельность. 2024. № 5. С. 98-109.

4. Обучение модели. На тренировочной выборке осуществляется обучение модели логистической регрессии. Модель строит функцию, которая пытается предсказать вероятность принадлежности текста к экстремистскому или неэкстремистскому классу.

5. Оценка модели. После обучения модель тестируется на отложенной выборке для оценки ее качества. Используются метрики, такие как точность (accuracy), полнота (recall) и др. Метрики используются, чтобы оценить, насколько хорошо модель справляется с задачей классификации.

Таким образом, реализовав сбор большого количества качественных текстовых данных для обучения модели и применив вышеуказанный алгоритм, можно получить инструмент, который позволит в автоматизированном режиме классифицировать большой объем информации, определяя среди нее экстремистские материалы.

Вместе с тем, несмотря на то что, как отмечает в своем исследовании М. М. Льянов, в киберпространстве экстремистские материалы чаще всего представлены в текстовом виде, считаем вполне обоснованным также создание нейросетевой модели обработки изображений для идентификации на них запрещенной символики¹. В указанных целях следует использовать технологию сверточных нейронных сетей (Convolutional Neural Networks, CNNs).

Общий алгоритм разработки указанных моделей состоит из следующих этапов:

1. Сбор и разметка данных. Собирается набор данных, включающий изображения, содержащие запрещенную символику, в размере не менее 1000 изображений на каждый детектируемый объект (например, нацистской символики), а также изображения, не содержащие такую символику. Данные размечаются, то есть для каждого изображения указывается, присутствует ли на нем запрещенная символика.

¹ Льянов М. М. Криминалистическое значение электронно-цифровых следов преступлений экстремистской и террористической направленности в сети «Интернет»: дис. ... канд. юрид. наук. Екатеринбург, 2025. С. 84.

2. Предобработка данных. Изображения подготавливаются к обработке:

а) все изображения приводятся к единому размеру для обеспечения согласованности входных данных;

б) значения пикселей масштабируются в диапазон от 0 до 1 для улучшения сходимости модели при обучении.

3. Обучение модели. Используется архитектура сверточной нейронной сети:

а) набор данных делится на тренировочную (80%) и тестовую (20%) выборки;

б) модель обучается на тренировочных данных, используя алгоритмы оптимизации для минимизации функции потерь.

4. Оценка модели. После обучения модель тестируется на отложенной выборке данных.

В результате использование вышеуказанных технологий ИИ позволит решить задачу по автоматизации процесса идентификации основных форм экстремистских материалов в информационно-телекоммуникационном пространстве.

Однако, помимо непосредственно разработки соответствующих моделей, крайне важно определить порядок обеспечения их доступа к анализируемой ими информации.

Поскольку в большинстве случаев преступления экстремистской направленности совершаются путем размещения экстремистских материалов в социальных сетях и мессенджерах, считаем, что особое внимание следует уделить именно данному направлению. Для обеспечения автоматизированного выявления экстремистских материалов необходимо использовать комплекс технологий, позволяющих получать доступ к содержанию публикаций, а также комментариев к ним. В целях решения данной задачи можно определить два ключевых направления:

1) выявление факта размещения экстремистского материала в сообществе (группе, канале, чате и т.д.) социальной сети или мессенджера;

2) выявление факта размещения экстремистского материала на личной странице пользователя.

Предлагаемое разделение задачи обусловлено особенностями технической реализации для каждого вышеопределенного случая. Полагаем, что для реализации поставленной задачи в сообществах (группах, каналах, чатах и т.д.) социальных сетей или мессенджеров сегодня уже существует и активно используется необходимая технология, которую следует лишь адаптировать для обеспечения автоматического мониторинга размещаемой информации. В свою очередь для выявления факта размещения экстремистских материалов на личных страницах пользователей потребуются внесение изменений в алгоритм работы самих социальных сетей и мессенджеров. Далее рассмотрим возможный порядок реализации поставленной задачи в сообществах (группах, каналах, чатах и т.д.) социальных сетей и мессенджеров. Считаем, что здесь наиболее целесообразно использовать возможности программ, выполняющих автоматические заранее настроенные повторяющиеся задачи (ботов). Сегодня боты активно используются владельцами сообществ в социальных сетях и мессенджерах для различных задач, в том числе для анализа и обработки комментариев и иных сообщений, поступающих от пользователей.

Например, очень часто боты применяются для автоматического удаления комментариев, содержащих нецензурную лексику, рекламу и т.д. Таким образом, бот, который функционирует внутри сообщества или чата, имеет постоянный доступ ко всей информации, которая в них размещается. Следовательно, указанную возможность можно использовать для решения поставленной нами задачи по обеспечению доступа нейросетевых моделей к анализируемому контенту в целях автоматической идентификации экстремистского материала.

Представляется целесообразной предварительная разработка ботов и последующая их интеграция во все популярные среди российских пользователей социальные сети и мессенджеры. Следует отметить, что указанная задача не представляет серьезных трудностей и не подразумевает под собой создание уникальных ботов для каждого сообщества или чата в каждом отдельном мессенджере или социальной сети. В данном случае количество разрабатываемых ботов будет определяться лишь количеством социальных сетей и мессенджеров, в которых они бу-

дуг функционировать. Функционал данных ботов будет ограничиваться лишь возможностью автоматического сбора появляющейся в конкретном чате или сообществе информации и последующей ее передачей для анализа вышеописанными нейросетевыми моделями. В результате такие боты будут выполнять роль связующего звена между публикуемым контентом и нейросетевыми моделями, обеспечивая последним постоянный доступ к необходимой информации.

Однако важно понимать, что предлагаемые нами боты могут получить необходимый доступ только в случае, если они непосредственно добавлены в сообщество или чат. Считаем, что наиболее эффективным решением данной задачи может стать автоматическое добавление бота в каждое вновь создаваемое сообщество или чат. Обязанность по реализации следует возложить на владельцев социальных сетей и мессенджеров. Для этого предлагается внести соответствующие изменения в текст ст. 10.6 Федерального закона об информации¹.

Переходя к рассмотрению вопроса о возможности автоматического мониторинга содержания публикаций на личных страницах пользователей в социальных сетях, в первую очередь необходимо отметить, что предлагаемые меры не должны применяться в отношении личных переписок пользователя. Установление при помощи предложенных нами алгоритмов факта распространения экстремистского контента через личные сообщения неизбежно затрагивает конституционные права граждан, установленные в ст. 23 Конституции РФ. Следовательно, применение автоматического мониторинга всех личных сообщений пользователей при помощи программных средств в данном случае недопустимо. Выявление фактов совершения преступлений экстремистской направленности возможно только путем проведения соответствующих оперативно-розыскных мероприятий или следственных действий. Однако большинство социальных сетей предоставляют пользователям возможность размещать любую информацию на своих личных страницах, которые доступны для ознакомления неограниченному кругу лиц. Такие действия не охватываются положениями законодательства о неприкосновенности частной жизни. Публикации, размещаемые на личных страницах пользователей

¹ См. Приложение 6.

социальных сетей, обладают всеми признаками общедоступной информации, установленными ст. 7 Федерального закона об информации, следовательно, их можно и нужно собирать, чтобы подвергать анализу на предмет наличия в них экстремистских материалов.

Особенности получения доступа нейросетевых моделей к анализируемой информации, размещаемой на страницах пользователей социальных сетей, обусловлены тем, что в данном случае невозможно использовать такие встроенные в социальные сети и мессенджеры технические средства, как вышеописанные нами боты. Возможности ботов на данный момент чаще всего ограничиваются анализом содержания публикаций и комментариев к ним, размещаемых в сообществах, чатах, каналах и т.д., но не на личных страницах пользователей. Непосредственного и постоянного доступа к содержимому публикаций на личных страницах пользователей такие боты зачастую не имеют. Таким образом, обеспечения необходимого доступа, по нашему мнению, сегодня возможно добиться лишь двумя способами.

Первый способ заключается в разработке стороннего программного обеспечения (то есть не имеющего отношения к самой социальной сети), которое будет в автоматическом режиме путем сплошного перебора открывать все доступные страницы пользователей социальных сетей, сохранять их содержимое и отправлять полученные данные для анализа нейросетевым моделям. Данный метод называется *web scraping* (веб-скрейпинг). На наш взгляд, реализация данного способа будет затруднена тем, что такое программное обеспечение, вероятнее всего, будет автоматически блокироваться алгоритмами защиты самих социальных сетей. Большинство современных сайтов, в том числе сайтов социальных сетей, предусматривают защиту от веб-скрейпинга их ресурсов. Более того, для сбора информации в подобных масштабах при помощи стороннего ПО потребуются значительные вычислительные мощности и материальные затраты на разработку. Вышеописанный способ условно можно охарактеризовать как «внешний» по отношению к самой социальной сети.

Второй способ сбора необходимой информации заключается в доработке существующих алгоритмов социальных сетей для решения поставленной задачи. Полагаем, что организовать автоматическую передачу публикуемой на общедоступных страницах пользователей социальных сетей информации значительно проще и эффективнее «изнутри», без использования стороннего ПО. Реализация указанного способа видится значительно более простой и менее затратной по сравнению с первым способом. Более того, в данном случае от владельцев социальных сетей не потребуется отдельно хранить необходимую информацию, ее следует лишь с определенной периодичностью передавать соответствующим государственным структурам (каким именно, будет рассмотрено далее). Таким образом, будет исключен негативный эффект, связанный с большими материальными затратами на реализацию предлагаемых мер для владельцев социальных сетей, подобный эффекту, произведенному в связи с внесением в Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи» изменений, которые обязали операторов связи хранить данные обо всех сообщениях пользователей на срок до 6 месяцев¹. Для реализации данной меры потребовалось приобретение дополнительного дорогостоящего оборудования для хранения вышеуказанной информации.

В связи с этим полагаем, что предлагаемый нами порядок передачи информации с общедоступных страниц пользователей социальных сетей будет не только эффективно решать задачу по обеспечению доступа нейросетевых моделей к анализируемой информации, но также и не потребует от владельцев социальных сетей существенных материальных затрат на внесение соответствующих изменений в алгоритмы. Для обеспечения реализации указанной меры нами предлагается внести в ст. 10.6 Федерального закона об информации соответствующие изменения, которые обязывали бы владельцев социальных сетей обеспечить сбор и пере-

¹ О внесении изменений в Федеральный закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности: федеральный закон от 6 июля 2016 г. № 374-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

дачу информации с общедоступных страниц пользователей в автоматическом режиме путем установки соответствующего программного обеспечения¹.

Далее необходимо решить вопрос о том, какой государственный орган должен принимать поступающую информацию, а также обеспечивать разработку и поддержку предлагаемых нейросетевых моделей. Полагаем, что решение указанных задач возможно посредством полномочий, которыми Постановлением Правительства РФ от 16 марта 2009 г. № 228 наделен Роскомнадзор². Считаем, что именно Роскомнадзор является наиболее подходящей для решения указанной задачи службой ввиду имеющейся технической оснащенности, а также наличия квалифицированных кадров технического профиля. Как справедливо отмечают исследователи в области противодействия киберэкстремистским проявлениям, именно данная служба выступает одним из субъектов противодействия деструктивному влиянию сети Интернет³. Мнение о том, что среди приоритетных направлений деятельность именно государственных органов в сфере защиты информации необходимо усилить для повышения эффективности предупреждения киберэкстремистских преступлений, поддержало 34,4% опрошенных нами сотрудников ЦПЭ⁴.

В свою очередь, помимо непосредственной обработки результатов работы нейросетевых моделей, крайне важно обеспечить оперативную передачу информации о выявленных фактах распространения экстремистского контента соответствующим правоохранительным органам. Реализация данного взаимодействия должна осуществляться в порядке, установленном в соглашении о взаимодействии МВД России и Роскомнадзора от 23 августа 2017 г.⁵ Необходимо, чтобы пе-

¹ См. Приложение 6.

² О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций: Постановление Правительства РФ от 16 марта 2009 г. № 228. Доступ из справ.-правовой системы «КонсультантПлюс».

³ Сагайдак А. Ю., Турунова М. Н., Юзиханова Э. Г. Система противодействия преступности несовершеннолетних, обусловленной влиянием сети «Интернет» // Евразийский юридический журнал. 2024. № 5. С. 440.

⁴ См. Приложение 1.

⁵ Соглашение о взаимодействии Министерства внутренних дел Российской Федерации и Федеральной службы по надзору в сфере связи, информационных технологий и массовых ком-

редаваемая информация не только содержала бы результаты работы нейросетевых моделей, но и позволяла бы точно идентифицировать источник проверяемой информации. Это особенно важно, поскольку результаты работы нейросетевых моделей сами по себе не должны служить основанием для возбуждения уголовного дела. Каждый отдельный факт необходимо подвергать соответствующей проверке в установленном процессуальном порядке. Как нами уже отмечалось ранее, применение технологий ИИ без участия человека для решения юридических вопросов на данный момент затруднено в силу того, что нейросетевые модели иногда допускают ошибки, что в свою очередь совершенно недопустимо, когда речь идет о возможном уголовном преследовании человека.

Тем не менее применение ИИ для автоматизации процесса идентификации материалов экстремистского содержания в киберпространстве позволит существенно оптимизировать работу правоохранительных органов по поиску и анализу данных материалов в киберпространстве. Полагаем, что предлагаемая мера является наиболее эффективной для предупреждения неорганизованного уголовного киберэкстремизма. Однако считаем, что отдельные технические и организационные меры могут быть эффективны и для предупреждения организованной преступной деятельности экстремистской направленности, в частности, для прогнозирования подготовки к массовым беспорядкам или иным видам организационной деятельности для совершения преступлений экстремистской направленности в определенной области или среди определенных групп пользователей.

Как нами уже отмечалось ранее, зачастую подготовка к совершению вышеуказанных преступлений происходит в основном в сообществах и чатах социальных сетей и мессенджеров. В случае с подготовкой и координацией, например, массовых беспорядков для организаторов важно вовлечь в данную противоправную деятельность как можно большее количество людей. Для указанных целей, прежде всего, необходимо иметь сообщество или чат, состоящей из аудитории,

которую в короткие сроки можно организовать для совершения преступлений экстремистской направленности.

Сообщества или чаты, координируемые экстремистскими сообществами или организациями, условно можно охарактеризовать как «спящие ячейки». Как правило, до определенного момента организаторы не публикуют в них прямые призывы к совершению преступлений экстремистской направленности, ограничиваясь распространением деструктивного контента среди пользователей для поддержания активности аудитории. Однако в любой момент в таких сообществах или чатах можно быстро распространить призывы к совершению преступлений экстремистской направленности, как в случае с описанным нами ранее Telegram-каналом «Утро Дагестан». Крайне важно вовремя отследить такую «мобилизационную» активность, чтобы успеть предпринять необходимые предупредительные меры. Далее предложим механизм реализации программного обеспечения на примере прогнозирования массовых беспорядков, к которым призывают в сообществе или чате мессенджера Telegram.

Для решения поставленной задачи необходимо применять алгоритмы, которые позволяют отслеживать резкий всплеск количества сообщений, содержащих призывы к массовым беспорядкам. Общий алгоритм создания и работы необходимой нейросетевой модели будет схож с тем, который был нами предложен для идентификации экстремистских материалов. Он позволит определять те сообщения, которые содержат в себе призыв к массовым беспорядкам. Поскольку массовые беспорядки возможны только в определенном месте и времени, значит, соответствующие призывы также однозначно будут содержать такую информацию, отличая ее тем самым от любой другой. В связи с этим в качестве основных отличительных параметров для обучающей выборки текстов должны выступить сообщения, содержащие информацию о местах и времени сбора. Таким образом, полученная нейросеть сможет с наибольшей вероятностью правильно идентифицировать сообщения, содержащие призывы к беспорядкам. Далее необходимо лишь учитывать частоту данных сообщений, чтобы сделать правильный прогноз о подготовке к массовым беспорядкам.

В указанных целях необходимо обеспечить доступ предлагаемой нейросетевой модели к сообщениям или иным публикациям сообщества или чата. Однако здесь крайне затруднительно использовать описанную нами ранее технологию ботов, в силу того что бот может функционировать в сообществе или чате только если администратор сообщества предоставил ему необходимые права доступа (что крайне маловероятно, если речь идет об экстремистском сообществе или чате). В противном случае бот не будет иметь доступа к сообщениям или публикациям.

Общий алгоритм получения интересующей нас информации хорошо описал в своем исследовании М. А. Болвачев. Автор утверждает о необходимости использования «виртуальных агентов» (замаскированных профилей в социальных сетях, которые используются правоохранительными органами) для внедрения в закрытые экстремистские сообщества в социальных сетях¹. Полагаем, что такой подход является весьма эффективным для получения необходимой информации в закрытых экстремистских сообществах. Однако автором подразумевается ручное управление такими агентами, что снижает их эффективность, особенно при обработке большого объема данных. Считаем, что этот процесс нуждается в автоматизации (хотя бы частичной).

Для решения данной задачи целесообразно будет использовать возможности многих современных социальных сетей, которые позволяют получить автоматизированный доступ к пользовательскому аккаунту с использованием API (на примере Telegram). API (Application programming interface) – это интерфейс (набор сервисов и правил), позволяющий программам и компьютерам общаться друг с другом². Через API можно: получать сообщения из чатов, отправлять сообщения от имени пользователя, выполнять поиск по сообщениям, управлять списком контактов и т.д.³ При такой реализации для доступа к сообщениям в закрытом чате или сообществе не потребуются дополнительных разрешений со стороны админи-

¹ Болвачев М. А. Использование социальных сетей при расследовании преступлений экстремистской направленности: дис. ... канд. юрид. наук. Калининград, 2022. С. 86.

² Онлайн-руководство по наукометрии // Национальный исследовательский университет «Высшая школа экономики». URL: <https://sciguide.hse.ru/tech/api/> (дата обращения: 18.06.2024).

³ Telegram APIs // Telegram. URL: <https://core.telegram.org/api> (дата обращения: 15.02.2025).

стратора (в отличие от случая с добавлением бота). При вступлении в сообщество или чат в качестве «обычного» пользователя можно получить доступ ко всем содержащимся в них сообщениям, которые в автоматическом режиме можно передавать вышеуказанной нейросетевой модели.

Полагаем, что данная мера будет способствовать повышению эффективности предупреждения киберэкстремистских преступлений, подготавливаемых экстремистскими сообществами или организациями в закрытых сообществах социальных сетей и мессенджеров, за счет возможности автоматического выявления на ранних стадиях, что в свою очередь позволит правоохранительным органам своевременно принимать необходимые предупредительные меры.

Тем не менее в рамках настоящего исследования нерешенной остается проблема, связанная с необходимостью установления личностей лидеров и участников экстремистских сообществ и организаций, что, как нами уже отмечалось ранее, также крайне важно в контексте предупреждения киберэкстремизма. На сегодняшний день эффективное решение вышеуказанной задачи напрямую зависит от того, какие технологии и методы их использования применяются. Одним из наиболее перспективных и активно разрабатываемых в доктрине направлений сегодня является сбор, фильтрация и анализ данных, предоставляемых открытыми источниками в информационно-телекоммуникационном пространстве.

Под открытыми источниками понимается общедоступная информация, которая согласно ч. 4 ст. 7 Федерального закона об информации определяется как «информация, размещаемая ее обладателями в сети «Интернет» в формате, допускающем автоматизированную обработку без предварительных изменений человеком в целях повторного ее использования, является общедоступной информацией, размещаемой в форме открытых данных». В свою очередь совокупность методов по ее поиску, сбору и анализу охватывается термином OSINT (Open Source

Intelligence – от англ. «разведка на основе анализа открытых источников информации»)¹.

С учетом повсеместного использования ИТТ сегодня в открытом доступе хранится огромное количество информации, которая может быть использована для установления личности киберэкстремиста. Об эффективности применения OSINT в правоохранительной деятельности свидетельствуют результаты научных исследований. Например, В. Ю. Иванов справедливо утверждает о необходимости применения приемов и методов OSINT для получения криминалистически значимой информации². Аналогичную точку зрения высказывают также М. О. Янгаева и Н. О. Павленко³. В своем исследовании В. Б. Батоев прямо указывает на необходимость придания поиску по открытым источникам данных «статуса приоритетного направления совершенствования информационной основы решения задач ОРД наряду с традиционными формами и методами, и получения повсеместного внедрения и использования на всех уровнях организации ОРД»⁴.

Вместе с тем для эффективного поиска и анализа данной информации зачастую необходимо использовать комплекс специально разработанных для указанных целей программных средств. Несмотря на большое количество ведомственных научных исследований, нам не удалось найти сведений о данных комплексах, разработанных внутри ведомства и принадлежащих исключительно МВД России. Например, в работе А. А. Бессонова говорится о целесообразности использования программного комплекса «Охотник» (свидетельство о государственной регистрации программ для ЭВМ от 7 декабря 2021 г. № 2021680077) российского производителя ООО «Ти Хантер» для поиска оперативно значимой информации в соци-

¹ Качалов А. Г., Лантаев М. М. Подготовка специалистов по работе с открытыми данными в сети интернет (OSINT) в гражданских и ведомственных вузах // Юридическая наука: история и современность. 2021. № 9. С. 98-106.

² Иванов В. Ю. Использование OSINT в раскрытии и расследовании преступлений // Вестник Уральского юридического института МВД России. 2023. № 1. С. 66.

³ Янгаева М. О., Павленко Н. О. OSINT. Получение криминалистически значимой информации из сети Интернет // Алтайский юридический вестник. 2022. № 2. С. 135.

⁴ Батоев В. Б. О технологии поиска по открытым источникам «OSINT» в оперативно-розыскной деятельности // Вестник Уфимского юридического института МВД России. 2023. № 2. С. 69.

альных сетях и теневом сегменте Интернета – Даркнете (Dark Net). Однако данная разработка не принадлежит МВД России, а ее использование оперативными подразделениями осуществляется на контрактной основе.

На сегодняшний день практические сотрудники вынуждены использовать стороннее программное обеспечение, разработанное лицами или компаниями, не имеющими прямого отношения к отечественным государственным структурам. Согласно проведенному нами опросу сотрудников ЦПЭ для поиска экстремистского контента и лиц, его распространяющих, 62,5% опрошенных сегодня использовали Telegram-бот «Глаз Бога»; 28,1% – поисковую систему под названием «SEUSLab»; 6,2% – программное обеспечение для поиска и анализа информации в социальных сетях и мессенджерах Laplaces Demon. Необходимо отметить, что доступ к функционалу последних двух программных средств имеют сотрудники лишь в нескольких регионах Российской Федерации, поскольку данные ПО распространяются только на договорной основе за существенную плату; оставшиеся 3,2% опрошенных осуществляют малоэффективный ручной мониторинг киберпространства без использования специального программного обеспечения¹.

Полагаем, что сложившаяся ситуация препятствует эффективному предупреждению правоохранительными органами преступлений экстремистской направленности, совершаемых с использованием ИТТ. Использование стороннего программного обеспечения неизбежно сопряжено с рисками блокировки или ограничения функционала. Более того, нередко сотрудники вынуждены приобретать доступ к данным программам за счет личных денежных средств. Считаем, что данную проблему необходимо решать по двум направлениям: активизация разработки собственного программного обеспечения для осуществления OSINT; привлечение к содействию владельцев программного обеспечения, которое может быть использовано для осуществления OSINT.

Задачу по разработке собственного (внутриведомственного) программного обеспечения в первую очередь целесообразно решать путем улучшения взаимодействия ведомственных организаций системы высшего образования и террито-

¹ См. Приложение 1.

риальных органов на региональном уровне. Важно организовать работу по оперативному обмену опытом между исследователями из различных заведений. В указанных целях следует систематически организовать соответствующие научно-практические семинары и конференции. Важно привлекать к участию в них исследователей соответствующего профиля из гражданских учебных и научных заведений, сотрудников государственных и частных организаций, занимающихся разработкой программного обеспечения для решения задач в области информационной безопасности, а также представителей зарубежных стран для обмена международным опытом. В свою очередь непосредственная разработка необходимого ПО должна осуществляться преимущественно путем проведения заказных исследований, отражающих потребности практических сотрудников, занимающихся противодействием экстремизму¹.

В рамках проведенного нами исследования, основываясь на потребностях практических подразделений по противодействию киберпреступности, нами было разработано программное обеспечение, позволяющее осуществлять мониторинг выбранных пользователем чатов мессенджера Telegram на предмет появления в них сообщений, содержащих заранее определенные сотрудником ключевые слова. Данное ПО способно значительно снизить нагрузку на сотрудников по ручному мониторингу содержания чатов, проводя предварительную фильтрацию большого объема поступающей информации².

Кроме непосредственной разработки ПО, следует организовать работу по его оперативному внедрению в деятельность правоохранительных органов и своевременному обновлению. Важно обеспечить бесперебойный доступ к возможностям ПО для всех сотрудников, которым оно будет необходимо. В свою очередь интерфейс взаимодействия с программами должен быть понятен, удобен

¹ Ильиных Н. А. Ведомственное программное обеспечение анализа данных из открытых источников для предупреждения киберэкстремизма // Преемственность и новации в юридической науке : мат-лы междунар. науч. конф. адъюнктов, аспирантов и соискателей. Омск : Омская академия МВД России, 2025. Вып. 21. С. 63-65.

² См. Приложение 7.

и не вызывать затруднений при использовании лицами, не обладающими компетенциями в сфере ИТТ.

Как нами отмечалось выше, сегодня сотрудники подразделений, занимающихся противодействием экстремизму, в практической деятельности активно используют различное ПО сторонних разработчиков, которое позволяет эффективно осуществлять поиск по открытым источникам данных в киберпространстве. В науке существуют отдельные исследования, посвященные описанию таких программ и методов их применения правоохранительными органами. Например, в ходе комплексного исследования о способах получения значимой информации с использованием технологий OSINT Г. А. Рукавишников и П. М. Титов перечисляют ряд программ, которые целесообразно использовать в указанных целях. В их число вошли различные Telegram-боты, позволяющие осуществлять поиск: по номеру телефона абонента (@Usersbox), по фотографии (@FFace_bot; @FCfind_bot; @Poiskovichokbot), по адресу электронной почты (@SmartSearch_Bot), по номеру транспортного средства (@AVinfoBot, @AntiParkonBot, @avtocabot), по никнейму в Telegram (@TeleSINT)¹.

Вышеуказанный перечень не является исчерпывающим, существует множество других ботов с полезным функционалом. Например, можно отметить бот @Kto_ti_ai_search_bot, который позволяет по никнейму пользователя или по его ID Telegram предоставлять информацию о том, в каких чатах он может состоять и какие сообщения в них отправлял. Однако все указанные выше программные средства не имеют прямого отношения к правоохранительным органам, а доступ сотрудников к их функционалу осуществляться на общих со всеми остальными пользователями основаниях. При этом в подавляющем большинстве случаев данный функционал является платным, что препятствует его использованию для предупреждения преступлений.

¹ Рукавишников Г. А., Титов П. М. Общая характеристика технологий OSINT на платформе TELEGRAM для использования в получении значимой информации // Вопросы российской юстиции. 2023. № 27. С. 537-546.

Считаем, что необходимо организовать работу по привлечению к содействию разработчиков программного обеспечения, позволяющего осуществлять поиск по открытым источникам данных в киберпространстве и представляющего интерес для правоохранительных органов, занимающихся противодействием преступлениям экстремистской направленности, совершаемым с использованием ИТТ. Необходимый опыт по данному направлению у МВД уже имеется. О данном факте свидетельствует то, что большинство оперативных подразделений системы МВД имели бесплатный доступ к полному функционалу Telegram-бота «Глаз Бога», который позволял осуществлять поиск информации из открытых источников. В свою очередь разработчиком и владельцем данного программного обеспечения является частное лицо.

Таким образом, в рамках настоящего параграфа нами предложен следующий комплекс технических и организационно-тактических мер предупреждения преступлений экстремистской направленности, совершаемых с ИТТ:

1. Разработка и применение технологий искусственного интеллекта для автоматического выявления и идентификации экстремистских материалов, публикуемых на открытых страницах в социальных сетях и мессенджерах. Для реализации указанной меры и обеспечения постоянного мониторинга содержания открытых страниц пользователей нами предлагается внести в ст. 10.6 Федерального закона об информации соответствующие изменения, которые обязывали бы владельцев социальных сетей обеспечить сбор и передачу информации с общедоступных страниц пользователей в автоматическом режиме. Обязанность по принятию данной информации, а также по разработке необходимых нейросетевых моделей и предварительной обработке результатов их работы целесообразно возложить на Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор). В случае обнаружения материала, который нейросеть определила как экстремистский, необходимую информацию следует оперативно передавать соответствующим подразделениям правоохранительных органов, занимающимся противодействием экстремизму на региональном и районном уровнях, для последующей проверки и принятия решения о

возбуждении уголовного дела. Указанная мера способствует повышению эффективности выявления правоохранительными органами преступлений экстремистской направленности, совершаемых с использованием ИТТ.

2. В целях противодействия преступлениям, подготавливаемым и совершаемым экстремистскими организациями и сообществами, представляется целесообразным также использовать технологии искусственного интеллекта для прогнозирования подготовки к массовым беспорядкам или иным видам организационной деятельности для совершения преступлений экстремистской направленности в определенной области или среди определенных групп пользователей. Соответствующая нейросетевая модель способна определять содержание и частоту сообщений, отправляемых в сообществах и чатах социальных сетей или мессенджеров. Комплексный анализ данной информации позволит сделать прогноз подготовки к массовым беспорядкам или иным видам организационной деятельности, осуществляемой для совершения преступлений экстремистской направленности. В свою очередь, результаты таких прогнозов можно использовать для принятия правоохранительными органами своевременных мер по предупреждению преступлений экстремистской направленности.

3. В целях повышения эффективности выявления и установления личностей киберэкстремистов целесообразно использовать технологии и методы по сбору и анализу информации из открытых источников данных – OSINT. Практическими сотрудниками и различными исследователями отмечается перспективность использования методов OSINT для установления личности преступников в киберпространстве. Однако сегодня наиболее существенной проблемой, препятствующей использованию правоохранительными органами методов OSINT, является недостаток у подразделений МВД необходимого программного обеспечения, позволяющего автоматизировать поиск информации из открытых источников в киберпространстве. Сотрудники вынуждены использовать стороннее программное обеспечение за счет собственных денежных средств, к тому же такое ПО хотя и может быть полезно для установления личности преступника, однако чаще всего оно напрямую не предназначено для правоохранительной деятельности. Более то-

го, сложившаяся ситуация сопряжена с рисками блокировки или ограничения функционала стороннего ПО. Полагаем, что необходимо организовать работу по разработке собственного (внутриведомственного) ПО, позволяющего осуществлять автоматизированный поиск информации по открытым источникам данных в киберпространстве в целях установления личностей лидеров и участников экстремистских сообществ и организаций. Решение данной задачи должно осуществляться путем проведения заказных исследований, отражающих потребности практических сотрудников. Помимо разработки собственного ПО, необходимо проводить работу, направленную на привлечение к содействию разработчиков, владеющих ПО, которое может быть использовано в целях установления личностей лидеров и участников экстремистских сообществ и организаций в информационно-телекоммуникационном пространстве.

ЗАКЛЮЧЕНИЕ

Проведенное исследование криминологической характеристики и предупреждения преступлений экстремистской направленности, совершаемых с использованием ИТТ, показало, что с учетом повсеместного распространения новых технологий и продолжающейся тенденции к трансформации традиционных способов совершения преступлений определенная в работе проблема имеет существенное социальное и научное значение.

Итоги исследования. В целях дальнейшего совершенствования системы мер предупреждения преступлений экстремистской направленности, совершаемых с использованием ИТТ, и устранения неопределенности понятийного аппарата предлагается ввести определение «киберэкстремизм», под которым понимается социальное, относительно массовое явление, характеризующееся совокупностью запрещенных законом деяний, совершаемых по экстремистским мотивам, с обязательным использованием технологий, моделирующих информационно-телекоммуникационное пространство (киберпространство). В свою очередь в качестве предпосылки формирования экстремистских взглядов и убеждений следует рассматривать имплицитное деструктивное информационно-психологическое воздействие на личность в киберпространстве, под которым следует понимать не запрещенные действующим законодательством действия, зачастую не образующие состава какого-либо правонарушения по действующему законодательству.

При определении круга преступных деяний, которые характеризуют криминальный киберэкстремизм, нами были использованы перечни составов преступлений экстремистской направленности и преступлений, совершаемых с использованием (применением) ИТТ или в сфере компьютерной информации, которые содержатся в положениях Указания Генпрокуратуры России № 462/11, МВД России № 2 от 25 июня 2024 г. «О введении в действие перечней статей Уголовного кодекса Российской Федерации, используемых при формировании статистической отчетности». Учитывая специфику киберэкстремистских

преступлений, для целей криминологического исследования, а также для выработки наиболее эффективных теоретических положений по их предупреждению указанные деяния были разделены по направленности использования ИТТ для деятельности экстремистских сообществ и организаций на связанные и не связанные с деятельностью экстремистских сообществ и организаций.

В результате характеристики состояния рассматриваемых преступлений установлено, что более двух третей из них совершается с использованием ИТТ. В группе составов преступлений, не связанных с организацией деятельности экстремистских сообществ и организаций, доля зарегистрированных киберэкстремистских преступлений в среднем достигает 87,3%. Наиболее часто при совершении указанных деяний экстремисты используют возможности социальных сетей и мессенджеров.

Активно применяются ИТТ и для деятельности экстремистских сообществ и организаций. В среднем 23,12% данных преступлений имеют отметку об использовании ИТТ. Для связи между собой, а также для вербовки новых членов организаторы наиболее активно используют мессенджеры, для осуществления финансирования экстремистской деятельности – банковские онлайн-переводы и криптовалюту.

В структуре криминального киберэкстремизма преобладают преступления, совершаемые по политическим мотивам (около 44,9%). Около 26,1% киберэкстремистских деяний совершается по мотивам религиозной ненависти и вражды. По мотивам национальной ненависти и вражды, а также по идеологическим мотивам в среднем совершается 16,2% и 12,8% преступлений с использованием ИТТ соответственно.

В рамках исследования нами определены характеристики личности киберэкстремистов. Наиболее многочисленной группой являются киберэкстремисты, деяния которых не связаны с деятельностью экстремистских сообществ и организаций. Как правило, ими являются трудоспособные мужчины в возрасте от 30 до 49 лет со средним или средним профильным образованием, не имеющие по-

стоянного места работы либо трудящиеся в промышленном секторе. Рассматриваемые лица чаще всего действуют исключительно от своего имени, из своих личных побуждений, не упоминая какое-либо экстремистское сообщество или организацию. Общей для данной группы киберэкстремистов особенностью нравственно-психологической характеристики является их нежелание самостоятельно предпринимать активные преступные действия за пределами киберпространства. Вместо этого они стремятся побудить других лиц (преимущественно молодых людей в возрасте до 25 лет) к совершению преступлений экстремистской направленности в реальном мире.

Учитывая многочисленность группы киберэкстремистов, деяния которых не связаны с деятельностью экстремистских сообществ и организаций, целесообразно ее дополнительно разделить в зависимости от степени «открытости» действий данных лиц и их отношения к сохранению анонимности на 2 подгруппы: «неосмотрительные» и «осторожные». «Неосмотрительных» киберэкстремистов отличает их безразличное либо легкомысленное отношение к сохранению своей анонимности в киберпространстве. Данные лица, как правило, легко внушаемы, они обладают достаточно узким кругозором, а также склонны к импульсивным и необдуманным действиям. К подкатегории «осторожные» нами отнесены киберэкстремисты, которые в первую очередь обладают некоторыми знаниями по сокрытию своей личности в киберпространстве. По отношению к данным лицам негативные психологические особенности коммуникации в киберпространстве, такие как психологическая раскрепощенность, безответственность, а также стремление к ненормативному поведению, нередко служат катализатором для проявления их экстремистских воззрений. «Осторожные» киберэкстремисты могут вести «двойную» жизнь, выступая в киберпространстве в роли активиста, однако никак не проявляя своих экстремистских взглядов и убеждений уже в реальном мире.

Определяя криминологическую характеристику личности представителей организованного уголовного киберэкстремизма, необходимо учитывать тот факт, что сегодня такие лица нередко действуют в интересах отдельных зарубежных

стран. Как правило, ими являются образованные трудоспособные мужчины в возрасте 30–49 лет, которые часто имеют специальные знания по наиболее эффективному использованию возможностей современных ИТТ для сохранения своей анонимности, привлечению финансирования и эффективному деструктивному информационно-психологическому воздействию на пользователей.

Рассматривая комплекс детерминирующих факторов киберэкстремистской преступности, мы определили ряд объективных и субъективных предпосылок. В свою очередь объективные предпосылки целесообразно разделять на внешние (непосредственно связаны с участием представителей зарубежных стран) и внутренние (обусловленные процессами, протекающими без непосредственного участия в них представителей зарубежных государств).

К внешним объективным предпосылкам нами отнесено непосредственное участие представителей зарубежных государств в совершении киберэкстремистских преступлений, которое выражается: в организации массовых экстремистских акций посредством использования ИТТ; в фабрикации и вбросе в киберпространство недостоверных сведений экстремистского содержания; в поддержке крупных информационных площадок, на которых активно распространяются экстремистские материалы.

В качестве внутренней объективной предпосылки выступает имплицитное информационно-деструктивное воздействие на личность, которое выражается в формировании негативного отношения к какой-либо социальной группе, объединенной по политическим, религиозным, национальным или идеологическим признакам, путем распространения в киберпространстве сведений относительно совершения правонарушений с прямым указанием на представителя группы как виновного, а также в пропаганде деструктивных ценностей в фильмах, видеоиграх, книгах и т.д.

Внешней субъективной предпосылкой выступает восприятие значительной частью населения России идеологии либерализма как вседозволенности на фоне проводимых после распада СССР при активном участии недружественных стран реформ, совпавшее с началом широкого распространения в стране в 90-х гг. XX в.

информационно-телекоммуникационных технологий, в совокупности с недостаточным контролем за киберпространством со стороны правоохранительных органов. Все это способствовало формированию в российском обществе чувства безнаказанности за распространение экстремистских материалов при помощи ИТТ.

В качестве внутренних субъективных предпосылок совершения киберэкстремистских преступлений определены: высокая восприимчивость населения к экстремистским материалам, распространяемым в информационно-телекоммуникационном пространстве, и низкий уровень осведомленности граждан относительно форм проявления экстремизма и ответственности за совершение деяний экстремистской направленности.

В рамках настоящего исследования нами предлагается 2 основных направления по предупреждению преступлений экстремистской направленности, совершаемых с использованием ИТТ.

Первое направление – обеспечение информационно-психологической безопасности граждан. В указанных целях предлагается следующий комплекс мер, направленных преимущественно на устранение внутренних объективных и субъективных предпосылок:

1. Учитывая большую популярность среди населения формата получения новостной информации через социальные сети и мессенджеры, в целях предупреждения распространения экстремистской информации считаем необходимым законодательно урегулировать порядок администрирования данных новостных сообществ путем дополнения положений статьи 10.6 Федерального закона об информации частями 1.4 и 1.5, закрепив за владельцами новостных сообществ часть обязанностей, аналогичных тем, которые возложены сегодня на владельцев социальных сетей (п. 1–5 ч. 1 ст. 10.6).

2. Разработка и внедрение системы автоматизированной верификации новостной информации (САВНИ) в целях нивелирования негативного эффекта фейков. В основу работы САВНИ может быть положена технология искусственного интеллекта в области обработки естественного языка (NLP), которая будет выполнять задачу по анализу содержания проверяемой информации и сопоставлять

ее с данными, размещенными на официальных информационных порталах государственных органов и в СМИ.

3. Для предупреждения ИДИПВ на несовершеннолетних через пропаганду деструктивных ценностей в фильмах, видеоиграх, книгах и т.д. предлагается особое внимание уделять следующим перспективным направлениям обеспечения информационно-психологической безопасности личности:

а) мониторинг содержания информации, распространяемой популярными среди несовершеннолетних блогерами, путем привлечения к указанной деятельности общественных организаций, родительского сообщества и педагогических работников при координационной роли правоохранительных органов в целях своевременного выявления деструктивных идей;

б) увеличение в киберпространстве объема социально полезных материалов, пропагандирующих традиционные российские духовно-нравственные ценности и усиливающих их роль в воспитании у детей чувства неприязни к различным деструктивным идеям;

в) взаимодействие государства, педагогических работников и родительского сообщества по вопросам просветительской деятельности относительно новых деструктивных течений, появляющихся в киберпространстве.

4. В целях противодействия ИДИПВ как внутренней объективной предпосылке киберэкстремизма, выражающейся в распространении информации относительно совершения преступлений и (или) административных правонарушений с прямым указанием на принадлежность виновника к той или иной социальной группе, объединенной по политическим, религиозным, национальным или идеологическим признакам, предлагается внести изменения в действующую редакцию ст. 4 Закона о СМИ, закрепив соответствующий запрет и дополнив ее следующими словами: «...публично оправдывающих терроризм, других экстремистских материалов, *материалов, содержащих сведения относительно совершения правонарушений с прямым указанием на принадлежность лица, его совершившего, к той или иной социальной группе, объединенной по политическим, религиозным, национальным или идеологическим признакам...*». При этом важно обеспечить соблю-

дение указанных положений и администраторами новостных сообществ в социальных сетях и мессенджерах.

Второе направление предупреждения – внедрение комплекса технических и организационно-тактических мер, направленных на прогнозирование и своевременное пресечение готовящихся и на выявление уже совершенных киберэкстремистских преступлений, в том числе тех, в которых задействованы представители зарубежных стран (внешняя объективная предпосылка уголовного киберэкстремизма):

а) разработка и применение технологий ИИ для автоматического выявления и идентификации экстремистских материалов, публикуемых на открытых страницах в социальных сетях и мессенджерах. Для реализации указанной меры и обеспечения постоянного мониторинга содержания общедоступных страниц пользователей социальных сетей и мессенджеров нами предлагается внести в ст. 10.6 Федерального закона об информации соответствующие изменения, которые обязывали бы владельцев социальных сетей обеспечить сбор и передачу информации с общедоступных страниц пользователей в автоматическом режиме. Обязанность по принятию данной информации, а также по разработке необходимых нейросетевых моделей и предварительной обработке результатов их работы целесообразно возложить на Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций;

б) в целях противодействия преступлениям, подготавливаемым и совершаемым экстремистскими организациями и сообществами, также целесообразно использовать технологии ИИ для прогнозирования подготовки к массовым беспорядкам или иным видам организационной деятельности для совершения преступлений экстремистской направленности в определенной области или среди определенных групп пользователей. Соответствующая технология ИИ способна определять содержание и частоту сообщений, отправляемых в сообществах и чатах социальных сетей или мессенджеров. Комплексный анализ данной информации позволит сделать прогноз подготовки к массовым беспорядкам или иным видам организационной деятельности, осуществляемой для совершения преступлений

экстремистской направленности. Результаты данных прогнозов можно использовать для принятия правоохранительными органами своевременных мер по предупреждению преступлений экстремистской направленности;

в) в целях повышения эффективности выявления и установления личностей киберэкстремистов целесообразно использовать технологии и методы по сбору и анализу информации из открытых источников данных – OSINT. Практическими сотрудниками и исследователями отмечается перспективность использования методов OSINT для установления личности преступников в киберпространстве. Считаем целесообразным организовать работу по разработке собственного (внутриведомственного) ПО, позволяющего эффективно осуществлять поиск информации по открытым источникам данных в киберпространстве в целях установления личностей лидеров и участников экстремистских сообществ и организаций. Решение данной задачи должно осуществляться путем проведения заказных исследований, отражающих потребности практических сотрудников.

Сформулированные в диссертации предложения по предупреждению преступлений экстремистской направленности, совершаемых с использованием ИТТ, в будущем должны получить развитие. Перспективы исследований видятся в дальнейшем изучении детерминирующих факторов, а также в совершенствовании технических и организационно-тактических мер, с учетом стремительного развития научно-технического прогресса и последующей трансформации экстремистской преступности.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

Нормативные правовые акты и иные официальные документы

1. Конституция Российской Федерации: принята всенародным голосованием 12 декабря 1993 г. : с учетом поправок, внесенных Законом Российской Федерации о поправке к Конституции Российской Федерации от 14 марта 2020 г. № 1-ФКЗ. – Доступ из справ.-правовой системы «КонсультантПлюс».
2. Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ. – Доступ из справ.-правовой системы «КонсультантПлюс».
3. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ. – Доступ из справ.-правовой системы «КонсультантПлюс».
4. Закон Российской Федерации от 27 декабря 1991 г. № 2124-1 «О средствах массовой информации». – Доступ из справ.-правовой системы «КонсультантПлюс».
5. Федеральный закон от 25 июля 2002 г. № 114-ФЗ «О противодействии экстремистской деятельности». – Доступ из справ.-правовой системы «КонсультантПлюс».
6. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». – Доступ из справ.-правовой системы «КонсультантПлюс».
7. Федеральный закон от 6 июля 2016 г. № 374-ФЗ «О внесении изменений в Федеральный закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности». – Доступ из справ.-правовой системы «КонсультантПлюс».
8. Федеральный закон от 8 августа 2024 г. № 303-ФЗ «О внесении изменений в Федеральный закон «О связи» и отдельные законодательные акты Российской Федерации». – Доступ из справ.-правовой системы «КонсультантПлюс».

9. Указ Президента Российской Федерации от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации». – Доступ из справ.-правовой системы «КонсультантПлюс».

10. Указ Президента Российской Федерации от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы». – Доступ из справ.-правовой системы «КонсультантПлюс».

11. Указ Президента Российской Федерации от 9 ноября 2022 г. № 809 «Об утверждении Основ государственной политики по сохранению и укреплению традиционных российских духовно-нравственных ценностей». – Доступ из справ.-правовой системы «КонсультантПлюс».

12. Указ Президента Российской Федерации от 28 декабря 2024 г. № 1124 «Об утверждении Стратегии противодействия экстремизму в Российской Федерации до 2030 года». – Доступ из справ.-правовой системы «КонсультантПлюс».

13. Постановление Правительства Российской Федерации от 16 марта 2009 г. № 228 «О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций». – Доступ из справ.-правовой системы «КонсультантПлюс».

14. Распоряжение Президента Российской Федерации от 7 июня 2001 г. № 312-рп «О подписании Шанхайской конвенции о борьбе с сепаратизмом и экстремизмом». – Доступ из справ.-правовой системы «КонсультантПлюс».

15. Распоряжение Правительства Российской Федерации от 28 апреля 2023 г. № 1105-р «Об утверждении концепции информационной безопасности детей в Российской Федерации». – Доступ из справ.-правовой системы «КонсультантПлюс».

16. Постановление Пленума Верховного Суда Российской Федерации от 28 июня 2011 г. № 11 «О судебной практике по уголовным делам о преступлениях экстремистской направленности». – Доступ из справ.-правовой системы «КонсультантПлюс».

17. Указ Президиума Верховного Совета РСФСР от 11 сентября 1989 г. «О внесении изменений в Указ Президиума Верховного Совета РСФСР от 8 апре-

ля 1989 года «О внесении изменений и дополнений в Уголовный и Уголовно-процессуальный кодексы РСФСР и изложении его в новой редакции». – Доступ из справ.-правовой системы «КонсультантПлюс».

18. Шанхайская конвенция о борьбе с терроризмом, сепаратизмом и экстремизмом (заключена в г. Шанхае 15 июня 2001 г.). – Доступ из справ.-правовой системы «КонсультантПлюс».

19. Соглашение о взаимодействии Министерства внутренних дел Российской Федерации и Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций : утверждено МВД России, Роскомнадзором 23 августа 2017 г. – Доступ из справ.-правовой системы «КонсультантПлюс».

20. Программное обеспечение встроенных систем. Общие требования к разработке и документированию : государственный стандарт Российской Федерации ГОСТ Р 51904-2002 от 25 июня 2002 г. № 247-ст. – Доступ из справ.-правовой системы «КонсультантПлюс».

Научная и учебная литература

21. Авакьян, М. В. Методические рекомендации по профилактике распространения идеологии терроризма и экстремизма : учебное электронное издание / М. В. Авакьян, М. А. Болвачев, Т. С. Волчецкая, Е. В. Осипова. – Калининград : Балтийский федеральный университет им. И. Канта, 2023. – 44 с.

22. Антонян, Ю. М. Наука криминология : монография / Ю. М. Антонян. – Москва : Юрлитинформ, 2015. – 376 с.

23. Антонян, Ю. М. Личность корыстного преступника / Ю. М. Антонян, В. П. Голубев, Ю. Н. Кудряков. – Томск : Томский государственный университет, 1989. – 160 с.

24. Антонян, Ю. М. Причины преступности в России : монография / Ю. М. Антонян, Е. М. Тимошина ; под ред. Ю. М. Антоняна. – Москва, Санкт-Петербург : Нестор-История, 2013. – 348 с.

25. Антонян, Ю. М. Экстремизм и его причины : монография / Ю. М. Антонян, А. В. Ростокинский, Я. И. Гишинский [и др.] ; под ред. Ю. М. Антоняна. – Москва : Логос, 2020. – 312 с.

26. Верещагина, Л. А. Психология персонала. Потребности, мотивация и ценности / Л. А. Верещагина. – Харьков : Институт прикладной психологии «Гуманитарный Центр», 2012. – 212 с.
27. Винер Н. Кибернетика, или Управление и связь в животном и машине / пер. с англ. И. В. Соловьева и Г. Н. Поварова ; под ред. Г. Н. Поварова. – 2-е изд. – Москва : Наука, 1983. – 344 с.
28. Воронова, О. Е. Современные информационные войны: стратегии, типы, методы, приемы / О. Е. Воронова, А. С. Трушин. – Москва : Аспект Пресс, 2021. – 176 с.
29. Гишинский, Я. И. Криминология. Теория, история, эмпирическая база, социальный контроль. Курс лекций / Я. И. Гишинский. – Санкт-Петербург : Питер, 2002. – 384 с.
30. Клейменов, М. П. Криминология : учебник / М. П. Клейменов. – Москва : Норма, 2009. – 448 с.
31. Криминология : учебник / под общ. ред. А. И. Долговой. – 3-е изд., перераб. и доп. – Москва : Норма, 2008. – 912 с.
32. Кузнецова, Н. Ф. Проблемы криминологической детерминации / Н. Ф. Кузнецова. – Москва : МГУ, 1984. – 208 с.
33. Лозовицкая, Г. П. Проблема противодействия преступлениям экстремистского и террористического характера, совершаемого путем психотронного воздействия на личность : монография / Г. П. Лозовицкая. – Москва : Юрлитинформ, 2016. – 288 с.
34. Осипенко, А. Л. Сетевая компьютерная преступность. Теория и практика борьбы : монография / А. Л. Осипенко. – Омск : Омская академия МВД России, 2009. – 480 с.
35. Основные понятия в криминологии : словарь терминологический / сост. М. В. Гринь, М. А. Кондратов. – Краснодар : Кубанский государственный аграрный университет, 2017. – 30 с.

36. Петрянин, А. В. Концептуальные основы противодействия преступлениям экстремистской направленности: теоретико-прикладное исследование : монография / А. В. Петрянин. – Москва : Проспект, 2017. – 336 с.

37. Прокументов, Л. М. Криминология. Общая часть : учебник / Л. М. Прокументов, А. В. Шеслер. – Томск : ДиВо, 2007. – 230 с.

38. Рыдченко, К. Д. Государственная система противодействия обороту недостоверной информации и сведений экстремистского характера : монография / К. Д. Рыдченко. – Краснодар : Краснодарский университет МВД России, 2019. – 195 с.

39. Сидорова, Е. З. Уголовно-правовое противодействие финансированию экстремистской деятельности и терроризма : монография / Е. З. Сидорова. – Иркутск : Восточно-Сибирский институт МВД России, 2023. – 96 с.

40. Уголовный кодекс РСФСР : С постатейными материалами / колл. авторов. – Москва : Юридическая литература, 1987. – 464 с.

41. Ульянов, М. В. Миграционные процессы в системе детерминант экстремистской преступности : монография / М. В. Ульянов. – Москва : Юрлитинформ, 2019. – 176 с.

Научные статьи и публикации

42. 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. – № 2. – С. 121–126.

43. Акимова, Д. А. Современные каналы формирования и распространения идей экстремизма и терроризма в молодежной среде // 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. 98–105.

44. Аллахвердиева, Э. А. Понятие киберпреступности и киберпреступлений: теория и практика / Э. А. Аллахвердиева, А. В. Маслов // Общество. Закон. Правосудие. – 2021. – № 4. – С. 34–37.

45. Алхастов, А. М. Актуальные проблемы молодежного экстремизма: юридический анализ, современные способы противодействия / А. М. Алхастов // Юридическая наука. – 2022. – № 7. – С. 130–134.

46. Ананьев, А. В. Страна управляемого неонацизма / А. В. Ананьев, Е. В. Ананьева // Перспективы. – 2022. – № 2. – С. 26–48.

47. Андреев, Н. А. Криминологическая характеристика личности преступника, совершающего преступления экстремистской направленности в сети Интернет / Н. А. Андреев // Вестник Краснодарского университета МВД России. – 2023. – № 1. – С. 31–35.

48. Андронова, И. В. Финансирование терроризма: новые вызовы для международной безопасности / И. В. Андронова, Н. П. Гусаков, Е. Б. Завьялова // Вестник международных организаций: образование, наука, новая экономика. – 2020. – № 1. – С. 120–134.

49. Анисимова, И. А. Публичные призывы к осуществлению экстремистской и террористической деятельности как угроза безопасности / И. А. Анисимова, В. В. Ерахмилевич, Е. П. Веснина // Гуманитарные, социально-экономические и общественные науки. – 2023. – № 6. – С. 84–88.

50. Аносов, А. В. Специально-криминологическое предупреждение преступлений, совершаемых с использованием высоких технологий / А. В. Аносов // Труды Академии управления МВД России. – 2018. – № 4. – С. 93–97.

51. Арчаков, М. К. Русский религиозно-националистический радикализм в политическом процессе современной России / М. К. Арчаков // Социум и власть. – 2009. – № 1. – С. 59–63.

52. Бабурин, В. В. Криминологическая характеристика личности киберэкстремиста, деяния которого не связаны с организацией экстремистского сообщества или организации / В. В. Бабурин, Н. А. Ильиных // Психопедагогика в правоохранительных органах. – 2025. – Т. 30, № 2. – С. 234–240.

53. Батоев, В. Б. О технологии поиска по открытым источникам «OSINT» в оперативно-розыскной деятельности / В. Б. Батоев // Вестник Уфимского юридического института МВД России. – 2023. – № 2. – С. 66–71.

54. Баумтрог, В. Э. Прототип системы поиска и обнаружения экстремистских сообщений в социальной сети ВКонтакте / В. Э. Баумтрог, А. В. Еськов, Ю. А. Смирнов // Полицейская деятельность. – 2024. – № 5. – С. 98-109.

55. Березина, О. Б. Искусственный интеллект и противодействие экстремизму / О. Б. Березина // Актуальные вопросы образования. – 2023. – № 3. – С. 212–215.

56. Бессонов, А. А. Использование в раскрытии преступлений информации из открытых источников информации (OSINT) / А. А. Бессонов // Актуальные вопросы теории и практики оперативно-розыскной деятельности : сборник научных трудов Межведомственной научно-практической конференции. – Москва : Московский университет МВД России им. В. Я. Кикотя, 2022. – С. 40–45.

57. Бешукова, З. М. Участие в экстремистском сообществе: некоторые вопросы законодательного регулирования и правоприменения / З. М. Бешукова // Полицейская деятельность – 2016. – № 5. – С. 492–502.

58. Бирюков, В. В. В отношении изменений, внесенных в Федеральный закон № 114 «О противодействии экстремистской деятельности» / В. В. Бирюков // Военно-юридический журнал. – 2007. – № 12. – С. 20–26.

59. Боброва, О. В. Радикальные религиозные организации – угроза национальной безопасности и средств противодействия им / О. В. Боброва, В. В. Меркурьев // Обозреватель. – 2022. – № 9-10. – С. 106–127.

60. Богатырёв, А. Ю. Основные направления развития националистического движения в Российской Федерации с начала 90-х годов XX в. до настоящего времени / А. Ю. Богатырёв // Научный портал МВД России. – 2017. – № 3. – С. 102–109.

61. Ботвин, И. В. Роль современных технологий в предупреждении экстремизма в молодежной среде / И. В. Ботвин // Актуальные проблемы борьбы с преступлениями и иными правонарушениями. – 2023. – № 23-2. – С. 8–9.

62. Буров, И. В. Криминалистическая характеристика личности преступника экстремиста в Интернете / И. В. Буров // Вестник науки. – 2019. – № 1. – С. 57–60.

63. Бычков, В. В. Искусственный интеллект как средство противодействия преступлениям экстремистской направленности, совершаемым с использованием информационно-телекоммуникационных сетей, в том числе сети Интернет / В. В. Бычков, В. А. Прорвич // Вестник Академии Следственного комитета Российской Федерации. – 2020. – № 4. – С. 47–52.

64. Валуйцева, И. И. Разработка программы ASR для распознавания вариантов русского языка / И. И. Валуйцева, И. Е. Филатов // Полилингвильность и транскультурные практики. – 2021. – Т. 18, № 3. – С. 245–254.

65. Васильев, Н. А. Социальные сети. Формирование нового социального мира / Н.А. Васильев, С. Н. Комиссаров // Гуманитарий Юга России. – 2021. – № 4. – С. 43–60.

66. Вишневецкий, К. В. Влияние инновационных технологий на сферу предупреждения преступности / К. В. Вишневецкий // Уголовное законодательство: вчера, сегодня, завтра : материалы ежегодной всероссийской научно-практической конференции. – Санкт-Петербург : Санкт-Петербургский университет МВД России, 2021. – С. 67–74.

67. Волеводз, А. Г. Противодействие киберпреступности – тема первого тематического выпуска издания «Библиотека криминалиста. Научный журнал» № 4 (9)-2013 / А. Г. Волеводз // Библиотека криминалиста. – 2013. – № 5. – URL: <http://viperson.ru/wind.php?ID=666519&soch=1>.

68. Воронцовский, А. В. Цифровизация экономики и ее влияние на экономическое развитие и общественное благосостояние / А. В. Воронцовский // Вестник Санкт-Петербургского университета. Экономика. – 2020. – № 2. – С. 189–216.

69. Гладышев, В. В. Социальные сети как инструмент для пропаганды экстремизма / В. В. Гладышев // Национальный центр информационного противодействия терроризму и экстремизму в образовательной среде и сети Интернет. – URL: <http://nac.gov.ru/publikacii/stati-knigi-broshyury/gladyshev-v-socialnye-seti-kak-instrument-dlya.html>.

70. Давыдов, В. О. Экстремизм 2.0: криминалистически значимые аспекты организованного преступного формирования экстремистской направленности / В. О. Давыдов // Философия права. – 2023. – № 4. – С. 120–126.
71. Дуглас, Р. Яд для России / Р. Дуглас // Завтра. – 2010. – № 19. – С. 2. – URL: <https://zavtra.ru/blogs/2010-05-1221>.
72. Евтушенко, И. И. Мошенничества с цифровыми правами: вопросы квалификации / И. И. Евтушенко // Ученые записки Крымского федерального университета имени В. И. Вернадского. Юридические науки. – 2022. – № 1. – С. 131–140.
73. Елишев, С. О. Изучение понятий «Ценность», «Ценностные ориентации» в междисциплинарном аспекте / С. О. Елишев // Ценности и смыслы. – 2011. – № 2. – С. 82–96.
74. 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. – № 9. – С. 138–142.
75. Есаулова, К. С. К определению социальной смелости: в реальной жизни и интернет-коммуникации / К. С. Есаулова // Вестник РГГУ. Серия «Психология. Педагогика. Образование». – 2016. – № 2. – С. 53–56.
76. Засыпкина, Л. Р. Политические процессы в России конца XX века как объект социокультурного анализа / Л. Р. Засыпкина // Историческая и социально-образовательная мысль. – 2017. – Т. 9, № 3-1. – С. 50–55.
77. Иванов, А. К. Глобальное информационное пространство и его место в современном международном праве / А. К. Иванов // Ползуновский вестник. – 2005. – № 1. – С. 219–227.
78. Иванов, В. Ю. Использование OSINT в раскрытии и расследовании преступлений / В. Ю. Иванов // Вестник Уральского юридического института МВД России. – 2023. – № 1. – С. 62–66.
79. Иванько, А. Ф. Нейронные сети: общие технологические характеристики / А. Ф. Иванько, М. А. Иванько, Ю. А. Сизова // Научное обозрение. Технические науки. – 2019. – № 2. – С. 17–23.

80. Ильиных, Н. А. Ведомственное программное обеспечение анализа данных из открытых источников для предупреждения киберэкстремизма / Н. А. Ильиных // Преемственность и новации в юридической науке : материалы международной научной конференции адъюнктов, аспирантов и соискателей. – Омск : Омская академия МВД России, 2025. – Вып. 21. – С. 63–65.

81. Ильиных, Н. А. ИмPLICITное информационно-деструктивное воздействие как условие формирования экстремистских взглядов и убеждений / Н. А. Ильиных // Актуальные проблемы борьбы с преступностью: вопросы теории и практики : материалы XXVII международной научно-практической конференции : в 2 ч. – Ч. 2. – Красноярск : Сибирский юридический институт МВД России, 2024. – С. 19–22.

82. Ильиных, Н. А. Интернет как средство массовой манипуляции молодежью в экстремистских кругах / Н. А. Ильиных // Актуальные проблемы профилактики преступлений : материалы международного научно-практического семинара. – Омск : Омская академия МВД России, 2023. – С. 18–21.

83. Ильиных, Н. А. Использование информационных платформ и искусственного интеллекта в противодействии фейковым новостям как мера предупреждения киберэкстремизма / Н. А. Ильиных // Научный вестник Омской академии МВД России. – 2025. – Т. 31, № 1. – С. 37–43.

84. Ильиных, Н. А. Киберэкстремизм: понятие и разграничение с иным информационным деструктивным воздействием на человека в киберпространстве / Н. А. Ильиных // Известия Юго-Западного государственного университета. Серия: История и право. – 2023. – Т. 13, № 1. – С. 64–74.

85. Ильиных, Н. А. Новостные сообщества в социальных сетях и мессенджерах как источник распространения фейковой информации / Н. А. Ильиных // Актуальные проблемы профилактики преступлений : тезисы докладов и сообщений международного научно-практического семинара. – Омск : Омская академия МВД России, 2024. – С. 13–15.

86. Ильиных, Н. А. Отдельные аспекты характеристики личности лица, осуществляющего публичные призывы к экстремистской деятельности в

Интернете / Н. А. Ильиных // Актуальные проблемы борьбы с преступностью: вопросы теории и практики: материалы XXVI международной научно-практической конференции. – Красноярск: Сибирский юридический институт МВД России, 2023. – С. 134–136.

87. Ильиных, Н. А. Отдельные факторы распространения экстремизма среди детей в информационно-телекоммуникационном пространстве / Н. А. Ильиных // Правоохранительная деятельность органов внутренних дел в контексте современных научных исследований: материалы всероссийской научно-практической конференции адъюнктов, аспирантов и соискателей. – Санкт-Петербург: Санкт-Петербургский университет МВД России, 2022. – С. 230–232.

88. Ильиных, Н. А. Перспективы применения технологии нейронных сетей в профилактике киберэкстремизма / Н. А. Ильиных // Преемственность и новации в юридической науке: материалы международной научной конференции адъюнктов, аспирантов и соискателей. – Омск: Омская академия МВД России, 2023. – Вып. 19. – С. 47–49.

89. Ильиных, Н. А. Предпосылки киберэкстремистских преступлений и отдельные меры их предупреждения / Н. А. Ильиных // Вестник Дальневосточного юридического института МВД России имени И. Ф. Шилова. – 2025. – № 3. – С. 58–66.

90. Ильиных, Н. А. Роль информационно-телекоммуникационных технологий в совершении экстремистских преступлений в Российской Федерации, анализ судебной практики / Н. А. Ильиных // Мир Закона. – 2023. – № 1-2. – С. 32–39.

91. Ильиных, Н. А. Структура преступлений экстремистской направленности, совершаемых с использованием информационно-телекоммуникационных технологий / Н. А. Ильиных // Преемственность и новации в юридической науке: материалы международной научной конференции адъюнктов, аспирантов и соискателей. – Омск: Омская академия МВД России, 2024. – Вып. 20. – С. 52–54.

92. Ильиных, Н. А. Структура, уровень и динамика киберэкстремизма в Российской Федерации / Н. А. Ильиных // Вестник Сибирского юридического института МВД России. – 2023. – № 3. – С. 196–201.

93. Казбан, Е. П. Либерализм в ценностной системе российского общества / Е. П. Казбан, С. С. Степанова // PolitBook. – 2019. – № 1. – С. 181–193.

94. Качалов, А. Г. Подготовка специалистов по работе с открытыми данными в сети интернет (OSINT) в гражданских и ведомственных вузах / А. Г. Качалов, М. М. Лантаев // Юридическая наука: история и современность. – 2021. – № 9. – С. 98–106.

95. Кибальник, А. Г. Уголовная ответственность за публичное распространение фейков об использовании Вооруженных Сил РФ. Как применять новую статью УК / А. Г. Кибальник // Уголовный процесс. – 2022. – № 5. – С. 62–69.

96. Клишков, В. Б. Преступность и ее основные характеристики на современном этапе / В. Б. Клишков, В. В. Пасынков, Е. В. Стебенева // Вестник Санкт-Петербургского университета МВД России. – 2015. – № 4. – С. 158–164.

97. Кобец, П. Н. Киберпреступность: Современные виды, причины, ее порождающие, и особенности предупреждения / П. Н. Кобец // Вестник Самарского юридического института. – 2022. – № 1. – С. 52–58.

98. Козаев, Н. Ш. Особенности уголовной ответственности за публичное распространение заведомо ложной информации об использовании Вооруженных Сил Российской Федерации, исполнении государственными органами Российской Федерации своих полномочий (ст. 207.3 УК РФ) / Н. Ш. Козаев // Общество и право. – 2022. – № 2. – С. 48–51.

99. Коновалов, А. А. Киберпреступность как глобальная угроза экономической безопасности: виды, особенности, проблемы противодействия / А. А. Коновалов, С. А. Наумов, Д. Д. Колесникова // Ростовский научный журнал. – 2018. – № 1. – С. 20–27.

100. Коробеев, А. И. Кибервиктимология фейка: первичное досье / А. И. Коробеев, Д. В. Жмуров // Вестник Томского государственного университета. – 2021. – № 471. – С. 250–257.

101. 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 очно-заочной видеоконференции. – Барнаул : Алтайский государственный университет, 2020. – С. 11–12.

102. Лебедев, С. Я. Цифровой безопасности – цифровой уголовно-правовой ресурс / С. Я. Лебедев // Криминология: вчера, сегодня, завтра. – 2019. – № 4. – С. 17–25.

103. Леонтьева, Ю. В. Экстремизм в России: цифры и размышления / Ю. В. Леонтьева, О. А. Овчинко // Вестник Сибирского юридического института МВД России. – 2020. – № 3. – С. 133–140.

104. Лепский, В. Е. Информационно-психологическая безопасность субъектов дипломатической деятельности / В. Е. Лепский // Дипломатический ежегодник. 2002 : сборник статей. – Москва : Научная книга, 2003. – С. 233–248.

105. Лунеев, В. В. Российский экстремизм: политика и реалии / В. В. Лунеев // Всероссийский криминологический журнал. – 2009. – № 3. – С. 17–30.

106. Ляховенко, О. И. Телеграм-каналы в системе экспертной и политической коммуникации в современной России / О. И. Ляховенко // Galactica Media: Journal of Media Studies. – 2022. – № 1. – С. 114–144.

107. Маздогова, З. З. Предупреждение вовлечения молодежи в террористические и экстремистские организации / З. З. Маздогова // Проблемы экономики и юридической практики. – 2016. – № 5. – С. 227–229.

108. Макаров, Н. Е. Понятие и идеология экстремизма в современных условиях / Н. Е. Макаров, Ц. С. Дондоков // Закон и армия. – 2005. – № 11. – С. 56–57.

109. 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. – № 9. – С. 328–335.

110. Манойло, А. В. «Фейковые новости» как угроза национальной безопасности и инструмент информационного управления / А. В. Манойло // Вестник Московского университета. Серия 12. Политические науки. – 2019. – № 2. – С. 37–45.

111. Маркина, Ю. В. Мировые транснациональные медиакорпорации как сегмент глобализации информационной деятельности / Ю. В. Маркина // Вопросы журналистики, педагогики, языкознания. – 2018. – № 3. – С. 480–481.

112. Мельников, В. Ю. Преступления экстремистской направленности в Российской Федерации / В. Ю. Мельников // Журнал юридических исследований. – 2020. – Т. 5, № 2. – С. 14–22.

113. Меркушева, О. В. Современные процессы словообразования в аспекте когнитивной семантики / О. В. Меркушева, М. В. Попова // Известия ВГПУ. – 2021. – № 4. – С. 142–146.

114. Михалёв, Ю. А. «Исламское государство» в политике США / Ю. А. Михалёв // Вестник Московского государственного лингвистического университета. Общественные науки. – 2018. – № 2. – С. 92–99.

115. Могунова, М. М. Понятие современной киберпреступности и способы совершения финансово-ориентированных киберпреступлений / М. М. Могунова // Вестник ОмГУ. Серия Право. – 2022. – № 1. – С. 80–86.

116. Монахова, Л. Ю. Обучение противостоянию агрессивной коммуникации в киберпространстве / Л. Ю. Монахова // Человек и образование. – 2019. – № 58. – С. 42–46.

117. Морозов, И. Л. Государственная стратегия противодействия экстремизму в современной России / И. Л. Морозов, А. Э. Абрамов // Общество: политика, экономика, право. – 2020. – № 8. – С. 18–22.

118. Морозова, Ю. А. Цифровая трансформация российского здравоохранения как фактор развития отрасли / Ю. А. Морозова // Интеллект. Инновации. Инвестиции. – 2020. – № 2. – С. 36–47.

119. Мухтаров, Д. Д. Технологии вовлечения молодежи в экстремистскую деятельность: новые вызовы и пути противодействия / Д. Д. Мухтаров, Х. Л. Кушхов // Журнал прикладных исследований. – 2022. – № 3. – С. 72–74.

120. Немира, С. В. Искусственный интеллект в оценке достоверности заключения эксперта по уголовным делам. Постановка проблемы / С. В. Немира // Государственная служба и кадры. – 2023. – № 5. – С. 250–254.

121. Никульченкова, Е. В. Некоторые криминологические аспекты противодействия киберпреступлениям в России / Е. В. Никульченкова // Правоприменение в публичном и частном праве : материалы Международной научной конференции. – Омск : Омский государственный университет им. Ф. М. Достоевского, 2023. – С. 196–200.

122. Никульченкова, Е. В. Неопределенность терминологии и проблемы квалификации киберпреступлений (по материалам судебной практики) / Е. В. Никульченкова // Психопедагогика в правоохранительных органах. – 2024. – Т. 29, № 3. – С. 361–366.

123. Никульченкова, Е. В. О необходимости введения дефиниции «киберпреступление» в уголовный закон Российской Федерации / Е. В. Никульченкова // Вестник Омского университета. Серия: Право. – 2022. – Т. 19, № 3. – С. 98–107.

124. Никульченкова, Е. В. Причинностные факторы киберпреступности / Е. В. Никульченкова // Правоприменение в публичном и частном праве : материалы международной научной конференции. – Омск : Омский государственный университет им. Ф. М. Достоевского, 2024. – С. 119–123.

125. Номоконов, В. А. Киберпреступность как новая криминальная угроза / В. А. Номоконов, Т. Л. Тропина // Криминология: вчера, сегодня, завтра. – 2012. – № 24. – С. 45–56.

126. 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.

127. Петлин, М. А. Социально-философские аспекты киберпространства / М. А. Петлин // Вестник Омского университета. – 2014. – № 3. – С. 89–90.

128. Петров, А. И. Деятельность прокуратуры по правовому просвещению как средство профилактики правонарушений и преступлений / А. И. Петров // Oeconomia et Jus. – 2018. – № 3. – С. 48–62.

129. Пинкевич, Т. В. Современное состояние экстремизма и терроризма в условиях развития цифровых технологий / Т. В. Пинкевич, О. А. Заублова // Юрист-Правовед. – 2020. – № 3. – С. 64–68.

130. Пичугин, С. А. Организация экстремистского сообщества по российскому уголовному законодательству: нормативная регламентация и практика применения / С. А. Пичугин // Вестник Владимирского юридического института. – 2022. – № 4. – С. 85–92.

131. Пономарев, В. А. Информационный экстремизм и информационный терроризм в пространстве PR-технологий, СМИ и открытой информационной сети (Интернет): концептуальный аспект / В. А. Пономарев // Вопросы теории и практики журналистики. – 2018. – № 2. – С. 301–319.

132. Рассолов, И. М. Киберпространство и позитивное право / И. М. Рассолов // Политика и общество. – 2009. – № 2. – С. 33–37.

133. Рукавишникова, Г. А. Общая характеристика технологий OSINT на платформе TELEGRAM для использования в получении значимой информации / Г. А. Рукавишникова, П. М. Титов // Вопросы российской юстиции. – 2023. – № 27. – С. 537–546.

134. Сагайдак, А. Ю. Система противодействия преступности несовершеннолетних, обусловленной влиянием сети «Интернет» / А. Ю. Сагайдак, М. Н. Турунова, Э. Г. Юзиханова // Евразийский юридический журнал. – 2024. – № 5. – С. 438–440.

135. Сальников, Е. В. Экстремистские преступления: политико-правовой контекст / Е. В. Сальников, В. В. Соколов // Среднерусский вестник общественных наук. – 2019. – Т. 14, № 6. – С. 126–139.

136. Самурханов, М. С. Понятие и особенности киберпреступности / М. С. Самурханов // Международный журнал гуманитарных и естественных наук. – 2020. – № 4-3. – С. 219–221.

137. Сейдаметова, З. С. Системы рекомендаций в электронной коммерции / З. С. Сейдаметова // Ученые записки Крымского инженерно-педагогического университета. – 2018. – № 3. – С. 121–127.

138. Синцов Г. В. Экстремизм в Российской империи: причины зарождения / Г. В. Синцов, А. В. Первушкин // Вестник Пензенского государственного университета. – 2019. – № 1. – С. 25–29.

139. Смагулов, С. М. Цифровая трансформация здравоохранения / С. М. Смагулов, В. К. Смагулова // Инновации и инвестиции. – 2019. – № 2. – С. 290–291.

140. Сундиев, И. Ю. Технологии геймификации в экстремистской и террористической деятельности: опыт экспозиции / И. Ю. Сундиев, А. А. Смирнов // Научный портал МВД России. – 2021. – № 3. – С. 39–51.

141. Тамбиев, С. А. Криминологическая характеристика личности экстремиста / С. А. Тамбиев // Журнал прикладных исследований. – 2022. – № 2. – С. 56–60.

142. Тарасова, Н. В. Причинный комплекс преступности России периода реформ 90-х годов / Н. В. Тарасова // Вестник Брянского государственного университета. – 2008. – № 2. – С. 150–154.

143. 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.

144. Титова, О. И. Психолого-социальные факторы рисков вовлечения подростков в группы экстремистской направленности / О. И. Титова // Научный компонент. – 2019. – № 2. – С. 87–94.

145. Урбан, В. В. Преступления, совершаемые с использованием информационно-телекоммуникационных сетей: общая характеристика и уголовно-процессуальные меры по их противодействию / В. В. Урбан // Вестник Восточно-Сибирского института МВД России. – 2019. – № 1. – С. 55–63.

146. Хлебушкин, А. Г. Публичные призывы, направленные на нарушение территориальной целостности РФ (ст. 280.1 УК РФ): уголовно-правовая характеристика и вопросы квалификации / А. Г. Хлебушкин // Российский следователь. – 2014. – № 11. – С. 25–29.

147. Хмыз, А. И. Использование возможностей искусственного интеллекта в судебной экспертизе / А. И. Хмыз // Вестник экономической безопасности. – 2022. – № 5. – С. 224–227.

148. Худякова, Н. Л. Традиционные ценности как основа воспитания в современном быстроменяющемся обществе / Н. Л. Худякова // Вестник Челябинского государственного университета. – 2023. – № 4. – С. 91–99.

149. Цветова, Г. В. Цифровая экономика: преимущества, угрозы и факторы влияния / Г. В. Цветова // Власть и управление на Востоке России. – 2020. – № 2. – С. 45–50.

150. Цыбулька, А. М. Изменение ценностных основ в условиях глобальных вызовов человечеству / А. М. Цыбулька // Ученые записки Санкт-Петербургского имени В. Б. Бобкова филиала Российской таможенной академии. – 2022. – № 2. – С. 68–71.

151. Чимаров, С. Ю. Проблемный аспект ЧВК «Рёдан» и предметное поле правоохранительной деятельности ОВД России в формате молодежного дискурса / С. Ю. Чимаров // Международный журнал гуманитарных и естественных наук. – 2023. – № 3-3. – С. 97–99.

152. Чубриков, Е. Ю. Личность организованного преступника и детерминанты организованного преступного поведения / Е. Ю. Чубриков //

Развитие уголовно-исполнительной системы: организационные, правовые и экономические аспекты : сборник материалов международной научно-практической конференции в рамках международного юридического форума «Право и экономика: национальный опыт и стратегии развития». – Новосибирск, Новокузнецк : Новосибирский государственный университет экономики и управления ; Кузбасский институт ФСИН России, 2021. – С. 172–176.

153. Юзиханова, Э. Г. Криминологический анализ экстремизма в молодежной среде на современном этапе развития общества / Э. Г. Юзиханова, Н. А. Корсикова // Правопорядок: история, теория, практика. – 2024. – № 4. – С. 164–169.

154. Юзиханова, Э. Г. Организация профилактики правонарушений в сфере миграции / Э. Г. Юзиханова // Вестник Тюменского института повышения квалификации сотрудников МВД России. – 2021. – № 2. – С. 38–46.

155. Юзиханова, Э. Г. Содержание деятельности органов внутренних дел России по противодействию экстремизму в молодежной среде / Э. Г. Юзиханова, Н. А. Корсикова // Правопорядок: история, теория, практика. – 2025. – № 1. – С. 123–126.

156. Янгаева, М. О. OSINT. Получение криминалистически значимой информации из сети Интернет / М. О. Янгаева, Н. О. Павленко // Алтайский юридический вестник. – 2022. – № 2. – С. 131–135.

157. Aditya Jain, Gandhar Kulkarni, Vraj Shah: Natural Language Processing // International Journal of Computer Sciences and Engineering, Vol.6, Issue.1, pp.161-167 (2018).

Диссертации и авторефераты диссертаций

158. Ахметшин, А. С. Уголовно-правовое противодействие преступлениям с признаками экстремистской деятельности при обеспечении основ конституционного строя и безопасности государства : дис. ... канд. юрид. наук : 5.1.4 / Ахметшин Айрат Саатович. – Санкт-Петербург, 2025. – 387 с.

159. Баранов, В. В. Правовые и организационные основы деятельности органов внутренних дел по противодействию проявлениям экстремизма в

глобальной компьютерной сети : дис. ... канд. юрид. наук : 12.00.11 / Баранов Владимир Владимирович. – Москва, 2021. – 290 с.

160. Болвачев, М. А. Использование социальных сетей при расследовании преступлений экстремистской направленности : дис. ... канд. юрид. наук : 12.00.12 / Болвачев Михаил Александрович. – Калининград, 2022. – 206 с.

161. Борисов, С. В. Преступления экстремистской направленности: проблемы законодательства и правоприменения : дис. ... д-ра юрид. наук : 12.00.08 / Борисов Сергей Викторович. – Москва, 2012. – 484 с.

162. Глущенко, П. А. Криминологические основы противодействия финансированию экстремистской и террористической деятельности : дис. ... канд. юрид. наук : 5.1.4 / Глущенко Полина Андреевна. – Краснодар, 2025. – 204 с.

163. Грачев, Г. В. Информационно-психологическая безопасность личности: теория и технология психологической защиты : автореф. дис. ... д-ра психол. наук : 19.00.12 / Грачев Георгий Васильевич. – Москва, 2000. – 56 с.

164. Жукова, О. С. Правовые меры противодействия информационному экстремизму : автореф. дис. ... канд. юрид. наук : 05.13.19 / Жукова Ольга Степановна. – Воронеж, 2006. – 23 с.

165. Клейменов, И. М. «Сравнительная криминология: криминализация, преступность, уголовная политика в условиях глобализации : автореф. дис. ... д-ра юрид. наук : 12.00.08 / Клейменов Иван Михайлович. – Омск, 2015. – 40 с.

166. Кочергин, Р. О. Противодействие молодежному экстремизму: правовые и криминологические проблемы : дис. ... канд. юрид. наук : 12.00.08 / Кочергин Руслан Олегович. – Ростов-на-Дону, 2008. – 233 с.

167. Криштопов, С. В. Уголовно-правовое противодействие преступлениям экстремистской направленности : автореф. дис. ... д-ра юрид. наук : 12.00.08 / Криштопов Сергей Владимирович. – Москва, 2022. – 25 с.

168. Льянов, М. М. Криминалистическое значение электронно-цифровых следов преступлений экстремистской и террористической направленности в сети «Интернет» : дис. ... канд. юрид. наук : 5.1.4 / Льянов Муса Микаилович. – Екатеринбург, 2025. – 248 с.

169. Магнутов, Ю. С. Уголовно-правовое противодействие специальным организованным формам экстремистской деятельности (ст. 282.1 и ст. 282.2 УК РФ): теория, техника, практика : дис. ... канд. юрид. наук : 5.1.4 / Магнутов Юрий Сергеевич. – Нижний Новгород, 2022. – 384 с.

170. Простосердов, М. А. Экономические преступления, совершаемые в киберпространстве, и меры противодействия им : дис. ... канд. юрид. наук : 12.00.08 / Простосердов Михаил Александрович. – Москва, 2016. – 232 с.

171. Пучков, Д. В. Уголовно-правовая модель защиты телекоммуникаций от преступных посягательств: проблемы теории и практики : дис. ... д-ра юрид. наук : 12.00.08 / Пучков Денис Валентинович. – Екатеринбург, 2022. – 474 с.

172. Ростокинский, А. В. Преступления экстремистской направленности как проявления субкультурных конфликтов молодежных объединений: уголовно-правовые и криминологические проблемы : дис. ... д-ра юрид. наук : 12.00.08 / Ростокинский Александр Владимирович. – Москва, 2011. – 447 с.

173. Рыдченко, К. Д. Административно-правовое обеспечение информационно-психологической безопасности органами внутренних дел Российской Федерации : автореф. дис. ... канд. юрид. наук : 12.00.14 / Рыдченко Кирилл Дмитриевич. – Воронеж, 2011. – 27 с.

174. Сергун, Е. П. Экстремизм в российском уголовном праве: автореф. дис. ... канд. юрид. наук : 12.00.08 / Сергун Евгений Петрович. – Тамбов, 2009. – 25 с.

175. Сироткина, Т. Г. Криминологическая характеристика и предупреждение экстремистской преступности несовершеннолетних : автореф. дис. ... канд. юрид. наук : 5.1.4 / Сироткина Татьяна Геннадьевна. – Москва, 2024. – 29 с.

176. Скудин, А. С. Правовые меры противодействия экстремизму: дис. ... канд. юрид. наук : 12.00.08 / Скудин Андрей Сергеевич. – Москва, 2011. – 216 с.

177. Тамаев, Р. С. Организация правоохранительной деятельности в сфере противодействия экстремизму : автореф. дис. ... д-ра юрид. наук : 12.00.11 / Тамаев Руслан Сугаипович. – Москва, 2010. – 55 с.

178. Тропина, Т. Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы : автореф. дис. ... канд. юрид. наук : 12.00.08 / Тропина Татьяна Львовна. – Владивосток, 2005. – 28 с.

179. Узденов, Р. М. Экстремизм: криминологические и уголовно-правовые проблемы противодействия : автореф. дис. ... канд. юрид. наук : 12.00.08 / Узденов Расул Магометович. – Москва, 2008. – 29 с.

180. Узембаева, Г. И. Преступления экстремистской направленности, совершаемые с использованием средств массовой информации либо информационно-телекоммуникационных сетей : автореф. дис. ... канд. юрид. наук : 12.00.08 / Узембаева Гульфия Ишбулдовна. – Москва, 2016. – 24 с.

181. Упорников, Р. В. Политико-правовые технологии противодействия информационному экстремизму в России : автореф. дис.... канд. юрид. наук : 23.00.02 / Упорников Роман Владимирович. – Ростов-на-Дону, 2007. – 26 с.

182. Фридинский, С. Н. Противодействие экстремистской деятельности (экстремизму) в России (социально-правовое и криминологическое исследование) : автореф. дис. ... д-ра юрид. наук : 12.00.08 / Фридинский Сергей Николаевич. – Москва, 2011. – 37 с.

183. Чекунов, И. Г. Криминологическое и уголовно-правовое обеспечение предупреждения киберпреступности : автореф. дис. ... канд. юрид. наук : 12.00.08 / Чекунов Игорь Геннадьевич. – Москва, 2013. – 22 с.

Материалы судебной практики

184. Приговор Волжского районного суда г. Саратова Саратовской области от 25 августа 2021 г. по делу № 1-202/2021. – Доступ из справ.-правовой системы «ГАРАНТ».

185. Приговор Красноярского краевого суда от 14 октября 2022 г. по делу № 2-40/2022. – Доступ из справ.-правовой системы «ГАРАНТ».

186. Приговор Кумторкалинского районного суда Республики Дагестан от 15 августа 2023 г. по делу № 1-102/2023. – Доступ из справ.-правовой системы «ГАРАНТ».

187. Приговор Ленинского районного суда г. Кемерово Кемеровской области от 16 ноября 2020 г. по делу № 1-265/2020. – Доступ из справ.-правовой системы «ГАРАНТ».

188. Приговор Ленинского районного суда г. Махачкалы Республики Дагестан от 22 ноября 2021 г. по делу № 1-717/2021. – Доступ из справ.-правовой системы «ГАРАНТ».

189. Приговор Ленинского районного суда г. Ростова-на-Дону Ростовской области от 25 января 2021 г. по делу № 1-41/2021. – Доступ из справ.-правовой системы «ГАРАНТ».

190. Приговор Миасского городского суда Челябинской области от 19 мая 2023 г. по делу № 1-278/2023. – Доступ из справ.-правовой системы «ГАРАНТ».

191. Приговор Новочебоксарского городского суда Чувашской Республики – Чувашии от 21 сентября 2020 г. по делу № 1-136/2020. – Доступ из справ.-правовой системы «ГАРАНТ».

192. Приговор Сармановского районного суда Республики Татарстан от 28 июня 2023 г. по делу № 1-46/2023. – Доступ из справ.-правовой системы «ГАРАНТ».

193. Приговор Свердловского районного суда г. Иркутска Иркутской области от 22 мая 2023 г. по делу № 1-597/2023. – Доступ из справ.-правовой системы «ГАРАНТ».

194. Приговор Сулейман-Стальского районного суда Республики Дагестан от 14 ноября 2022 г. по делу № 1-87/2022. – Доступ из справ.-правовой системы «ГАРАНТ».

195. Приговор Сюзунского районного суда Удмуртской Республики от 5 мая 2021 г. по делу № 1-56/2021. – Доступ из справ.-правовой системы «ГАРАНТ».

196. Решение Верховного суда Российской Федерации от 2 августа 2022 г. № АКПИ 22-411С. – Доступ из справ.-правовой системы «ГАРАНТ».

197. Решение Верховного Суда Российской Федерации от 16 марта 2023 г. № АКПИ23-101С. – Доступ из справ.-правовой системы «ГАРАНТ».

198. Решение Верховного Суда Российской Федерации от 17 ноября 2014 г. № АКПИ14-1292С. – Доступ из справ.-правовой системы «ГАРАНТ».

199. Решение Верховного Суда Российской Федерации от 29 декабря 2014 г. № АКПИ 14-1424С. – Доступ из справ.-правовой системы «ГАРАНТ».

200. Решение Верховного Суда Российской Федерации от 17 августа 2020 г. по делу № АКПИ20-514с. – Доступ из справ.-правовой системы «ГАРАНТ».

201. Решение Московского городского суда от 9 июня 2021 г. № 3а-1573/2021. – Доступ из справ.-правовой системы «ГАРАНТ».

202. Решение Останкинского районного суда г. Москвы от 30 ноября 2020 г. по делу № 2а-556/2020. – Доступ из справ.-правовой системы «ГАРАНТ».

203. Решение Тверского районного суда г. Москвы от 21 марта 2022 г. № 02-2473/2022. – Доступ из справ.-правовой системы «ГАРАНТ».

Электронные источники информации

204. «Обстрел» Мариуполя Вооруженными Силами России оказался фейком. – URL: <https://iz.ru/1296705/2022-02-25/obstrel-mariupolia-vooruzhennymi-silami-rossii-okazalsia-feikom>.

205. Telegram APIs // Telegram. – URL: <https://core.telegram.org/api>.

206. Telegram начнет платить владельцам каналов за рекламу // РБК. – URL: https://www.rbc.ru/technology_and_media/28/02/2024/65df2cf39a794735d2013709.

207. Аудитория интернета в 2022 году // Mediascope. URL: https://mediascope.net/upload/iblock/3d8/qrlhud7t7dxyzw1rhtzxcg3rwk8deg7uk/2022_%D0%98%D0%9D%D0%A2%D0%95%D0%A0%D0%9D%D0%95%D0%A2.pdf.

208. Беспорядки в Махачкале организованы через социальные сети // Известия. – URL: <https://iz.ru/1597736/alena-nefedova/ne-dobivaias-rezultatov-na-pole-boia-khotiat-raskolot-nas-iznutri>.

209. Блогера Хасбика за антисемитизм и призывы к беспорядкам проверит Генпрокуратура // РБК. – URL: <https://lenta.ru/news/2023/10/31/blogera-hasbika-za-antisemitizm-i-prizyvvy-k-besporiyadkam-proverit-genprokuratura/>.

210. Более 22 тысяч молодежных организаций работает в России // Парламентская газета. Общество. – URL: <https://www.pnp.ru/social/bole-22-tysyach-molodezhnykh-organizaciy-rabotaet-v-rossii.html>.

211. Власти ХМАО создадут нейросеть для написания законов // Ведомости. Страна. – URL: <https://www.vedomosti.ru/strana/ural/news/2024/03/05/1023817-vlasti-hmao-sozdadut>.

212. Дуров пригрозил блокировать телеграм-каналы за фейки о ситуации на Украине // Интерфакс. – URL: <https://www.interfax.ru/russia/824977>.

213. Итоги выборочного федерального статистического наблюдения по вопросам использования населением информационных технологий и информационно-телекоммуникационных сетей // Федеральная служба государственной статистики. – URL: https://rosstat.gov.ru/free_doc/new_site/business/it/ikt22/index.html.

214. Кадыров раскритиковал СМИ и Симоньян за освещение драки в Новой Москве // РБК. – URL: <https://www.rbc.ru/politics/06/11/2021/6186ac0b9a7947b2c2e4ea59>.

215. Как устроена аудитория социальных медиа // Mediascope. – URL: <https://mediascope.net/news/2544317>.

216. Каталог Telegram-каналов и чатов Новости и СМИ // Сервис аналитики Telegram-каналов и чатов «TGStat». – URL: <https://tgstat.ru/news>.

217. Лучшие фильмы 1990-х годов // Кинопоиск. – URL: <https://www.kinopoisk.ru/lists/movies/year--1990-1999>.

218. Министерство внутренних дел Российской Федерации. Состояние преступности в Российской Федерации. – URL: <https://xn--b1aew.xnp1ai/reports/item/28021552>.

219. МО РФ заявило о нарастании количества фейков по ситуации на Украине. – URL: <https://iz.ru/1297404/2022-02-26/mo-rf-zaiavilo-o-narastanii-kolichestva-feikov-po-situacii-naukraine>.

220. Молодежный контент. Требования к проекту. // АНО «Институт развития интернета». – URL: <https://xn--h1aax.xn--p1ai/contests/molodezhnyy-kontent-10-24>.

221. Молодежная субкультура ЧВК «Редан» захлестнула Россию: что это такое и зачем подростки снимают на видео драки в ТЦ // Комсомольская правда. – URL: <https://www.kp.ru/daily/27470/4726359>.

222. О внесении изменения в статью 4 Федерального закона «О средствах массовой информации» // Система обеспечения законодательной деятельности. – URL: <https://sozd.duma.gov.ru/bill/21931-8>.

223. Онлайн-руководство по наукометрии // Национальный исследовательский университет «Высшая школа экономики». – URL: <https://sciguide.hse.ru/tech/api>.

224. Подробнее про программу AT35 – автомобиль за 35% от стоимости // Finiko. – URL: <https://www.youtube.com/watch?v=ZtonloYiVEw>.

225. Профилактика экстремизма в молодежной среде и противодействие вовлечению молодежи в деструктивные организации : методическое пособие. – Казань, 2019. – URL: https://minmol.tatarstan.ru/rus/file/pub/pub_2415831.pdf.

226. Путин назвал беспорядки в Махачкале событием, а не тенденцией // РБК. – URL: <https://www.rbc.ru/rbcfreenews/6544f1519a794794e21391bd>.

227. Путин назвал западные страны «империей лжи» после введения новых санкций // РБК. – URL: <https://www.rbc.ru/politics/28/02/2022/621cbe6b9a794770558ada7f>.

228. Путин В.В. Доклад на заседании коллегии Федеральной службы безопасности по подведению основных итогов оперативно-служебной деятельности органов ФСБ России за 2014 г. (Москва, 26 марта 2015 г.). – URL: <http://www.kremlin.ru/events/president/transcripts/deliberations/49006>.

229. Социальные сети и мессенджеры: вовлеченность и предпочтения // ВЦИОМ. – URL: <https://wciom.ru/analytical-reviews/analiticheskii-obzor/socialnye-seti-i-messendzhery-vovlechennost-i-predpochtenija>.

230. Суд приговорил экс-главу штаба Навального в Томске к девяти годам // РБК. – URL: <https://www.rbc.ru/politics/29/12/2023/658e914d9a7947516efa674c>.

231. Суд признал Meta экстремистской организацией и запретил в России Facebook и Instagram // Российская газета. – URL: <https://rg.ru/2022/03/21/reg-cfo/sud-zapretil-v-rossii-instagram-i-facebook-za-ekstremistskuiu-deiatelnost.html>.

232. Уильям Гибсон. О возникновении «киберпространства». – URL: https://cyberpunkworld.net/news/uiljam_gibson_o_vozniknovenii_kiberprostranstva/2011-06-25-126.

Приложения

Приложение 1.

Результаты анкетирования сотрудников Центра по противодействию экстремизму УМВД России по Омской области

Общее количество респондентов – 32 человека

<i>№</i>	<i>Вопрос</i>	<i>Ответ</i>
1	Является ли, на Ваш взгляд, использование информационно-телекоммуникационных технологий (соцсети, мессенджеры, веб-сайты и т.д.) приоритетным для экстремистов способом совершения преступлений экстремистской направленности в Российской Федерации?	1. Да – 81,25%. 2. Нет – 18,75%. 3. Затрудняюсь ответить – 0%.
2	Считаете ли Вы использование информационно-телекоммуникационных технологий более общественно опасным способом совершения преступлений экстремистской направленности по сравнению с другими (например, печатная или устная агитация)?	1. Да – 62,5%. 2. Нет – 31,3%. 3. Затрудняюсь ответить – 6,2%.
3	При помощи каких информационно-телекоммуникационных технологий чаще всего совершаются преступления экстремистской направленности?	1. Социальные сети (ВКонтакте, Одноклассники, Twitter, Instagram и т.д.) – 50%. 2. Мессенджеры (Телеграм, WhatsApp, Viber и т.д.) – 42,3%. 3. Отдельные веб-сайты в интернете – 3,8%. 4. Сотовая мобильная связь – 3,8%.
4	По каким мотивам наиболее часто совершаются преступления экстремистской направленности с использованием информационно-телекоммуникационных технологий?	1. Политический (например, призывы к насилию в отношении представителей власти) – 37,5%. 2. Религиозный (например, пропаганда деятельности запрещенной в Российской Федерации религиозной организации и вербовка новых участников) – 25%. 3. Националистический (например, призывы к насилию в отноше-

		нии группы людей, объединенных по признаку национальной принадлежности) – 28,2%. 4. Идеологический (например, реабилитация нацизма) – 9,3%.
5	Что, на Ваш взгляд, в большей степени способствует совершению киберпреступлений экстремистской направленности?	1. Условная анонимность – 42,8%. 2. Опосредованное общение между пользователями – 9,5%. 3. Возможность осуществлять экстремистскую деятельность из любого места – 47,6%. 4. Затрудняюсь ответить – 0%.
6	Как Вы оцениваете роль представителей недружественных стран в координации экстремистской деятельности (финансирование, подготовка и т.д.)?	1. Оказывают значительное влияние, и с началом СВО их влияние возросло – 68,75%. 2. Оказывают значительное влияние, но с началом СВО их влияние не возросло – 18,75%. 3. Оказывают незначительное влияние – 12,5%. 4. Затрудняюсь ответить – 0%.
7	Большинство преступлений экстремистской направленности с использованием информационно-телекоммуникационных технологий совершаются:	1. Специально обученными лицами, действующими строго в соответствии с инструкциями организаторов экстремистских сообществ – 25%. 2. Членами экстремистских организаций, совершающих преступления сугубо из личной приверженности идеям организации, однако без специальной подготовки и инструкций со стороны организаторов сообщества – 18,75%. 3. Лицами, не относящими себя к экстремистской организации, действующими без инструкций и сугубо из своих личных побуждений – 56,25%.
8	Как бы Вы оценили уровень критического отношения населения к недостоверным сведениям, публикуемым из неофициальных источников (фейков)?	1. Большинство населения легко внушаемо, граждане информацию не перепроверяют – 62,5%. 2. Большинство населения скорее легко внушаемо, чем нет, граждане изредка перепроверяют информацию – 25%.

		3. Большинство населения скорее не внушаемо, граждане чаще всего перепроверяют информацию – 12,5%. 4. Большинство населения не внушаемо, граждане всегда перепроверяют информацию – 0%.
9	На Ваш взгляд, направление деятельности каких органов, организаций, подразделений следует усилить в целях повышения эффективности предупреждения экстремизма?	1. Подразделения ОВД (ПДН, УУП, УБК) – 6,2%. 2. Государственные органы в сфере защиты информации (например, Роскомнадзор) – 34,4%. 3. Школы – 25%. 4. Вузы, ССУЗы – 28,2%. 5. Проф. комитеты в админ. округах районах – 6,2%.
10	Считаете ли Вы эффективной мерой предупреждения экстремизма, пропагандистскую деятельность в интернете, направленную на формирование у населения критического отношения к публикуемой в интернете информации?	1. Да – 56,25% 2. Скорее да, чем нет – 25% 3. Скорее нет, чем да – 18,75% 4. Нет – 0%
11	Каким программным обеспечением Вы пользуетесь для поиска экстремистских материалов и экстремистов в интернете?	1. Laplaces Demon (Демон Лапласа) – 6,2%. 2. SEUSLab – 28,1%. 3. Телеграм-бот «Глаз Бога» и т.п. – 62,5%. 4. Личный мониторинг – 3,2%.
12	Существует ли необходимость разработки методических рекомендаций по использованию специальных технических инструментов для выявления экстремистских материалов и установления личности экстремиста в интернете?	1. Да – 75%. 2. Нет – 25%. 3. Затрудняюсь ответить – 0%.
13	Присутствует ли на данный момент проблема недостатка времени, сил и средств на выявление и обработку содержащихся в интернете проявлений экстремизма?	1. Да, в интернете содержится много потенциально экстремистской информации, не всегда есть возможность ее полностью отработать – 87,5%. 2. Нет, имеющихся времени сил и средств вполне достаточно для об-

		работки всех фактов проявления экстремизма в интернете – 12,5%. 3. Затрудняюсь ответить – 0%.
14	Повысит ли эффективность Вашей деятельности созданная на основе искусственного интеллекта программа, обеспечивающая автоматизацию поиска и анализа информации в интернете на предмет экстремизма?	1. Да, существенно – 56,35%. 2. Да, частично – 31,25%. 3. Скорее нет – 12,5%. 4. Нет – 0%. 5. Затрудняюсь ответить – 0%.

**Результаты анкетирования сотрудников полиции, проходящих службу
в подразделениях: участковых-уполномоченных полиции; по делам
несовершеннолетних; следствия и др. МВД России по Омской, Новосибирской,
Тюменской, Кемеровской, Томской областям, Красноярскому и Алтайскому
краям, Ямало-Ненецкому и Ханты-Мансийскому автономным округам**

Общее количество респондентов – 134 человека

<i>№</i>	<i>Вопрос</i>	<i>Ответ</i>
1	Является ли, на Ваш взгляд, использование информационно-телекоммуникационных технологий (соцсети, мессенджеры, веб-сайты и т.д.) приоритетным для экстремистов способом совершения преступлений экстремистской направленности в Российской Федерации?	1. Да – 91,1%. 2. Нет – 5,2%. 3. Затрудняюсь ответить – 3,7%.
2	Считаете ли Вы использование информационно-телекоммуникационных технологий более общественно опасным способом совершения преступлений экстремистской направленности по сравнению с другими (например, печатная или устная агитация)?	1. Да – 82,2%. 2. Нет – 13,4%. 3. Затрудняюсь ответить – 4,4%.
3	На Ваш взгляд, большинство киберпреступлений совершается при помощи:	1. Социальных сетей, мессенджеров, отдельных сайтов, находящихся в юрисдикции зарубежных стран (Instagram, Twitter, Facebook, Telegram и т.д.) – 79,9%. 2. Отечественных социальных сетей, мессенджеров, отдельных веб-сайтов (ВКонтакте, Одноклассники и т.д.) – 20,1%.
4	Лица какого возраста чаще всего совершают преступления экстремистской направленности с использованием информационно-телекоммуникационных технологий?	1. Несовершеннолетние (до 17 лет включительно) – 11,2%. 2. 18-25 лет – 49,2%. 3. 25-35 лет – 35,1%. 4. Старше 35 лет – 4,5%.
5	На какую возрастную категорию	1. Несовершеннолетние (до 17 лет

	лиц чаще всего направлено деструктивное воздействие (кого вовлекают в экстремистскую деятельность)?	включительно) – 35,8%. 2. 18-25 лет – 52,9%. 3. 25-35 лет – 8,9%. 4. Старше 35 лет – 2,4%.
6	Как бы Вы оценили уровень осведомленности граждан относительно того, какие деяния по законодательству Российской Федерации квалифицируются как преступления экстремистской направленности?	1. Высокая осведомленность, (большинство граждан хорошо осведомлено о существующих составах преступлений экстремистской направленности) – 13,4%. 2. Низкая осведомленность (большинство граждан не знает, какие деяния по действующему законодательству признаются экстремистскими преступлениями) – 86,6%. 3. Затрудняюсь ответить – 0%.
7	Оцените степень деструктивного психологического воздействия фейковой информации на общественное спокойствие.	1. Оказывает сильное воздействие – 14,9%. 2. Оказывает значительное воздействие – 61,9%. 3. Оказывает незначительное воздействие – 18,6%. 4. Не оказывает воздействие – 4,6%.

Приложение 3.

**Программа контент-анализа публикаций в новостных сообществах
мессенджеров и социальных сетей в целях выявления уровня
восприимчивости пользователей к недостоверной информации и иному
информационно-деструктивному воздействию**

Периодизация рассмотренных материалов: 01.01.2022 – 01.01.2024 гг.

Критерием для выбора анализируемых новостных сообществ послужило наличие в них не менее 50 тыс. пользователей.

Основные направления исследования:

1. Анализ новостных публикаций в социальных сетях и мессенджерах относительно совершения преступлений и (или) административных правонарушений с прямым указанием на принадлежность виновника к той или иной социальной группе, объединенной по политическим, религиозным, национальным или идеологическим признакам.

<i>№ п/п</i>	<i>Единицы анализа</i>	<i>Индикаторы оценки</i>	<i>Всего</i>	<i>Процентное соотношение</i>
1	Количество рассмотренных мессенджеров и социальных сетей	Мессенджер Telegram Социальные сети: ВКонтакте	1 1	
2	Количество проанализированных новостных сообществ		10	
3	Количество проанализированных публикаций		40	
4	Комментарии пользователей к публикациям	Комментарии к публикациям, содержащие негативные высказывания в адрес всей группы, объединенной по политическим, религиозным, национальным или идеологическим признакам, представителем кото-		

	рой является лицо, указанное в публикации как виновник	349	34,9%
	Комментарии к публикациям, содержащие негативные высказывания непосредственно в отношении лица, указанного в публикации как виновник, безотносительно его политической, религиозной, национальной или религиозной принадлежности	422	42,2%
	Иные комментарии к публикациям	229	22,9%

2. Анализ комментариев и реакций¹ пользователей социальных сетей и мессенджеров к новостным публикациям, содержащим недостоверные сведения (фейковые новости).

<i>№ п/п</i>	<i>Единицы анализа</i>	<i>Индикаторы оценки</i>	<i>Всего</i>	<i>Процентное соотношение</i>
1	Количество рассмотренных мессенджеров и социальных сетей	Мессенджеры: Telegram, WhatsApp Социальные сети: ВКонтакте, Одноклассники, Instagram	2 3	
2	Количество проанализированных новостных сообществ		15	

¹ Под реакциями понимаются условные обозначения, располагающиеся непосредственно под публикацией, при помощи которых пользователи могут оценить контент.

3	Количество проанализированных публикаций		30	
4	Реакции пользователей на публикации	Реакции к публикациям, подтверждающие восприятие пользователями информации как достоверной Реакции к публикациям, подтверждающие восприятие пользователями информации как недостоверной	42300 11700	78,3% 21,7%
5	Комментарии пользователей к публикациям	Комментарии к публикациям, подтверждающие восприятие пользователями информации как достоверной Комментарии к публикациям, подтверждающие восприятие пользователями информации как недостоверной Иные комментарии к публикациям	535 262 203	53,5% 26,2% 20,3%

Результаты анкетирования совершеннолетних жителей Омской области

Общее количество респондентов – 853 человека

<i>№</i>	<i>Вопрос</i>	<i>Ответ</i>
1	Есть ли в Конституции Российской Федерации нормы, регламентирующие запрет экстремистских проявлений?	1. Да – 39,7%. 2. Нет – 27,6%. 3. Затрудняюсь ответить – 32,7%.
2	Существует ли специализированный федеральный закон Российской Федерации, определяющий сущность экстремизма?	1. Да – 64,3%. 2. Нет – 11,4%. 3. Затрудняюсь ответить – 24,3%.
3	Какие действия признаются экстремизмом?	1. Публичное оправдание терроризма – 21,8%. 2. Реабилитация нацизма – 28,2%. 3. Клевета – 17,9%. 4. Затрудняюсь ответить – 32,1%.
4	Уголовная ответственность за публичные призывы к экстремизму в Интернете в соответствии с УК РФ:	1. Штраф до 100 000 рублей – 26,7%. 2. Лишение свободы до 10 лет – 16,8%. 3. Лишение свободы до 5 лет – 36,3%. 4. Затрудняюсь ответить – 20,2%.
5	Знаете ли Вы официальные интернет-ресурсы, куда можно отправить информацию о факте размещения в сети Интернет экстремистского материала?	1. Да – 62,8%. 2. Нет – 37,2%.
6	Какими источниками Вы пользуетесь для получения информации об актуальных новостях?	1. Телевидение – 23,9%. 2. Печатные издания – 2,3%. 3. Веб-сайты и мобильные приложения официальных СМИ – 31,2%. 4. Новостные сообщества в социальных сетях и мессенджерах (в том числе неофициальных СМИ) – 42,6%.
7	Оцените, как часто Вы встречаетесь с фейковой (недоверенной) информацией в размещении в мессенджерах, социальных сетях, веб-сайтах?	1. 1 раз в неделю – 35,3%. 2. 1 раз в месяц – 37,6%. 3. За все время встретил 1 раз – 20,1%. 4. Ни разу не встречал(а) – 7%

8	Оцените степень деструктивного психологического воздействия фейковой информации на общественное спокойствие по 10-балльной шкале.	1. 1 балл – 12,4%. 2. 2 балла – 3,1%. 3. 3 балла – 7,2%. 4. 4 балла – 1,7%. 5. 5 баллов – 1,2%. 6. 6 баллов – 4,6%. 7. 7 баллов – 9,8%. 8. 8 баллов – 9,6%. 9. 9 баллов – 20,9%. 10. 10 баллов – 29,5%.
9	Как часто Вы перепроверяете информацию, опубликованную в мессенджерах, социальных сетях, вэб-сайтах в иных источниках?	1. Перепроверяю каждую новость – 13,6%. 2. Перепроверяю только интересные меня новости – 46,9%. 3. Отношусь к перепроверке безразлично – 29,8%. 4. Никогда не перепроверяю – 9,7%.
10	Как часто люди из Вашего близкого окружения перепроверяют информацию, опубликованную в мессенджерах, социальных сетях, вэб-сайтах в иных источниках?	1. Перепроверяют каждую новость – 12,3%. 2. Перепроверяют только интересные меня новости – 26,9%. 3. Относятся к перепроверке безразлично – 37,8%. 4. Никогда не перепроверяют – 9,7%. 5. Затрудняюсь ответить – 13,3%.

**Результаты анкетирования педагогических работников
в сфере школьного образования**

Общее количество респондентов – 53 человека

№	Вопрос	Ответ
1	Считаете ли Вы, что сегодня дети большую часть свободного времени проводят за просмотром различного контента в Интернете?	1. Да – 94,4%. 2. Нет – 5,6%.
2	Как Вы оцениваете степень осведомленности родителей о том, какой контент сегодня популярен среди детей?	1. Высоко (большинство родителей осведомлены) – 3,8%. 2. Средне (около половины родителей осведомлены) – 18,8%. 3. Низко (лишь малая часть родителей осведомлена) – 77,4%.
3	Как вы оцениваете степень осведомленности педагогических работников о том, какой контент сегодня популярен среди детей?	1. Высоко (большинство педработников осведомлены) – 24,6%. 2. Средне (около половины педработников осведомлены) – 64,1%. 3. Низко (лишь малая часть педработников осведомлена) – 11,3%.
4	Какой, на Ваш взгляд, вид контента сегодня наиболее популярен среди детей?	1. Образовательный – 5,7%. 2. Развлекательный – 88,7%. 3. Иное – 5,6%.
5	Считаете ли Вы справедливым утверждение о том, что сегодня популярный среди детей контент зачастую имеет мало общего с формированием социально одобряемых ценностно-моральных ориентиров, а скорее нередко носит деструктивный характер?	1. Да – 84,9%. 2. Нет – 15,1%.
6	Считаете ли Вы целесообразным осуществлять государственную поддержку информационной продукции для детей, способствующей формированию у них социально одобряемых ценностно-моральных ориентиров?	1. Да – 98,1%. 2. Нет – 1,9%.

Проект Федерального закона «О внесении изменений в Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и Закон РФ от 27 декабря 1991 г. № 2124-1 «О средствах массовой информации»

Внести в Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» следующие изменения:

Дополнить статью 10.6 частями 1.4 и 1.5 следующего содержания:

«1.4. В случае, если объем аудитории персональной страницы составляет более десяти тысяч пользователей социальной сети и на ней систематически распространяется общественно значимая информация, указанная в подпункте «з» пункта 5 части 1 настоящей статьи, то создавший такую страницу пользователь социальной сети обязан соблюдать требования, указанные в пунктах 1–5 части 1 настоящей статьи, положения которых применяются в отношении такой страницы и ее владельца. Владелец персональной страницы, объем аудитории которой составляет более десяти тысяч пользователей социальной сети и на которой систематически распространяется общественно значимая информация, кроме предоставления сведений в перечень персональных страниц, указанный в части 1.2 настоящей статьи, также обязан указать о том, что на его странице систематически распространяется общественно значимая информация. На основании данных сведений формируется перечень персональных страниц, на которых систематически распространяется общественно значимая информация.

1.5. Порядок формирования и ведения перечня персональных страниц, на которых систематически распространяется общественно значимая информация, определяется федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи.».

Пункт 10 части 1 статьи 10.6 после слов «для определения количества пользователей информационным ресурсом в сети «Интернет» дополнить словами:

«предназначенных для автоматического мониторинга и передачи общедоступной информации».

Внести в Закон РФ от 27 декабря 1991 г. № 2124-1 «О средствах массовой информации» следующие изменения:

1) пункт 1 статьи 4 после слов «публично оправдывающих терроризм, других экстремистских материалов,» *дополнить словами:* «материалов, содержащих сведения относительно совершения правонарушения с прямым указанием на принадлежность лица, его совершившего, к той или иной социальной группе, объединенной по политическим, религиозным, национальным или идеологическим признакам».

Свидетельство о регистрации программы для ЭВМ
«Система автоматизированного мониторинга и извлечения данных
из сервисов обмена мгновенными сообщениями»,
регистрационный номер 2024688641

РОССИЙСКАЯ ФЕДЕРАЦИЯ



СВИДЕТЕЛЬСТВО
о государственной регистрации программы для ЭВМ
№ 2024688641

**Система автоматизированного мониторинга и
извлечения данных из сервисов обмена мгновенными
сообщениями**

Правообладатель: *Федеральное государственное казенное
образовательное учреждение высшего образования «Омская
академия Министерства внутренних дел Российской
Федерации» (RU)*

Авторы: *Ильиных Никита Андреевич (RU), Ревягин Александр
Валерьевич (RU), Бабурин Василий Васильевич (RU),
Нечепуренко Алексей Алексеевич (RU), Дорош Егор Юрьевич
(RU), Бойко Ольга Альбертовна (RU)*

Заявка № **2024687716**
Дата поступления **14 ноября 2024 г.**
Дата государственной регистрации
в Реестре программ для ЭВМ **29 ноября 2024 г.**

Руководитель Федеральной службы
по интеллектуальной собственности

Ю.С. Зубов

