



Министерство внутренних дел Российской Федерации
Омская академия

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

*Автореферат
диссертации на соискание ученой степени
кандидата юридических наук*

Омск 2025

Работа выполнена в федеральном государственном казенном образовательном учреждении высшего образования «Омская ордена Почета академия Министерства внутренних дел Российской Федерации».

Научный руководитель:

Бабурин Василий Васильевич, Заслуженный работник высшей школы Российской Федерации, доктор юридических наук, профессор, профессор кафедры криминологии и профилактики преступлений федерального государственного казенного образовательного учреждения высшего образования «Омская ордена Почета академия Министерства внутренних дел Российской Федерации»

Официальные оппоненты:

Юзиханова Эльвира Гумеровна, доктор юридических наук, профессор, начальник кафедры криминологии федерального государственного казенного образовательного учреждения высшего образования «Санкт-Петербургский университет Министерства внутренних дел Российской Федерации»;

Никульченкова Елена Владимировна, кандидат юридических наук, доцент, доцент кафедры уголовного права и криминологии федерального государственного автономного образовательного учреждения высшего образования «Омский государственный университет им. Ф. М. Достоевского»

Ведущая организация:

федеральное государственное казенное образовательное учреждение высшего образования «Барнаульский юридический институт Министерства внутренних дел Российской Федерации»

Защита состоится 11 декабря 2025 г. в 13:00 часов на заседании диссертационного совета 03.2.010.01, созданного на базе федерального государственного казенного образовательного учреждения высшего образования «Омская ордена Почета академия Министерства внутренних дел Российской Федерации» по адресу: 644092, г. Омск, пр-т Комарова, д. 7, зал заседаний ученого совета.

С диссертацией можно ознакомиться в библиотеке и на сайте федерального государственного казенного образовательного учреждения высшего образования «Омская ордена Почета академия Министерства внутренних дел Российской Федерации» (<http://www.omamvd.ru/diss/>).

Автореферат разослан «___» октября 2025 г.

**Ученый секретарь
диссертационного совета
кандидат юридических наук,
доцент**



Ларин Евгений Геннадьевич

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

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 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 реаль-

¹ Министерство внутренних дел Российской Федерации. Состояние преступности в Российской Федерации. URL: <https://xn--b1aew.xnp1ai/reports/item/28021552> (дата обращения: 19.04.2025).

ную 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 стабильности².

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 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 способ-

² 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».

ствует 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. Дави-тадзе, 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. Ростокинский («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. Хлеб-бушкин («Преступный экстремизм: понятие, виды, проблемы криминализации и пенализации», 2007), Р. О. Кочергин («Противодействие молодежному экстремизму: правовые и криминологические проблемы», 2008), Р. М. Узде-нов («Экстремизм: криминологические и уголовно-правовые проблемы противодействия», 2008), Е. П. Сергун («Экстремизм в российском уголовном праве», 2009), А. С. Скудин («Правовые меры противодействия экс-

тремизму», 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 деструк-

тивному 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 постоянно-

го 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, принимающие 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 свя-

занные 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 вбро-се 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 информа-

ции 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 Судебного 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-телекоммуникационных 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.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **введении** излагается актуальность избранной темы, дается оценка степени ее научной разработанности, определяются объект, предмет, цель и задачи исследования, его теоретическая основа, формулируется научная новизна, раскрываются теоретическая и практическая значимость работы, описываются методология и методы исследования, приводятся положения, выносимые на защиту, и сведения о степени достоверности и апробации результатов полученного исследования, а также структуре и объеме работы.

Первая глава «Понятие и криминологическая характеристика преступлений экстремистской направленности, совершаемых с использованием информационно-телекоммуникационных технологий» состоит из трех параграфов.

В *первом параграфе* «Понятие и сущность киберэкстремизма в современной России» указывается, что массовое использование ИТТ для совершения экстремистских проявлений формирует особенности детерминации и механизма деструктивного воздействия на личность. Данный факт, в свою очередь, обуславливает необходимость в комплексном криминологическом исследовании такого явления, как киберэкстремизм.

Отсутствие среди исследователей единообразного подхода по данному вопросу препятствует выработке соответствующих последовательных и системных мер предупреждения. Определяя существенные признаки киберэкстремизма, автор, помимо прочего, отмечает, что данное явление включает исключительно противоправные деяния. Такой вывод следует из анализа содержащихся в законодательстве признаков самого экстремизма. Таким образом, предлагается разграничивать киберэкстремизм и имплицитное деструктивное информационно-психологическое воздействие на человека в киберпространстве (ИДИПВ).

В контексте 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 деструктивно-информационно-психологического воздействия сам по себе не является

экстремизмом, поскольку указанные действия не запрещены действующим законодательством. Дифференциация понятий «киберэкстремизм» и «ИДИПВ» позволит устранить имеющуюся на данный момент неопределенность в понимании сущности экстремистских проявлений, совершаемых с использованием ИТТ, соответствующих факторов, причин и условий, а также способствует выработке эффективной системы предупреждения рассматриваемых явлений.

Таким образом, под киберэкстремизмом диссертант предлагает понимать социальное, относительно массовое явление, проявляющееся в совокупности запрещенных законом деяний, совершаемых по экстремистским мотивам, с обязательным использованием ИТТ, моделирующих киберпространство.

На основе содержания перечней статей Уголовного кодекса Российской Федерации, используемых при формировании статистической отчетности, определен круг киберэкстремистских преступлений. Учитывая их специфику, для выработки наиболее эффективных теоретических положений по предупреждению указанные деяния разделены 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.

Второй параграф «Состояние киберэкстремистской преступности. Структура и тенденции преступлений экстремистской направленности, совершаемых с использованием информационно-телекоммуникационных технологий» содержит анализ качественных и количественных показателей неорганизованной и организованной киберэкстремистской преступности.

На основе анализа статистических данных установлено, что около двух третей всех преступлений экстремистской направленности совершается с использованием ИТТ.

В группе преступлений, не связанных с организацией деятельности экстремистских сообществ и организаций, доля зарегистрированных киберэкстремистских деяний в среднем достигает 87,3%. В результате изучения судебной практики установлено, что наиболее часто при совершении указанных деяний использовались возможности социальных сетей и мессенджеров.

Несколько реже, однако тоже активно используются ИТТ и для организации деятельности экстремистских сообществ и организаций. В среднем 18,7% всех таких зарегистрированных преступлений имеют соответствующую отметку. Автором отмечаются трудности при выявлении указанных

фактов ввиду преимущественного непубличного характера организаторской деятельности и достаточно высокого уровня владения навыками по использованию организаторами ИТТ для сохранения своей анонимности. Вместе с тем на основе анализа имеющейся судебной практики установлено, что для связи между собой, а также для вербовки новых членов организаторы наиболее активно используют мессенджеры, для осуществления финансирования своей деятельности — банковские онлайн-переводы и криптовалюту.

В структуре криминального киберэкстремизма преобладают деяния, совершаемые по политическим мотивам (около 44,9%). Свыше четверти преступлений совершается по мотивам религиозной ненависти и вражды. По идеологическим мотивам, а также по мотивам национальной ненависти и вражды в среднем совершается 12,8% и 16,2% преступлений соответственно.

Отдельно диссертант отмечает усиливающуюся в последнее время роль недостоверной информации в деструктивном информационно-психологическом воздействии на население. Большинство опрошенных практических сотрудников органов внутренних дел (76,8%) отмечают рост количества фактов ее распространения и ее значительное негативное воздействие на общественный порядок. Результаты социологического опроса граждан свидетельствуют о большом количестве недостоверных сведений, распространяемых в киберпространстве. Свыше 72,9% респондентов отметили, что встречаются с такой информацией не реже 1 раза в месяц.

В *третьем параграфе* «Криминологическая характеристика личностей киберэкстремистов и их влияние на формирование экстремистских воззрений у населения» определена характеристика личностей киберэкстремистов, а также оценено их влияние на формирование экстремистских взглядов и убеждений у населения.

Киберэкстремистами, деяния которых напрямую не связаны с деятельностью экстремистских сообществ и организаций, как правило, являются трудоспособные мужчины в возрасте от 30 до 49 лет со средним профессиональным образованием, не имеющие постоянного места работы либо трудящиеся в промышленном секторе. 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 и стремление побуждать других лиц (преимущественно молодых людей в возрасте до 25 лет)

к совершению преступлений экстремистской направленности в реальном мире.

Учитывая многочисленность рассматриваемой группы, автором предложено дополнительно разделить ее в зависимости от степени «открытости» действий и отношения данных лиц к сохранению своей анонимности на 2 подгруппы: «неосмотрительные» и «осторожные».

«Неосмотрительных» киберэкстремистов отличает их безразличное либо легкомысленное отношение к сохранению своей анонимности в киберпространстве. Уровень влияния данных лиц на формирование экстремистских воззрений у населения оценивается как низкий, поскольку их противоправная деятельность весьма непродолжительна, не спланирована и не систематична.

К подкатегории «осторожных» отнесены киберэкстремисты, которые обладают отдельными знаниями и умениями по сокрытию своей личности при помощи ИТТ. В свою очередь такие негативные психологические особенности коммуникации в киберпространстве, как психологическая раскрепощенность, безответственность, а также стремление к ненормативному поведению, нередко служат для данных лиц катализатором проявления своих экстремистских воззрений. Рассматриваемые киберэкстремисты могут вести «двойную» жизнь, выступая в киберпространстве в роли активиста, однако никак не проявляя своих взглядов и убеждений уже в реальном мире. За счет возможности долгое время скрывать свою личность их противоправная деятельность может быть весьма продолжительной.

Влияние данных лиц на формирование экстремистских воззрений у населения представляется более существенным, в отличие от действий «неосмотрительных» киберэкстремистов. У «осторожных» киберэкстремистов прослеживается стремление к последовательности и систематичности негативного информационно-психологического воздействия. Несмотря на то, что рассматриваемые лица, как правило, не известны широкому кругу общественности, они стремятся своими действиями охватить как можно большую аудиторию пользователей.

Характеризуя криминологическую характеристику личности представителей организованного киберэкстремизма, автор отмечает, что сегодня они нередко действуют в интересах зарубежных стран. Данные лица часто имеют высшее образование и специальные знания по наиболее эффективному использованию ИТТ для сохранения своей анонимности, привлечения финансирования и создания экстремистских материалов.

Влияние организованного криминального киберэкстремизма на формирование у населения экстремистских воззрений является наиболее опасным. Практически любой гражданин регулярно может наблюдать экстре-

мистские материалы, массово создаваемые и распространяемые в киберпространстве на профессиональной основе.

Вторая глава «Предпосылки уголовного киберэкстремизма и его предупреждение в Российской Федерации» состоит из трех параграфов.

В *первом параграфе* «Объективные и субъективные предпосылки совершения преступлений экстремистской направленности посредством использования информационно-телекоммуникационных технологий» автор обосновывает необходимость дифференцированного подхода к рассмотрению факторов, детерминирующих киберэкстремистскую преступность. Разделение предпосылок позволяет установить степень воздействия объективных факторов на человеческое поведение и субъективных, личностных особенностей индивида — на его поступки.

В свою очередь, возросшая роль зарубежных стран в распространении экстремизма в России обуславливает целесообразность отдельного рассмотрения внешних (т. е. связанных с непосредственным участием представителей отдельных зарубежных стран) и внутренних (без непосредственного участия представителей отдельных зарубежных стран) предпосылок.

В качестве внешней объективной предпосылки определена непосредственная подготовка и совершение киберэкстремистских преступлений при прямом участии представителей зарубежных стран. Особенно отмечается опасность использования данными лицами ИТТ для организации массовых беспорядков, а также для оперативной и удаленной координации их.

Внутренней объективной предпосылкой является ИДИПВ, которое выражается в скрытой пропаганде деструктивных ценностей, а также в формировании негативного отношения к какой-либо социальной группе путем распространения новостных публикаций относительно совершения преступлений и (или) административных правонарушений с прямым указанием на представителя социальной группы как виновного.

В качестве внешней субъективной предпосылки автором определено вмешательство зарубежных стран во внутривнутриполитические процессы Российской Федерации после распада СССР, способствовавшее в совокупности с рядом взаимосвязанных факторов укоренению у части населения чувства вседозволенности и безнаказанности за распространение экстремистских материалов в киберпространстве. Выделение именно этого исторического периода в качестве предмета изучения обусловлено большим количеством киберэкстремистов в возрасте 30–49 лет. В свою очередь, процесс социализации и формирования основных убеждений человека протекает в период обучения в старшей школе, в вузе (или ССУЗе). Таким образом, наибольший интерес представляет комплекс негативных факторов, действовавших на рассматриваемую категорию граждан, когда они были в возрасте примерно

от 14 до 24 лет. В свою очередь, данный период практически совпадает с периодом формирования государственности в Российской Федерации после распада СССР, сопровождавшегося при активном участии зарубежных стран глобальными изменениями ценностных ориентиров общества в сторону восприятия идеологии либерализма как вседозволенности без ответственности. Кроме того, именно в тот период в нашей стране получили распространение ИТТ, что в совокупности с отсутствием системного контроля со стороны правоохранительных органов за киберпространством еще более способствовало укоренению у части населения чувства безнаказанности за распространение информации противоправного содержания. Автор указывает на прямую взаимосвязь данных факторов и предлагает рассматривать их комплексно как предпосылку совершения киберэкстремистских преступлений сегодня.

К внутренним субъективным предпосылкам отнесены: высокий уровень восприимчивости населения к экстремистским материалам, распространяемым в киберпространстве; низкий уровень осведомленности граждан относительно форм проявления экстремизма, а также ответственности за совершение деяний экстремистской направленности.

Во *втором параграфе* «Обеспечение информационно-психологической безопасности граждан как мера нивелирования деструктивного информационно-психологического воздействия и предупреждения киберэкстремистских преступлений» рассматриваются основные направления соответствующей предупредительной деятельности, преимущественно направленные на устранение внутренних объективных и субъективных предпосылок.

Автор отмечает, что обеспечение информационно-психологической безопасности должно представлять собой комплекс мер, направленных на сохранение состояния защищенности психики личности и общественного сознания от широкого спектра деструктивного информационного воздействия. Одним из источников, через которые деструктивная информация может доходить до большей части населения, являются новостные сообщества в социальных сетях и мессенджерах. Диссертант указывает на их особую популярность среди граждан. Учитывая важность распространяемой в таких сообществах информации, можно говорить о том, что именно она вызывает наибольший интерес граждан, зачастую провоцируя эмоциональные обсуждения, среди которых нередко могут распространяться экстремистские материалы. Вместе с тем сам формат ее распространения создает условия для негативных явлений, что обусловлено особенностями механизма создания и администрирования новостных сообществ. Их владельцам нередко выгодно не пресекать эмоциональные обсуждения для поддержа-

ния активности аудитории. Особенно опасной представляется ситуация, при которой распространяется информация сомнительного происхождения, специально провоцирующая реакцию пользователей.

В связи с этим предлагается законодательное урегулирование порядка администрирования сообществ социальных сетей и мессенджеров, в которых регулярно распространяется общественно значимая информация, а также создание соответствующего реестра в целях осуществления надлежащего контроля. Положения действующей статьи 10.6 «Особенности распространения информации в социальных сетях» Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» в большей степени касаются владельцев самих социальных сетей, но не владельцев новостных сообществ, функционирующих уже непосредственно внутри соцсетей. Соответствующая ответственность для таких лиц наступает на общих для всех пользователей основаниях, что не вполне обоснованно ввиду несопоставимых объемов аудитории, на которую они имеют возможность оказывать воздействие, и специфики распространяемой ими информации. Таким образом, для устранения условий распространения экстремистской информации целесообразно дополнить 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). В целях обеспечения контроля следует создать соответствующий реестр.

Автор также отмечает важность осуществления среди населения просветительской деятельности по разоблачению недостоверных сведений для нивелирования негативного эффекта от высокой восприимчивости населения к экстремистским материалам, распространяемым в киберпространстве.

Исследователем разработана 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 (от англ. «natural language processing» — обработка естественного языка), которая будет выполнять задачу по анализу содержания проверяемой информации и сопоставлять ее с данными, размещенными на официальных информационных порталах государственных органов и в СМИ.

Также предлагается создание соответствующих информационных площадок в социальных сетях, мессенджерах и видеохостингах с обязательной отметкой, позволяющей гарантировано идентифицировать их как официальные государственные.

В целях противодействия ИДИПВ, выражающемуся в распространении информации относительно совершения правонарушений с прямым указанием на принадлежность виновника к той или иной социальной группе, следует предусмотреть соответствующий законодательный запрет в положениях ст. 4 Закона РФ от 27 декабря 1991 г. № 2124 «О средствах массовой информации».

Для предупреждения ИДИПВ на несовершеннолетних через пропаганду деструктивных идей в фильмах, видеоиграх, книгах и т.д. особое внимание необходимо уделять следующим направлениям обеспечения информационно-психологической безопасности: работе по мониторингу содержания информации, распространяемой популярными среди несовершеннолетних блогерами; увеличению в киберпространстве объема социально полезных материалов, усиливающих роль традиционных российских духовно-нравственных ценностей в воспитании детей для формирования у них чувства неприязни к различным деструктивным идеям; взаимодействию государства, педагогических работников и родительского сообщества по вопросам просветительской деятельности относительно новых деструктивных течений.

В *третьем параграфе* «Организационно-тактические и технические меры по предупреждению преступлений экстремистской направленности, совершаемых с использованием информационно-телекоммуникационных технологий» рассмотрены меры, направленные преимущественно на прогнозирование и своевременное пресечение готовящихся и выявление уже совершенных киберэкстремистских преступлений, в том числе тех, в которых задействованы представители зарубежных стран (внешняя объективная предпосылка уголовного киберэкстремизма).

Автором представлен алгоритм по разработке и внедрению технологий искусственного интеллекта для автоматического выявления и идентификации экстремистских материалов на общедоступных страницах пользователей социальных сетей и мессенджеров. Для идентификации наиболее целесообразно применять нейросетевые модели (инструменты машинного обучения, в которых компьютер учится выполнять определенную задачу, анализируя примеры обучения). Соответствующим образом обученная нейросеть способна выполнять задачу бинарной классификации, определяя входящую информацию как экстремистскую или неэкстремистскую.

Обучить такую модель возможно только путем сбора и адаптации качественных обучающих данных (т.е. большой выборки экстремистских материалов разнообразного содержания и форматов представления). Вместе с тем проведенный автором анализ показал, что в доктрине и правоприменительной практике уже определен ряд неизменных признаков, которыми обладает

каждый вид экстремистской информации. Взяв их за основу можно без существенных затрат собрать большое количество данных, по которым следует обучить нейросетевую модель идентификации экстремистских материалов.

Вместе с тем, кроме непосредственного создания модели, необходимо предпринять ряд мер организационного характера, направленных на автоматический сбор и передачу информации, которую нейросеть будет обрабатывать. Учитывая популярность социальных сетей среди населения, по мнению автора, наиболее перспективными и не нарушающими конституционные права граждан являются сбор и обработка информации с общедоступных страниц, на которых часто распространяются экстремистские материалы. В указанных целях предлагается внести в ст. 10.6 Федерального закона от 27 июля 2006 г. № 149-ФЗ дополнения, которые обязывали бы владельцев социальных сетей обеспечить сбор и передачу информации с таких страниц в автоматическом режиме. Обязанность по принятию данной информации, а также по разработке нейросетевой модели целесообразно возложить на Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций.

В целях противодействия организованному криминальному киберэкстремизму перспективным видится применение технологий искусственного интеллекта для прогнозирования подготовки к массовым беспорядкам или иным видам организационной деятельности среди определенных групп пользователей. На основе автоматического анализа содержания и частоты сообщений, отправляемых в чатах социальных сетей или мессенджеров, соответствующая модель способна сделать прогноз такой подготовки, результаты которого следует оперативно использовать для своевременного принятия предупредительных мер.

Автор также отмечает целесообразность совершенствования методов по поиску и анализу информации из открытых источников для установления личности киберэкстремистов в целях своевременного пресечения их противоправной деятельности. Вместе с тем для эффективного поиска и анализа данной информации целесообразно применять специализированное программное обеспечение. Диссертант указывает на необходимость разработки соответствующих внутриведомственных программных комплексов, поскольку использование сторонних средств неизбежно сопряжено с рисками их блокировки или ограничения функционала.

В **заключении** содержатся основные результаты и выводы диссертационного исследования, изложены ключевые элементы криминологической характеристики преступлений экстремистской направленности, совершаемых с использованием ИТТ, представлен комплекс мер по их предупреждению, а также определены перспективы дальнейшей научной разработки темы.

В приложениях представлены результаты анкетирования практических сотрудников правоохранительных органов, педагогических работников и жителей Омской области, программа контент-анализа публикаций в новостных сообществах мессенджеров и социальных сетей, обзор предлагаемых изменений и дополнений в нормативно-правовые акты.

**Основные положения диссертационного исследования
опубликованы в следующих работах:**

Статьи в рецензируемых научных изданиях, рекомендованных Высшей аттестационной комиссией при Министерстве науки и высшего образования Российской Федерации для опубликования основных научных результатов диссертаций:

1. Ильиных, Н. А. Киберэкстремизм: понятие и разграничение с иным информационным деструктивным воздействием на человека в киберпространстве / Н. А. Ильиных. — Текст : непосредственный // Известия Юго-Западного государственного университета. Серия: История и право. — 2023. — Т. 13, № 1. — С. 64–74 (0,78 п. л.).

2. Ильиных, Н. А. Структура, уровень динамика киберэкстремизма в Российской Федерации / Н. А. Ильиных. — Текст : непосредственный // Вестник Сибирского юридического института МВД России. — 2023. — № 3. — С. 196–201 (0,49 п. л.).

3. Ильиных, Н. А. Использование информационных платформ и искусственного интеллекта в противодействии фейковым новостям как мера предупреждения киберэкстремизма / Н. А. Ильиных. — Текст : непосредственный // Научный вестник Омской академии МВД России. — 2025. — Т. 31, № 1. — С. 37–43 (0,76 п. л.).

4. Ильиных, Н. А. Криминологическая характеристика личности киберэкстремиста, деяния которого не связаны с организацией экстремистского сообщества или организации / Н. А. Ильиных, В. В. Бабурин. — Текст : непосредственный // Психопедагогика в правоохранительных органах. — 2025. — № 2. — С. 234–240 (0,98 п. л. / 0,98 п. л.).

5. Ильиных, Н. А. Предпосылки киберэкстремистских преступлений и отдельные меры их предупреждения / Н. А. Ильиных. — Текст : непосредственный // Вестник Дальневосточного юридического института МВД России имени И. Ф. Шилова. — 2025. — № 3. — С. 58–66 (0,82 п. л.).

Иные публикации:

6. Ильиных, Н. А. Отдельные факторы распространения экстремизма среди детей в информационно-телекоммуникационном пространстве /

Н. А. Ильиных. — Текст : электронный // Правоохранительная деятельность органов внутренних дел в контексте современных научных исследований : материалы всероссийской научно-практической конференции адъюнктов, аспирантов и соискателей (г. Санкт-Петербург, 23 декабря 2022 г.). — Санкт-Петербург : Санкт-Петербургский университет МВД России, 2022. — С. 230–232 (0,2 п. л.).

7. *Ильиных, Н. А.* Роль информационно-телекоммуникационных технологий в совершении экстремистских преступлений в Российской Федерации, анализ судебной практики / Н. А. Ильиных. — Текст: непосредственный // Мир Закона. — 2023. — № 1-2. — С. 32–39 (0,29 п. л.).

8. *Ильиных, Н. А.* Интернет как средство массовой манипуляции молодежью в экстремистских кругах / Н. А. Ильиных. — Текст : электронный // Актуальные проблемы профилактики преступлений : материалы международного научно-практического семинара (г. Омск, 28 марта 2023 г.). — Омск : Омская академия МВД России, 2023. — С. 18–21 (0,18 п. л.).

9. *Ильиных, Н. А.* Риски и угрозы использования нейросетевых моделей в противоправных целях / Н. А. Ильиных. — Текст : непосредственный // Современные тенденции развития юридической науки : материалы международной научно-теоретической конференции молодых ученых, посвященной 100-летию Б. С. Бейсенова (г. Караганда, 12 апреля 2023 г.). — Караганда : Карагандинская академия МВД РК имени Б. Бейсенова, 2023. — С. 100–101 (0,19 п. л.).

10. *Ильиных, Н. А.* Перспективы применения технологии нейронных сетей в профилактике киберэкстремизма / Н. А. Ильиных. — Текст : непосредственный // Преемственность и новации в юридической науке : материалы международной научной конференции адъюнктов, аспирантов и соискателей (г. Омск, 23 мая 2023 г.). — Омск : Омская академия МВД России, 2023. — Вып. 19. — С. 47–49 (0,15 п. л.).

11. *Ильиных, Н. А.* Отдельные аспекты характеристики личности лица, осуществляющего публичные призывы к экстремистской деятельности в Интернете / Н. А. Ильиных. — Текст : непосредственный // Актуальные проблемы борьбы с преступностью: вопросы теории и практики : материалы XXVI международной научно-практической конференции (г. Красноярск, 20–21 апреля 2023 г.). — Красноярск : Сибирский юридический институт МВД России, 2023. — С. 134–136 (0,22 п. л.).

12. *Ильиных, Н. А.* ИмPLICITное информационно-деструктивное воздействие как условие формирования экстремистских взглядов и убеждений / Н. А. Ильиных. — Текст : непосредственный // Актуальные проблемы борьбы с преступностью: вопросы теории и практики : материалы XXVII международной научно-практической конференции (г. Красноярск,

4–5 апреля 2024 г.) : в 2 ч. — Ч. 2. — Красноярск : Сибирский юридический институт МВД России, 2024. — С. 19–22 (0,24 п. л.).

13. *Ильиных, Н. А.* Структура преступлений экстремистской направленности, совершаемых с использованием информационно-телекоммуникационных технологий / Н. А. Ильиных. — Текст : непосредственный // Преемственность и новации в юридической науке : материалы международной научной конференции адъюнктов, аспирантов и соискателей (г. Омск, 21 мая 2024 г.). — Вып. 20. — Омск : Омская академия МВД России, 2024. — С. 52–54 (0,15 п. л.).

14. *Ильиных, Н. А.* Новостные сообщества в социальных сетях и мессенджерах как источник распространения фейковой информации / Н. А. Ильиных. — Текст : электронный // Актуальные проблемы профилактики преступлений : тезисы докладов и сообщений международного научно-практического семинара (г. Омск, 31 октября 2024 г.). — Омск : Омская академия МВД России, 2024. — С. 13–15 (0,14 п. л.).

15. *Ильиных, Н. А.* Ведомственное программное обеспечение анализа данных из открытых источников для предупреждения киберэкстремизма / Н. А. Ильиных. — Текст : непосредственный // Преемственность и новации в юридической науке : материалы международной научной конференции адъюнктов, аспирантов и соискателей (г. Омск, 20 мая 2025 г.). — Омск : Омская академия МВД России, 2025. — Вып. 21. — С. 63–65 (0,15 п. л.).

Подписано в печать ____ .10.2025

Усл. печ. л. 1,5
Тираж 130 экз.

Уч.-изд. л. 1,5
Заказ № ____

ОПиОП РИО Омской академии МВД России
644092, г. Омск, пр-т Комарова, д. 7