

В диссертационный совет 03.2.010.01
на базе федерального государственного
казённого образовательного учреждения
высшего образования «Омская ордена
Почета академия Министерства
внутренних дел Российской Федерации»
(644092, г. Омск, пр-т Комарова, д. 7).

ОТЗЫВ ОФИЦИАЛЬНОГО ОППОНЕНТА
на диссертацию Ильиных Никиты Андреевича
«Криминологическая характеристика и предупреждение преступлений
экстремистской направленности, совершаемых с использованием
информационно-телекоммуникационных технологий», представленной
на соискание учёной степени кандидата юридических наук
по специальности 5.1.4 – Уголовно-правовые науки

Тема диссертационного исследования Ильиных Н.А. является актуальной, чрезвычайно своевременной и значимой. Активное развитие информационно-телекоммуникационных технологий, глобальная цифровизация нашего мира, объективно вывела общество за рамки привычного общения и переключила нас на виртуальное взаимодействие. Новейшие кибертехнологии позволяют мгновенно решать серьёзные вопросы, подписывать необходимые документы, совершать сделки, и даже проводить высокотехнологичные операции на расстоянии. Вместе с тем, появляются и новые киберпреступления, а также изменяются способы их совершения, где на передний план выступает использование преступниками информационно-коммуникационных технологий.

Экстремистская идеология определяется Стратегией противодействия экстремизму в Российской Федерации¹ как совокупность взглядов и идей, пропагандирующих насильственные и иные противоправные действия как основное средство разрешения политических, расовых, национальных, религиозных и социальных конфликтов и противоречий.

¹ Указ Президента Российской Федерации от 28.12.2024 г. № 1124 «Об утверждении Стратегии противодействия экстремизму в Российской Федерации». – Консультант Плюс. 12.09.2025 г.

Одним из наиболее опасных видов киберпреступлений являются преступления экстремистской направленности. Особенность экстремистских угроз выражается в различных проявлениях деструктивного характера, направленного на продвижение радикальной идеологии, направленной на дестабилизацию общественно-политической, экономической жизни государства, нарушения единства и целостности Российской Федерации, «расшатывание» изнутри исторических и традиционных ценностей.

Киберэкстремизм является высоко латентным, так как совершается скрытно, обезличено, носит трансграничный, дистанционный характер, предполагает разнообразие способов совершения преступления с использованием информационно-телекоммуникационных технологий. Киберэкстремистов сложно вычислить и своевременно обезвредить. В государстве отсутствует обоснованный комплекс технологий, который целесообразно применять для автоматизированной идентификации экстремистского контента в киберпространстве.

Одной из причин подобной ситуации является недостаточное научное изучение преступлений данной направленности. Полагаем, что диссертационное исследование Ильиных Н.А. во многом способствует решению указанных проблем.

Соискателем правильно определены основные методологические направления исследования, объект, предмет, а также задачи диссертации. Широкая нормативная и эмпирическая база исследования позволили комплексно охватить проблематику киберэкстремизма, определить сущностные признаки и сформулировать определение киберэкстремизма в России, оценить современное состояние киберэкстремистской преступности, определить типологию киберэкстремистов, оценить их влияние на формирование экстремистских взглядов и убеждений у населения, выявить тенденции предпосылок совершения указанных видов преступлений.

Объектом диссертационного исследования определена совокупность общественных отношений, складывающихся в связи с совершением преступлений экстремистской направленности с использованием информационно-телекоммуникационных технологий, а также их предупреждением.

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

Цель диссертационного исследования Ильиных Н.А. состояла в получении нового криминологического знания о преступлениях экстремистской направленности, совершаемых с использованием информационно-телекоммуникационных технологий, и разработке на данной основе теоретически обоснованных предложений по их предупреждению.

Результаты исследования Ильиных Н.А. позволяют расширить представление о киберпреступности и киберугрозах в современном обществе и направить вектор для проведения дальнейших исследований в области кибербезопасности, уголовно-правовой регламентации киберпреступлений с целью приведения в соответствие с требованиями сегодняшнего времени уголовного законодательства.

Достоверность и объективность сформулированных положений, выносимых на защиту, получена путем общенаучных и частнонаучных методов познания, а также с использованием системно-структурного метода, метода анализа, что позволило диссертанту классифицировать совокупность преступлений киберэкстремистской направленности, дать криминологическую характеристику киберэкстремистов, выявить тенденции экстремистских преступлений с использованием информационно - телекоммуникационных технологий и предложить меры предупреждения указанных преступлений.

Метод статистики и опроса позволил диссертанту объективно проанализировать современное состояние и структуру киберэкстремистской преступности, выделить существенные проблемы и сформулировать предложения по их эффективному предупреждению.

Теоретическая значимость диссертационного исследования Ильиных Н.А. обоснована задачей комплексного изучения и обобщения имеющихся научных взглядов о противодействии киберэкстремизму, устранения пробелов уголовного законодательства, а также необходимостью своевременного принятия мер правоохрательными органами в отношении киберэкстремистских угроз.

Практическая значимость диссертации обусловлена неготовностью современного общества к своевременному уголовно-правовому реагированию на киберугрозы экстремистской направленности, необходимостью внесения изменений в уголовное законодательство, так как существуют постоянные проблемы квалификации экстремистских преступлений, и выработке мер криминологического воздействия на

преступность в сфере экстремизма с использованием интернет и телекоммуникационных технологий.

Диссертантом предложен комплекс мер, направленных на обеспечение информационно-психологической безопасности личности, а также обоснованы организационно-тактические и технические меры по предупреждению киберэкстремизма, что значительно обогатит криминологическую науку и позволит помочь правоохранительным органам в предупреждении киберэкстремизма.

Степень обоснованности научных положений, выводов и рекомендаций, сформулированных в диссертации Ильиных Н.А. их достоверность, определяются качеством содержания и объёмом использованных источников, образующих теоретическую и эмпирическую базу исследования, его правовую основу, использованием апробированного научно-методического аппарата, внутренней логической связке суждений и выводов.

Эмпирическая база диссертации включает объективные статистические данные Генеральной прокуратуры Российской Федерации и Судебного департамента при Верховном Суде Российской Федерации за 2003–2024 гг.; изучение и анализ судебных решений по делам о киберпреступлениях экстремисткой направленности (111 судебных дел), проведение анкетирования сотрудников Центра по противодействию экстремизму УМВД России по Омской области, широкого круга сотрудников органов внутренних дел, следственных подразделений МВД России по Омской, Новосибирской, Тюменской, Кемеровской, Томской областям, Красноярскому и Алтайскому краям, Ямало-Ненецкому и Ханты-Мансийскому автономным округам, педагогических работников, а также жителей Омской области.

Высокая степень достоверности результатов диссертационного исследования Ильиных Н.А. обеспечена глубоким и многоаспектным изучением киберэкстремистских преступлений, методологией исследования, опирающейся на диалектический, общенаучные и частнонаучные методы познания; репрезентативностью эмпирического материала, включающего данные судебной и правоохранительной практики, результаты собственных исследований. Перечень источников, изученных диссертантом, составляет 232 источника.

Результаты исследования обосновывают возможность применения мер предупреждения преступлений киберэкстремистской направленности в

современной правоохранительной деятельности, а также в образовательном процессе при изучении учебных дисциплин «Криминология» и «Предупреждение преступлений и административных правонарушений органами внутренних дел».

Диссертационное исследование прошло апробацию на научных и научно-практических конференциях, в том числе международного и всероссийского уровней. Основные теоретические положения, выводы и рекомендации соискателя, содержащиеся в работе, были представлены на всероссийских и международных конференциях.

Результаты диссертационного исследования Ильиных Н.А. 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».

Разработанная диссертантом 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).

Основные положения, выводы и рекомендации, полученные в результате диссертационного исследования, отражены в опубликованных работах (15 статей), 5 из которых – в рецензируемых научных изданиях, рекомендованных Высшей аттестационной комиссией при Министерстве науки и высшего образования РФ для публикаций основных научных результатов диссертаций.

Структура диссертационного исследования Ильиных Н.А. подчинена логике научного исследования, состоит из введения, двух глав, объединяющих шесть параграфов, заключения, списка источников и приложения.

Во введении отражена актуальность темы диссертационного исследования, охарактеризована степень её научной обоснованности; определены объект, предмет, цель и задачи, методологическая база, теоретическая, нормативно-правовая и эмпирическая основы исследования, раскрывается научная новизна; сформулированы положения, выносимые на защиту; определена теоретическая и практическая значимость; приведены сведения об обоснованности, достоверности, апробации и внедрении полученных результатов и структуре диссертации.

В первой главе «Понятие и криминологическая характеристика преступлений экстремистской направленности, совершаемых с использованием информационно-телекоммуникационных технологий» в рамках отдельных параграфов исследуются вопросы сущности киберэкстремизма в современной России, анализируется его понятие, выявлены детерминанты и механизм деструктивного воздействия на граждан с использованием информационных и телекоммуникационных технологий. Автор приводит данные официальной статистики за период с 2020 по 2024 год, где киберэкстремистских преступлений было совершено 56,42%. Согласимся с диссертантом в его выводах о том, что преступления экстремистской направленности с использованием информационно-телекоммуникационных технологий являются преступлениями высокой степени общественной опасности (с. 21).

Обосновывая понятие киберэкстремизма, диссертант правильно оттолкнулся от дефиниции «киберпреступление» (ст. 23 – 26), отметив дискуссионность и проблемность определения признаков киберэкстремизма в научной среде и неопределённость термина «экстремизм», содержащегося в нескольких нормативных правовых актах (с. 27 – 28; 30 – 32).

Диссертантом верно определён вектор детерминантного формирования у пользователей Интернет экстремистских взглядов при скрытом деструктивном информационно-психологическим воздействием личность в киберпространстве (с. 29).

Интересным является авторский подход к определению понятия «киберэкстремизм», под которым диссертант понимает социальное, относительно массовое явление, проявляющееся в совокупности запрещенных законом деяний, совершаемых по экстремистским мотивам, с обязательным использованием информационно-телекоммуникационных технологий, моделирующих киберпространство (с. 36).

Особый акцент диссертант делает на то, 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 (51 – 52).

Диссертант верно подметил одну из современных тенденций киберэкстремистской преступности, в частности, усиление роли зарубежных стран в подготовке и совершении преступлений экстремистской направленности в России (с. 59), что на наш взгляд является весьма важным и подтверждается данный факт криминологическим обоснованием структуры преступлений киберэкстремистского характера, в которой около 44,9% преступлений совершаются по политическим мотивам (с. 61).

Криминологическая характеристика личностей киберэкстремистов, представленная диссертантом, позволила выявить тот факт, что большинство киберэкстремистов на момент совершения преступления были в возрасте от 30 до 49 лет (66,8%) (с. 64); наиболее часто киберэкстремистские преступления совершали мужчины (в 93,4%) (с. 65).

Диссертантом установлено на основе анализа материалов судебной практики (изученных уголовных дел, приговоров судов), что основным способом распространения информации, содержащей публичные призывы к экстремистской деятельности, оскорбления, высказывания, выражающие ненависть в отношении какой-либо социальной группы, объединенной по политическому, религиозному, национальному, расовому или иному признаку является систематическое распространение таких сведений путем размещения преступниками на своих личных страницах в социальных сетях и мессенджерах (с. 66).

Вторая глава диссертации «Предпосылки уголовного киберэкстремизма и его предупреждение в Российской Федерации» раскрывает объективные и субъективные факторы совершения преступлений киберэкстремистских преступлений.

Среди наиболее значимых автор выделяет непосредственное участие в экстремистских преступлениях с использованием интернета и телекоммуникационных технологий представителей отдельных зарубежных стран или аффилированных ими коммерческих организаций (с. 95).

Внутренней объективной предпосылкой является формирование в контенте скрытой пропаганды насилия в отношении определенных групп

людей или иные деструктивные идеи, которые могут выступить в качестве возможной предпосылки приобретения пользователем экстремистских взглядов и убеждений. Автор отмечает, что особенно опасным является такое информационно-психологическое воздействие на несовершеннолетних, так как у них еще не сформирована устойчивая психика и может отсутствовать достаточный уровень критического отношения к просматриваемому контенту (с. 96).

Автор выявляет и внешние объективные факторы киберэкстремизма, среди которых отмечено активное участие 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 (с. 101).

Диссертантом сформулирован вывод о недостаточном контроле за информационно-телекоммуникационным пространством со стороны государственных органов в совокупности с убежденностью пользователей во вседозволенности своих действий, что способствовало укоренению в обществе мнение о том, что в киберпространстве можно безнаказанно распространять контент любого содержания, в том числе и экстремистского, что может выступать в качестве предпосылки совершения киберэкстремистских преступлений (с. 104).

Согласимся с выводом диссертанта о том, что существующий сегодня достаточно низкий уровень осведомленности населения относительно сущности экстремизма, форм его проявления, может выступать в качестве субъективной предпосылки киберэкстремистской преступности (с. 108). И многозадачным процессом своевременного реагирования здесь должна выступать информационно-психологическая безопасности общества.

Обеспечение информационно-психологической безопасности, как отмечает диссертант, должно представлять собой комплекс мер, направленных на сохранение состояния защищенности психики личности и общественного сознания от масштабного деструктивного информационного воздействия (с. 111). В обоснование данного предложения предлагается внесение изменений в Федеральный закон «Об информации, информационных технологиях и защите информации» от 27.07.2006 № 149-ФЗ в части дополнения статьи 10.6 частями 1.4 и 1.5 о закреплении за владельцами новостных сообществ части обязанностей и ответственности, аналогичных тем, которые возложены сегодня на владельцев социальных сетей (с. 118).

Весьма актуальным и своевременным на наш взгляд является предложение диссертанта об усилении работы государства, педагогического сообщества в обеспечении информационно-психологической безопасности несовершеннолетних, как наиболее уязвимой категории, подверженной в большей степени деструктивному воздействию экстремистов (с. 131). Автором предложена разработка ботов и последующая их интеграция во все популярные среди российских пользователей социальные сети и мессенджеры (с. 147) с необходимостью его оперативного внедрения в деятельность правоохранительных органов (с. 159).

Таким образом, выводы диссертанта являются обоснованными для совершенствования предупредительных мер противодействия киберэкстремизму. Предложенная автором разработка применения технологий искусственного интеллекта для автоматического выявления и идентификации экстремистских материалов, публикуемых на открытых страницах в социальных сетях и мессенджерах, своевременна и поможет существенно снизить риск попадания в интернет-пространство экстремистских материалов.

Подводя итог, можно заключить, что диссертация Ильиных Н.А. обладает научной новизной и практической значимостью. Принципиально новыми положениями, разработанными диссертантом, являются следующие:

1. предложено понятие «киберэкстремизма»;
2. проведён актуальный криминологический анализ экстремистских преступлений, совершаемых с использованием информационно-телекоммуникационных технологий, выявлены их детерминаты, разработана типология киберэкстремистов;
3. в структуре киберэкстремистских преступлений выявлены основные мотивы их совершения;
4. представлен криминологический портрет представителя организованного киберэкстремизма (трудоспособный мужчина в возрасте 30–49 лет, целенаправленно вступивший в экстремистское сообщество или организацию;
7. определены объективные и субъективные предпосылки совершения киберэкстремистских преступлений;
8. предложено создание реестра новостных сообществ в отношении владельцев страниц социальных и интернет сетей для организации контроля за информацией, размещаемой на их контентх;

9. в целях противодействия распространению недостоверной общественно значимой информации предложена концепция программного обеспечения, представляющего собой систему автоматизированной верификации новостной информации (САВНИ) и внедрение в деятельность правоохранительных органов технологий искусственного интеллекта для идентификации экстремистских материалов, публикуемых на общедоступных страницах в социальных сетях и мессенджерах.

В целом, положительно оценивая качество диссертационного исследования, проведённого Ильиных Н.А., обращаем внимание на некоторые положения, которые являются спорными и полагаем, в процессе защиты диссертации будут уточнены:

1. Видится необходимость уточнения понятия киберэкстремизма, под которым автор понимает социальное, относительно массовое явление, характеризующееся совокупностью запрещенных законом деяний, совершаемых по экстремистским мотивам, с обязательным использованием технологий, моделирующих информационно-телекоммуникационное пространство (киберпространство). Использование в терминологии таких дефиниций как «социальное» - которое может употребляться как в широком, так и в узком смысле, а также «относительно массовое явление» - вызывает неопределённость и не способствует правильному пониманию и толкованию новых явлений. Кроме того, указание на «совокупность запрещённых законом деяний, совершаемых по экстремистским мотивам» должна быть конкретизирована, так как не совсем понятно, какая «совокупность деяний» и какой закон в данном случае имел ввиду диссертант, учитывая, что понятие «экстремизм» содержится в нескольких нормативных правовых актах.

2. В криминологическом анализе экстремистских преступлений, совершаемых с использованием интернета и телекоммуникационных технологий, автор отмечает преобладающими – политические мотивы (44,9%), но недостаточно аргументирует свою позицию, ссылаясь на изучение судебной практики. Не раскрываются виды политических мотивов совершаемых преступлений, отсутствуют примеры совершаемых по данным мотивам киберэкстремистских преступлений, что не отражает в полной мере вывод о преобладании именно политической мотивации преступлений киберэкстремистской направленности.

3. Автором предлагается проводить просветительскую работу среди населения по разоблачению недостоверных сведений для нивелирования негативного эффекта от высокой восприимчивости населения к

экстремистским материалам, распространяемым в киберпространстве, однако не уточняется, в чём именно должна состоять такая просветительская работа, какая информация будет относиться к таковой, то есть просветительской, кто и каким образом должен такую работу проводить. Между тем, именно широкое информирование населения о способах совершения преступлений, и в целом о том, какая именно информация содержит признаки экстремистской и будет признана таковой, необходимо доводить до сведения граждан. Как, например, способы борьбы с кибермошенничеством в настоящее время, широкое информирование о которых дает свои положительные результаты.

4. Диссертантом предложена система автоматизированной верификации новостных публикаций в информационно-телекоммуникационном пространстве, где каждый пользователь интернета самостоятельного может использовать формат бота для определения степени достоверности любой новости в киберпространстве. В целом, соглашаясь с тем, что использование интеллектуального разума достаточно эффективно работает и может существенно помочь и в борьбе с киберэкстремизмом, вместе с тем, отметим, что в работе ботов бывает много ошибок. Соответственно, возникает вопрос о том, кто и как должен контролировать работу системы автоматизированной верификации новостных публикаций в интернете и проверять работу ботов, в какой последовательности и как часто?

5. При проведении криминологического анализа и статистических данных о количестве зарегистрированных экстремистских преступлений с использованием информационно-телекоммуникационных технологий диссертант отмечает, что 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 (с. 45), но данный факт оставляет без дальнейшего внимания. Диссертантом не исследовался вопрос о том, почему в общей криминологической структуре не выявляются указанные преступления: данный факт свидетельствует о недоработке указанных составов преступлений с точки зрения их сложного толкования, или здесь иные причины, и в чём они состоят.

Вместе с тем, указанные замечания не влияют на общую положительную оценку работы, носят рекомендательный и дискуссионный характер, что позволяет сделать следующие выводы:

– диссертационное исследование Ильиных Никиты Андреевича на тему «Криминологическая характеристика и предупреждение преступлений

экстремистской направленности, совершаемых с использованием информационно-телекоммуникационных технологий», является самостоятельным научным завершённым исследованием, содержащим научные теоретические и практические решения актуальных проблем в рамках специальности 5.1.4 – Уголовно-правовые науки;

– диссертация и автореферат соответствуют друг другу по структуре и содержания;

– представленное научное исследование отвечает требованиям, предъявляемым к кандидатским диссертациям, предусмотренным Положением о присуждении учёных степеней, утверждённым Постановлением Правительства Российской Федерации 24.09.2013 г. № 842;

– автор представленной диссертации Ильиных Никита Андреевич – заслуживает присуждения учёной степени кандидата юридических наук по специальности 5.1.4 – Уголовно-правовые науки.

Официальный оппонент:

Доцент кафедры уголовного права и криминологии федерального государственного автономного образовательного учреждения высшего образования «Омский государственный университет им. Ф.М. Достоевского», кандидат юридических наук, доцент
Никульченкова Елена Владимировна
«22» октября 2025 г.

Подпись Никульченковой Е.В. удостоверяю.

Учёный секретарь учёного совета
ФГАОУ ВО «Омский государственный
Университет им. Ф.М. Достоевского



О.С. Роголёва

Федеральное государственное автономное образовательное учреждение высшего образования «Омский государственный университет им. Ф.М. Достоевского», 644077, Россия, Омская область, г. Омск, проспект Мира, д. 55-А, тел. +7 (3812) 67-01-04; e-mail: rector@omsu.ru; официальный сайт: <https://omsu.ru>.