Гибридные угрозы как фактор трансформации современной преступности: уголовно-правовые и криминологические аспекты противодействия

Савельева Ирина Владимировна
канд. псих. наук, доцент, Белгородский государственный национальный исследовательский университет, I_Saveljeva@bsuedu.ru

Статья посвящена теме трансформации современной преступности в Российской Федерации под влиянием гибридных угроз. Особое внимание уделяется изменению криминальной детерминации, при которой преступность приобретает черты инструмента межгосударственного противоборства, а классические институты уголовного права (соучастие, вина, квалифицирующие признаки) оказываются недостаточно эффективными в условиях «серых зон». Цель исследования – разработка теоретической модели совершенствования уголовно-правового и криминологического инструментария противодействия преступлениям, совершаемым в контексте гибридных конфликтов. Методы включают диалектический, системный, формально-юридический, сравнительно-правовой, статистический анализ и метод экспертных оценок. Результаты: выявлены три системных тренда – технологизация и дистанционность посягательств (массовое применение БПЛА, кибератаки), вовлечение уязвимых категорий населения (эффект «прокси-акторов») и сращивание информационно-психологического воздействия с уголовно-наказуемыми деяниями. Обоснован феномен «правоприменительного паралича» при квалификации деяний в условиях внешнего дистанционного управления. Выводы: предложен комплекс законодательных изменений (дополнение ст. 63 УК РФ новыми отягчающими обстоятельствами, расширение ст. 281 УК РФ) и разработка постановления Пленума Верховного Суда РФ, а также организационно-профилактические меры.

Ключевые слова: гибридные угрозы; трансформация преступности; диверсия; беспилотные летательные аппараты; информационно-психологическое воздействие; уголовно-правовая квалификация; правоприменительный паралич; прокси-акторы; серая зона; противодействие.

Введение

Современный этап развития государственно-правовой системы Российской Федерации характеризуется беспрецедентным усложнением характера внешних и внутренних вызовов безопасности. Одним из наиболее деструктивных факторов выступает феномен гибридных угроз. Несмотря на закрепление данного понятия в стратегических документах (включая его фиксацию в качестве большого вызова в Стратегии научно-технологического развития РФ [7]), отсутствие единой легальной дефиниции создает правоприменительные риски. Это вынуждает правоохранительные органы действовать в условиях правовой неопределенности, опираясь на разрозненные положения Стратегии национальной безопасности 2021 года, касающиеся защиты информационного суверенитета и противодействия деструктивному информационно-психологическому воздействию [8].

Существующие институты Общей части УК РФ демонстрируют недостаточную эффективность при квалификации деяний, детерминированных гибридным воздействием. Организованная преступность и экстремистские формирования все чаще выступают в качестве прокси-акторов, реализуя цели иностранных государств через внутреннюю криминальную среду. Транснациональные криминальные сети интегрируются в механизмы гибридной войны, предоставляя свои инфраструктурные и логистические возможности государственным субъектам для дестабилизации обстановки.

Объектом исследования выступают общественные отношения в сфере обеспечения национальной безопасности от криминальных проявлений гибридных конфликтов. Предметом исследования являются уголовно-правовые и криминологические аспекты трансформации современной преступности под влиянием гибридных угроз. Целью работы является разработка теоретической модели совершенствования уголовно-правового и криминологического инструментария противодействия преступлениям, совершаемым в контексте гибридных конфликтов.

Материалы и методы Методологическую основу исследования составил диалектический подход в сочетании с системным методом анализа социально-правовых явлений. Применялись формально-юридический метод для толкования норм УК РФ, сравнительно-правовой метод при анализе доктрины НАТО и ЕС, а также статистический анализ данных официальной ведомственной отчетности МВД России за период 2020–2025 гг. (с учетом предварительных данных за 2026 г.). Специфика предмета потребовала обращения к методу экспертных оценок для верификации гипотезы о возникновении «правоприменительного паралича».

Эмпирическую базу составили: официальные статистические данные МВД России за 2020–2026 гг.; данные Минобороны России о количестве сбитых БПЛА; обобщенные судебные решения по делам о диверсиях и террористических актах; материалы аналитических докладов и экспертные оценки, представленные в открытых источниках.

Литературный обзор. Принципиальным для криминологического анализа представляется разграничение гибридной угрозы как потенциального вызова и гибридной войны как процесса практической реализации деструктивных механизмов.

Формирование современного понимания гибридных угроз прошло несколько этапов, отражающих смещение акцентов с сугубо военно-стратегических аспектов на правовые и криминологические измерения. Впервые термин получил концептуальное оформление в работах Ф. Хоффмана (2007), который охарактеризовал гибридные угрозы как «смесь смертоносности межгосударственного конфликта с фанатичным и продолжительным пылом ведения войны нестандартными средствами» [14], включающую обычные вооружения, нерегулярную тактику, терроризм и преступное поведение. На институциональном уровне дефиниция была закреплена в документах НАТО, где под гибридными угрозами понимаются «угрозы, исходящие от противников с возможностью одновременного адаптивного использования обычных и нетрадиционных средств для достижения

своих целей» [11]. Европейская комиссия и институты ЕС определили их как меры с использованием дипломатических, военных, экономических и технологических тактик для дестабилизации политического противника [1].

В российской науке гибридная война определяется как «война нового типа, проводимая без признаков открытого нападения и внешней агрессии, без применения обычных вооружений, совершаемая группой лиц без объявления начала своих действий» [4], а гибридные угрозы – как «проведение комплексных мероприятий, сочетающих в себе элементы военного и невоенного воздействия на противника и направленных на дезорганизацию и дестабилизацию ситуации на его территории без явного вмешательства» [6, с.207]. Г. Б. Романовский отмечает, что во многих официальных документах проводится прямая связь гибридных угроз с гибридной войной, включающей различные асимметричные действия, не пересекающие порог классического вооруженного конфликта [10]. К таковым относятся: разжигание очагов напряженности; экономическое и информационное давление; кибератаки; формирование военной инфраструктуры в приграничной зоне; использование транснациональной организованной преступности; распространение экстремистской и террористической идеологии [10].

Центральной теоретической конструкцией, позволяющей осмыслить феномен гибридных угроз в криминологическом ключе, выступает понятие «серой зоны». По справедливому замечанию А. В. Федорова, гибридные угрозы функционируют именно в «серых зонах», где трудно установить факт агрессии и своевременно отреагировать классическими средствами [13]. Эти зоны характеризуются тем, что действия находятся ниже порога вооруженного конфликта (не подпадают под международное гуманитарное право), но одновременно выходят за рамки обычных правонарушений, поскольку имеют системный, целенаправленный характер и внешнее управление. Следствием становится невозможность адекватной квалификации содеянного либо необоснованное смягчение наказания, так как действующий УК РФ не содержит специальных норм оценки гибридных посягательств. В такой ситуации классические институты уголовного права (соучастие, вина, квалифицирующие признаки) утрачивают эффективность при квалификации деяний, совершаемых под внешним управлением, что порождает «правоприменительный паралич» и требует институциональных изменений.

Результаты. Период 2022–2026 гг. характеризуется устойчивой корреляцией между внешнеполитической напряженностью и изменением структуры преступности. На фоне общего снижения числа регистрируемых преступлений (в 2025 году – на 12% по киберпреступности; за 5 месяцев 2026 года – на 31,2% по сравнению с аналогичным периодом 2025 года) наблюдается рост тяжких и особо тяжких деяний: 537 тыс. (2022), 589,1 тыс. (2023), 617,3 тыс. (2024) – рекордный показатель за последние 14 лет. За первый квартал 2026 года зафиксировано снижение таких преступлений на 20,4% [9]. Эта парадоксальная динамика свидетельствует не об улучшении криминогенной обстановки, а о переходе преступности в более латентные и технологичные формы, что полностью согласуется с логикой гибридного противоборства.

Анализ официальной статистики МВД России за 2024–2026 годы позволяет выявить специфические тренды, которые могут служить индикаторами гибридного воздействия на криминогенную обстановку.

Тренд 1. Технологизация и дистанционность преступных посягательств. Гибридные угрозы радикально меняют инструментарий преступной деятельности: физический контакт между субъектом и объектом посягательства становится исключением, а не правилом. Наиболее ярким проявлением этого тренда является массовое применение беспилотных летательных аппаратов (БПЛА) и вредоносного программного обеспечения для достижения криминальных целей: от использования БПЛА в целях контрабанды (в том числе наркотических средств), совершения диверсий и террористических актов до заказных убийств с применением FPV-дронов.

По данным Минобороны России, количество сбитых БПЛА над территорией РФ выросло с 300–500 единиц в 2023 году до 7 345 в 2024 и рекордных 27 400 в 2025 году; за первый квартал 2026 года, по оценочным данным, уничтожено около 13 000 беспилотников. Атаки зафиксированы в 49 регионах, включая удаленные территории (Татарстан – до 1 300 км от границы, Башкортостан – до 1 400 км, Тюменская область – около 2 000 км, Иркутская область – до 4 700 км) [12]. При этом эволюция тактик – переход от одиночных запусков к массированным налетам, применение систем наведения на оптоволокне, устойчивых к средствам радиоэлектронной борьбы, – свидетельствует о качественном скачке в милитаризации общеуголовных методов.

Содержащееся в п. 5 ст. 32 Воздушного кодекса РФ («воздушное судно, управляемое, контролируемое в полете пилотом, находящимся вне борта») [3] легальное определение БПЛА ориентировано на гражданскую авиацию и не учитывает полностью автономные системы с элементами искусственного интеллекта, что создает серьезные сложности для правоприменительной практики при квалификации деяний по ст. 281 (диверсия), ст. 205 (террористический акт) и ст. 271.1 УК РФ (нарушение правил использования воздушного пространства). Дополнительную сложность представляет квалификация кибератак на управление дронами: существующие нормы главы 28 УК РФ не охватывают всей специфики перехвата управления, что требует квалификации по совокупности преступлений. Дискуссионным остается вопрос об отнесении БПЛА к предметам хищения или угона (ст. 166 УК РФ) – в отсутствие судебного толкования правоприменитель вынужден действовать в условиях неопределенности.

Тренд 2. Вовлечение уязвимых категорий населения (эффект «прокси-акторов»). Второй системный тренд – замещение профессиональных агентов иностранных спецслужб лицами из социально незащищенных, возрастно-уязвимых и маргинальных групп, действующими за незначительное вознаграждение и не осознающими в полной мере политического контекста своих действий.

Число осужденных по ст. 281 УК РФ (диверсия) выросло с 1 человека в 2022 году до 9 в 2023, 48 в 2024 и еще 48 за первое полугодие 2025 года. Доля несовершеннолетних, осужденных за террористические преступления и диверсии, выросла с 26 (2022) до 41 (2024) человека. Характерно, что в подавляющем большинстве случаев вербовка осуществляется дистанционно через интернет-мессенджеры (Telegram, WhatsApp, Signal и др.) [2] неустановленными лицами, находящимися за пределами РФ, а мотивация исполнителей носит корыстный, а не идеологический характер [5]. С началом специальной военной операции на различных интернет-площадках и в Telegram-каналах резко возросло количество объявлений о «быстром заработке», целевой аудиторией которых являются прежде всего молодежь и представители пожилого поколения.

Центральная проблема квалификации диверсионных преступлений – доказывание обязательного признака субъективной стороны, предусмотренного ч. 1 ст. 281 УК РФ, а именно специальной цели подрыва экономической безопасности и обороноспособности государства. При корыстной мотивации исполнителя (получение денежного вознаграждения) и отсутствии у него идеологической приверженности установить данную цель крайне затруднительно. Это влечет переквалификацию на другие составы – умышленное уничтожение или повреждение имущества (ст. 167 УК РФ) или террористический акт – что не отражает действительной общественной опасности деяния, совершенного под внешним управлением. Дополнительная сложность связана с доказыванием соучастия (ст. 32–36 УК РФ) при дистанционном руководстве: рядовой исполнитель не знает организатора и не осознает конечных целей, что делает невозможным квалификацию как организованной группы. Проблема усугубляется использованием подставных лиц и анонимных платежных систем для финансирования, что делает реальных заказчиков недосягаемыми для российского правосудия.

Тренд 3. Сращивание информационно-психологического воздействия с уголовно-наказуемыми деяниями. Третий тренд заключается в том, что информационно-психологическое воздействие (ИПВ) перестает быть вспомогательным элементом гибридной стратегии и становится самостоятельным инструментом дестабилизации, формирующим мотивационную готовность населения к деструктивным действиям и создающим благоприятный фон для совершения конкретных преступлений.

Парадоксальное снижение регистрируемой киберпреступности (на 12% в 2025 году; на 31,2% за 5 месяцев 2026 года) не свидетельствует о реальном улучшении безопасности, а объясняется переходом криминальных методов в «серые зоны» – использование деструктивного контента, не подпадающего под формальные признаки экстремизма, но системно подрывающего доверие к государственным институтам. Одновременно наблюдается рост числа зарегистрированных терактов, что указывает на усиление информацион-

ной составляющей: подготовка теракта часто сопровождается массированным информационным сопровождением в соцсетях с целью деморализации населения. В структуре преступлений экстремистской направленности преобладают деяния, совершенные с использованием интернет-платформ и мессенджеров.

Наиболее острая проблема – разграничение уголовно наказуемой дезинформации по ст. 207.3 УК РФ (публичное распространение заведомо ложной информации об использовании Вооруженных Сил РФ) и реализации конституционного права на свободу слова (ст. 29 Конституции РФ). Отсутствие критериев отграничения вынуждает правоприменителя оценивать субъективную сторону – наличие специальной цели дестабилизации общественно-политической обстановки, что чрезвычайно сложно доказать в отсутствие прямых доказательств связи с внешним источником. Аналогичная проблема возникает при конкуренции ст. 280 УК РФ (публичные призывы к экстремистской деятельности) и ст. 282 УК РФ (возбуждение ненависти либо вражды). Одно информационное сообщение может содержать признаки обоих составов, и квалификация зависит от направленности умысла: если цель – инициировать немедленные действия – применяется ст. 280; если цель – формирование долгосрочной агрессии – ст. 282. Однако в условиях гибридного воздействия, растянутого во времени, установление такой направленности представляет значительную методологическую проблему для следствия. Не менее сложным является отграничение организации преступного сообщества (ст. 210 УК РФ) от организации экстремистского сообщества (ст. 282.1 УК РФ) при использовании криминальных сетей в качестве прокси-акторов, где внешнее управление маскируется под корыстную мотивацию.

Выявленные тренды свидетельствуют о том, что гибридные угрозы трансформируют современную преступность не столько через появление новых составов, сколько через изменение самой логики криминальной детерминации, классические институты уголовного права – соучастие, вина, объективная сторона, квалифицирующие признаки – оказываются недостаточно эффективными при квалификации деяний, совершаемых в условиях гибридного противоборства. Преступность перестает быть исключительно внутренней социальной патологией и приобретает черты инструмента геополитического давления: организованная преступность и террористические структуры все чаще выступают прокси-акторами в межгосударственных конфликтах.

С учетом изложенного, уголовно-правовые риски целесообразно классифицировать по трем группам, каждая из которых требует специфических подходов к противодействию:

1. Преступления экстремистской направленности (ст. 280–282.3 УК РФ) – где ИПВ выступает не просто способом совершения, а инструментом формирования мотивационной готовности к деструктивным действиям; их объективная сторона сконструирована как формальный состав, что делает их идеальным оружием дистанционного воздействия.

2. Общеуголовные преступления, совершенные под информационно-психологическим воздействием (ст. 110, 128.1, 303 УК РФ и др.) – где ИПВ является средством достижения цели, а также специальные составы, такие как ст. 207.3 УК РФ, используемые для системной дискредитации государственных институтов.

3. Компьютерные преступления (глава 28 УК РФ) – выступающие технологической инфраструктурой гибридных угроз, где неправомерный доступ и создание вредоносных программ являются этапом подготовки информационно-психологических операций или физических атак.

Основная сложность противодействия заключается не в пробелах законодательства как таковых, а в конкуренции смежных составов и отсутствии механизмов учета внешнего управления при квалификации деяний. Разрешение этих проблем требует пересмотра институтов соучастия, вины и объективного вменения, а также разработки специальных критериев для ситуаций, где исполнитель действует под информационно-психологическим контролем извне. Именно это состояние – когда правоприменитель не может адекватно квалифицировать содеянное из-за невозможности вписать его в существующие нормы – мы определяем как «правоприменительный паралич» в условиях «серой зоны».

Обсуждение. Полученные результаты подтверждают исходную гипотезу о возникновении «правоприменительного паралича» в «серых зонах» гибридного противоборства. Выявленные тренды – технологизация, вовлечение уязвимых категорий и сращивание с ИПВ – не являются изолированными, а образуют взаимосвязанную систему, где каждый элемент усиливает действие другого. Так, дистанционное управление через мессенджеры (тренд 2) становится возможным благодаря технологической платформе (тренд 1), а информационное сопровождение (тренд 3) создает легитимизирующий фон для рекрутинга исполнителей.

Сравнение с зарубежными исследованиями показывает, что аналогичные процессы фиксируются и в других государствах, сталкивающихся с гибридными угрозами. Однако российская специфика заключается в масштабном вовлечении несовершеннолетних и социально незащищенных слоев, что связано с высокой цифровой грамотностью молодежи и одновременно низкой правовой осведомленностью, а также с экономической уязвимостью значительной части населения. В отличие от классических террористических организаций, где мотивация преимущественно идеологическая, в российских реалиях доминирует корыстный мотив, что существенно осложняет квалификацию по ст. 281 УК РФ, требующей доказывания специальной цели.

Ограничения исследования связаны с отсутствием полных статистических данных за 2026 год, а также с закрытостью части материалов по делам о диверсиях и терроризме. В перспективе необходимо проведение эмпирических исследований среди сотрудников правоохранительных органов для выявления типичных проблем квалификации, а также анализ судебных решений на предмет единообразия практики.

Теоретическая значимость работы заключается в введении понятия «правоприменительный паралич» и обосновании необходимости пересмотра институтов Общей части УК РФ применительно к гибридным угрозам. Практическая ценность состоит в разработке конкретных законодательных изменений и предложений для Пленума Верховного Суда РФ, которые могут быть использованы в законотворческой и правоприменительной деятельности.

Заключение. Проведенное исследование позволяет сформулировать следующие основные выводы.

1. Гибридные угрозы выступают системным криминогенным фактором, трансформирующим современную преступность не через появление новых составов, а через изменение логики криминальной детерминации. Преступность перестает быть исключительно внутренней социальной патологией и приобретает черты инструмента геополитического давления, а организованные преступные группы и террористические структуры все чаще выполняют функции прокси-акторов в межгосударственном противоборстве.

2. Выявлены три системных тренда трансформации преступности под влиянием гибридных угроз:

- технологизация и дистанционность преступных посягательств (массовое применение БПЛА, вредоносного ПО, кибератак);
- вовлечение уязвимых категорий населения (эффект «прокси-акторов») с корыстной, а не идеологической мотивацией;
- сращивание информационно-психологического воздействия с уголовно-наказуемыми деяниями, при котором ИПВ становится самостоятельным инструментом дестабилизации.

3. Эмпирически подтверждена корреляция между внешнеполитической динамикой 2022–2026 гг. и изменением структуры преступности. На фоне общего снижения регистрируемой преступности наблюдается устойчивый рост тяжких и особо тяжких деяний, диверсионно-террористической активности и вовлечения несовершеннолетних. Приграничные регионы, и прежде всего Белгородская область, выступают в качестве естественных криминологических полигонов, где эффекты гибридного воздействия проявляются наиболее отчетливо и где фиксируется рост латентной преступности, не находящей адекватной уголовно-правовой оценки.

4. Классические институты уголовного права – соучастие, вина, объективная сторона, квалифицирующие признаки – демонстрируют недостаточную эффективность при квалификации деяний, совершаемых в условиях внешнего дистанционного управления. Отсутствие механизмов учета такого управления порождает «правоприменительный паралич» в «серых зонах», когда деяние объективно обладает высокой общественной опасностью, но не может быть квалифицировано в полном объеме из-за невозможности доказать специальную цель, установить организатора или разграничить смежные составы.

5. Разрешение выявленных проблем требует не столько введения новых составов преступлений, сколько пересмотра подходов к квалификации в условиях гибридного противоборства. Необходимы:

○ законодательное закрепление отягчающих обстоятельств, учитывающих технологические способы совершения преступлений;

○ расширение диспозиций существующих норм для охвата кибердиверсий и иных форм дистанционного воздействия;

○ судебное толкование ключевых институтов Общей части УК РФ применительно к «серым зонам»;

○ совершенствование профилактической работы с уязвимыми категориями населения и реабилитация ветеранов боевых действий.

На основе проведенного анализа предлагается комплекс мер, направленных на повышение эффективности противодействия преступности, детерминированной гибридными угрозами.

I. Изменения в Уголовный кодекс Российской Федерации

1. Дополнить статью 63 УК РФ «Обстоятельства, отягчающие наказание» новым пунктом:

«т) совершение преступления с использованием беспилотных летательных аппаратов, роботизированных систем или иных автономных устройств, а равно с использованием программно-аппаратных средств, обеспечивающих дистанционное управление такими устройствами».

Данная норма позволит суду учитывать повышенную общественную опасность деяний, совершенных с использованием высокотехнологичных средств, без необходимости введения квалифицирующих признаков в каждую статью Особенной части УК РФ, что соответствует принципу экономии уголовной репрессии.

2. Дополнить статью 63 УК РФ новым пунктом:

«у) совершение преступления по заданию иностранного государства, международной организации или их представителей, а равно по указанию лиц, действующих в их интересах».

Данное отягчающее обстоятельство позволит дифференцировать ответственность исполнителей, действующих под внешним управлением, и учесть межгосударственный характер угрозы без необходимости доказывания идеологической мотивации.

3. Изложить часть 1 статьи 281 УК РФ в следующей редакции:

«1. Совершение взрыва, поджога или иных действий, направленных на разрушение или повреждение предприятий, сооружений, объектов транспортной инфраструктуры и транспортных средств, средств связи, объектов жизнеобеспечения населения, критической информационной инфраструктуры, а также иных объектов, имеющих стратегическое значение для экономической безопасности и обороноспособности Российской Федерации, в целях подрыва экономической безопасности и обороноспособности Российской Федерации, а равно совершение указанных действий дистанционно, в том числе с использованием информационно-телекоммуникационных сетей, программно-аппаратных средств или беспилотных летательных аппаратов, – наказывается…».

Расширение предмета преступления за счет критической информационной инфраструктуры и включение дистанционных способов совершения (кибердиверсии, атаки с использованием БПЛА) устраняет пробел, выявленный в ходе анализа правоприменительной практики.

4. Внести изменения в статью 281.1 УК РФ, исключив из диспозиции альтернативные действия, не имеющие самостоятельного криминообразующего значения, и уточнив критерии пособничества.

Существующая конструкция ст. 281.1 УК РФ «перегружена» альтернативными действиями, что создает сложности в доказывании и разграничении с общей нормой о пособничестве (ч. 5 ст. 33 УК РФ). Целесообразно сократить число альтернативных деяний до системообразующих (склонение, вербовка, финансирование) и дать легальное определение «содействия» через критерии осведомленности о диверсионном характере деятельности.

II. Разъяснения Пленума Верховного Суда Российской Федерации.

Предлагается разработать и принять постановление Пленума Верховного Суда РФ «О некоторых вопросах квалификации преступлений, совершаемых в условиях гибридного противоборства» (либо включить соответствующие разъяснения в уже существующие постановления по смежным категориям дел).

В указанном постановлении целесообразно отразить следующие позиции:

1. О квалификации диверсионных преступлений, совершенных с использованием БПЛА. Разъяснить, что применение беспилотных летательных аппаратов для поражения объектов, перечисленных в ст. 281 УК РФ, квалифицируется как диверсия при доказанности специальной цели, независимо от способа доставки поражающего элемента. При этом само управление БПЛА не требует дополнительной квалификации по ст. 271.1 УК РФ, если оно охватывалось умыслом на диверсию (по принципу поглощения).

2. О доказательственном значении специальной цели при диверсии. Разъяснить, что специальная цель подрыва экономической безопасности и обороноспособности может устанавливаться не только на основании прямых доказательств (инструктаж, переписка с куратором), но и на основании совокупности косвенных признаков: выбор объекта, способ его повреждения, связь с внешними источниками финансирования, политический контекст, – при этом корыстная мотивация исполнителя не исключает наличия указанной цели, если он осознавал или должен был осознавать, что его действия направлены на подрыв безопасности государства.

3. Об особенностях соучастия при дистанционном управлении. Разъяснить, что при совершении преступления по заданию неустановленного лица, находящегося за пределами РФ, исполнитель может нести ответственность как за оконченное преступление (при наличии всех признаков состава), а организатор (куратор) — подлежит уголовному преследованию по правилам ч. 3 ст. 33 УК РФ, если его личность установлена; при невозможности установления организатора квалификация действий исполнителя не исключается.

4. О разграничении ст. 280 и 282 УК РФ в условиях информационно-психологического воздействия. Дать критерии разграничения: если контент содержит прямые призывы к конкретным действиям (поджоги, насилие, блокировка дорог) — квалифицировать по ст. 280 УК РФ; если контент направлен на формирование негативных установок в отношении социальной группы без прямых призывов к действиям — по ст. 282 УК РФ; при наличии обоих признаков — по совокупности.

5. Об отнесении БПЛА к предметам преступлений. Разъяснить, что беспилотный летательный аппарат, имеющий стоимость и обладающий признаками движимого имущества, может быть предметом хищения (ст. 158–162 УК РФ) и угона (ст. 166 УК РФ) при условии, что он не является средством совершения более тяжкого преступления; при использовании БПЛА для совершения диверсии или теракта квалификация по ст. 166 УК РФ не требуется.

III. Организационные и профилактические меры. Помимо законодательных изменений, в статье может быть отражен краткий перечень мер, не требующих изменения УК, но повышающих эффективность противодействия:

- Усиление контроля за оборотом комплектующих БПЛА (внесение изменений в подзаконные акты о лицензировании импорта и продажи компонентов, создание единой базы данных о лицах, прошедших обучение управлению БПЛА в зоне боевых действий).

- Профилактическая работа с населением (разработка и внедрение образовательных программ для школ и вузов о методах вербовки через интернет-мессенджеры, создание горячих линий для сообщения о попытках вовлечения в диверсионную деятельность).

- Реабилитация ветеранов боевых действий (разработка государственной программы психологической и социальной адаптации для военнослужащих, возвращающихся из зоны СВО, включая их трудоустройство и вовлечение в гражданские профессии, связанные с управлением БПЛА (например, в аграрном секторе, мониторинге инфраструктуры), что позволит легализовать полученные навыки и снизить криминогенные риски).

Комплекс предложенных мер — от изменений в Общей и Особенной частях УК РФ до судебного толкования и организационных решений — направлен на преодоление «правоприменительного паралича» в «серых зонах» и адаптацию уголовно-правовой системы к новым реалиям гибридного противоборства. Только синтез законодательных, правоприменительных и криминологических подходов позволит снизить уровень угроз, связанных с гибридными формами противостояния, и предотвратить их дальнейшую трансформацию в еще более опасные формы.

Литература

1. Безопасная Европа: Противодействие гибридным угрозам // [Электронный ресурс]. Режим доступа: https://www.eeas.europa.eu/node/46393_ru (дата обращения: 15.06.2026).

2. В ФСБ раскрыли, как Telegram и WhatsApp стали ловушкой для россиян // News.ru. 23.08.2025. [Электронный ресурс]. Режим доступа: https://news.ru/russia/fsb-ukraina-pytaetsya-vovlech-rossiyan-v-diversii-cherez-telegram-i-whatsapp/ (дата обращения: 20.06.2026).

3. Воздушный кодекс Российской Федерации от 19 марта 1996 г. № 60-ФЗ (ред. от 28.11.2025) // Собрание законодательства РФ. – 1996. – № 12. – Ст. 1383.

4. Голоскоков Л. В. Уголовное право и гибридные войны // Журнал прикладных исследований. – 2020. – № 4. – С. 52–57.

5. Дозорцева Е. Г., Бадмаева В. Д., Кастальская-Бороздина А. А., Федонкина А. А., Чибисова И. А. Клинико-психологические характеристики подростков, совершивших диверсионные действия. // *Психология и право, 16*(1). – 2026. – С. 83–101.

6. Зеленова Д. А., Романов С. А. Гибридные угрозы» и национальная безопасность Российской Федерации // Право и государство: теория и практика. – 2025. – № 6. – С. 207–209.

7. О Стратегии научно-технологического развития Российской Федерации: указ Президента РФ от 28 февраля 2024 г. № 145 // Собрание законодательства РФ. – 2024. – Т. 1373, № 145. – С. Ст. 1373.

8. О Стратегии национальной безопасности Российской Федерации: указ Президента РФ от 02 июля 2021 г. № 400 // Собрание законодательства 9. РФ. – 2021. – Т. 5351, № 400. – С. Ст. 5351.

9. Официальный сайт МВД РФ. Раздел: Статистика и аналитика. / [Электронный ресурс]. Режим доступа: https://xn--b1aew.xn--p1ai/dejatelnost/statistic / (дата обращения 11.07.2026).

10. Романовский Г. Б. Право, гибридные угрозы и борьба с терроризмом // Академический юридический журнал. – 2022. – Т. 23, № 1. – С. 21–29.

11. Стратегическая концепция НАТО 2022 года. Принята главами государств и правительств на встрече в верхах НАТО в Мадриде 29 июня 2022 г. / [Электронный ресурс]. Режим доступа: https://www.nato.int/content/dam/nato/webready/documents/publications-and-reports/strategic-concepts/2022/290622-strategic-concept-ru.pdf (дата обращения: 11.07.2026).

12. Удары ВСУ по объектам России. Аналитический бюллетень. // КЦПН: Аналитический центр. – 2026. [Электронный ресурс]. Режим доступа: https://kcpn.info/articles/strike-vsu/?ysclid=msc6c7csry952292738 (дата обращения: 11.07.2026).

13. Федоров А.В. Гибридные угрозы – новый вызов или жупел постдемократии? (западный дискурс) // Полилог/Polylogos. – 2022. – Т. 6. – № 4. [Электронный ресурс]. Режим доступа: https://polylogos-journal.ru/s258770110023746-2-1/ (дата обращения: 11.07.2026).

14. Hoffman F. Conflict in the 21st Century: The Rise of Hybrid Wars. – Arlington: Potomac Institute for Policy Studies. – 2007. – 72 p.

Hybrid threats as a factor in the transformation of modern crime: criminal law and criminological aspects of counteraction

Savel'eva I.V.

Belgorod State National Research University

The article is devoted to the topic of the transformation of modern crime in the Russian Federation under the influence of hybrid threats. Special attention is paid to the change in criminal determination, in which crime acquires the features of an instrument of interstate confrontation, and classical institutions of criminal law (complicity, guilt, qualifying signs) are not effective enough in the conditions of «gray zones». The purpose of the study is to develop a theoretical model for improving the criminal law and criminological tools for countering crimes committed in the context of hybrid conflicts. The methods include dialectical, systematic, formal-legal, comparative-legal, statistical analysis and the method of expert assessments. Results: three systemic trends have been identified – the technologization and remoteness of attacks (mass use of UAVs, cyber attacks), the involvement of vulnerable groups of the population (the effect of «proxy actors») and the merging of information and psychological effects with criminally punishable acts. The phenomenon of «law enforcement paralysis» in the qualification of acts under conditions of external remote control is substantiated. Conclusions: a set of legislative amendments has been proposed (addition of new aggravating circumstances to Article 63 of the Criminal Code of the Russian Federation, extension of art. 281 of the Criminal Code of the Russian Federation) and the development of a resolution of the Plenum of the Supreme Court of the Russian Federation, as well as organizational and preventive measures.

Keywords: hybrid threats, crime transformation, sabotage, unmanned aerial vehicles, informational and psychological impact, criminal law qualification, law enforcement paralysis, proxy actors, gray zone, counteraction.

References

1. Secure Europe: Countering hybrid threats. // [Electronic resource]. Access mode: URL: https://www.eeas.europa.eu/node/46393_ru. (date of appeal: 06/15/2026).

2. The FSB revealed how Telegram and WhatsApp became a trap for Russians // News.ru. 08/23/2025. // [Electronic resource]. Access mode: URL: https://news.ru/russia/fsb-ukraina-pytaetsya-vovlech-rossiyan-v-diversii-cherez-telegram-i-whatsapp. / (date of reference: 06/20/2026).

3. The Air Code of the Russian Federation dated March 19, 1996, No. 60-FZ (as amended on 11/28/2025) // Collection of Legislation of the Russian Federation. – 1996. – T. 1383, № 60. – P. Ст. 1383.

4. Goloskokov L.V. Criminal law and hybrid wars // Journal of Applied Research. – 2020. – № 4. – P. 52–57.

5. Dozortseva E. G., Badmaeva V. D. Kastalskaya-Borozdina A. A., Fedonkina A. A., Chibisova I. A. Clinical and psychological characteristics of adolescents who committed acts of sabotage // Psychology and Law, 16(1). – 2026. – P. 83–101.

6. Zelenova D. A., Romanov S. A. Hybrid threats and national security of the Russian Federation // Law and the State: theory and practice. – 2025. – № 6. – P. 207–209.

7. On the Strategy of Scientific and Technological Development of the Russian Federation: Decree of the President of the Russian Federation No. 145 dated February 28, 2024 // Collection of Legislation of the Russian Federation. – 2024. – T. 1373, № 145. – P. C. 1373.

8. On the National Security Strategy of the Russian Federation: Decree of the President of the Russian Federation No. 400 dated July 02, 2021 // Collection of legislation of the Russian Federation. – 2021. – T. 5351, № 400. – P. C. 5351.

9. Official website of the Ministry of Internal Affairs of the Russian Federation. Chapter: Statistics and analytics. / [Electronic resource]. Access mode: RL: https://xn--b1aew.xn--p1ai/dejatelnost/statistic (date of reference: 07/11/2026).

10. Romanovsky G.B. Law, hybrid threats and the fight against terrorism // Academic Law Journal. – 2022. – № 1. – P. 21–29.

11. The NATO Strategic Concept of 2022. Adopted by the heads of State and Government at the NATO Summit in Madrid on June 29, 2022. // [Electronic resource]. Access mode: URL: https://www.nato.int/content/dam/nato/webready/documents/publications-and-reports/strategic-concepts/2022/290622-strategic-concept-ru.pdf. (date of reference: 07/11/2026).

12. Attacks by the Ukrainian Armed Forces on Russian targets. / Analytical bulletin. / KTSPN: Analytical Center. 2026. // [Electronic resource]. Access mode: URL: https://kcpn.info/articles/strike-vsu/?ysclid=msc6c7csry952292738 (date of reference: 07/11/2026).

13. Fedorov A.V. Hybrid threats – a new challenge or the bogey of post-democracy? (Western discourse) // Polylogos/Polylogos. – 2022. – № 4. // [Electronic resource]. Access mode: URL: https://polylogos-journal.ru/s258770110023746-2-1/(date of reference: 07/11/2026).

14. Hoffman F. Conflict in the 21st Century: The Rise of Hybrid Wars. – Arlington: Potomac Institute for Policy Studies. – 2007. – 72 p.