Дата поступления рукописи в редакцию: 04.10.2026 г. DOI: 10.24412/2224-9133-2026-10-577-582
Дата принятия рукописи в печать: 10.11.2026 г.

ПИЛЮГИНА Юлия Геннадиевна,
доцент кафедры специальных дисциплин
Краснодарского университета МВД России,
кандидат философских наук,
e-mail: pilyugina81@bk.ru

ВОВЛЕЧЕНИЕ НЕСОВЕРШЕННОЛЕТНИХ В ТЕРРОРИСТИЧЕСКУЮ И ДИВЕРСИОННУЮ ДЕЯТЕЛЬНОСТЬ ПОСРЕДСТВОМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ: УГОЛОВНО-ПРАВОВЫЕ И КРИМИНОЛОГИЧЕСКИЕ ПРОБЛЕМЫ

Аннотация. *В статье исследуются уголовно-правовые и криминологические проблемы вовлечения несовершеннолетних в террористическую и диверсионную деятельность посредством информационно-телекоммуникационных сетей. Анализируются изменения, внесенные Федеральным законом от 17 ноября 2025 г. № 420-ФЗ, двойственный статус несовершеннолетнего как объекта преступного воздействия и возможного субъекта уголовной ответственности, разграничение террористической и диверсионной направленности, а также особенности ступенчатой цифровой вербовки. Предлагается трехэлементный критерий квалификации цифрового вовлечения: адресность воздействия, преступная направленность коммуникации и самостоятельное установление субъективной стороны каждого участника. Формулируются предложения по судебному толкованию и профилактике.*

Ключевые слова: *несовершеннолетние, терроризм, диверсия, содействие террористической деятельности, содействие диверсионной деятельности, вербовка, вовлечение, информационно-телекоммуникационные сети, социальная инженерия, уголовная ответственность, профилактика.*

Для цитирования: *Пилюгина Ю. Г. Вовлечение несовершеннолетних в террористическую и диверсионную деятельность посредством информационно-телекоммуникационных сетей: уголовно-правовые и криминологические проблемы // Право и управление. 2026. № 10. С. 577–582.*

PILYUGINA Yulia Gennadievna,
Associate Professor of the Department of Special Disciplines of the Krasnodar University of the Ministry of Internal Affairs of Russia, Candidate of Philosophical Sciences

INVOLVEMENT OF MINORS IN TERRORIST AND SABOTAGE ACTIVITIES THROUGH INFORMATION AND TELECOMMUNICATION NETWORKS: CRIMINAL LAW AND CRIMINOLOGICAL PROBLEMS

Annotation. *The article examines criminal-law and criminological problems of involving minors in terrorist and sabotage activities through information and telecommunication networks. It analyzes the amendments introduced by Federal Law No. 420-FZ of November 17, 2025, the dual position of a minor as both the object of criminal influence and a possible offender, the distinction between terrorist and sabotage purposes and staged digital recruitment. A three-element test is proposed: individualized targeting, criminal orientation of communication and separate assessment of the mental element of each participant. Proposals are formulated for judicial interpretation and prevention.*

Key words: *minors, terrorism, sabotage, recruitment, involvement, terrorist activity, sabotage activity, information and telecommunication networks, social engineering, criminal liability, prevention.*

For citation: *Pilyugina Yu. G. Involvement of minors in terrorist and sabotage activities through information and telecommunication networks: criminal law and criminological problems. Law and administration. 2026;(10):577–582. (In Russ.).*

Вовлечение несовершеннолетних в террористическую и диверсионную деятельность посредством информационно-телекоммуникационных сетей представляет собой одну из наиболее опасных форм современной преступной активности, поскольку цифровая среда используется не только как канал связи, но и как самостоятельный механизм поиска потенциального исполнителя, установления доверительного контакта, постепенного изменения мотивации, передачи инструкций, контроля выполнения задания и получения отчета. Для подростка же первоначальное взаимодействие может выглядеть как обычное знакомство, предложение подработки, участие в игре, просьба выполнить несложное поручение или обсуждение общественно значимой темы, а уже по мере закрепления контакта действия усложняются, убеждение способно сочетаться с обещанием вознаграждения, манипуляцией, шантажом или угрозой и в результате традиционная вербовка дополняется цифровой социальной инженерией, что требует одновременного уголовно-правового и криминологического анализа [1; 5].

На наш взгляд уголовно-правовая актуальность темы существенно возросла после принятия Федерального закона от 17 ноября 2025 г. № 420-ФЗ, которым законодатель усилил ответственность за содействие террористической и диверсионной деятельности в отношении несовершеннолетнего и расширил перечень преступлений, за совершение которых уголовная ответственность наступает с четырнадцати лет. В этот перечень были включены, в частности, содействие террористической деятельности, отдельные преступления, связанные с террористическими организациями и сообществами, диверсия, содействие диверсионной деятельности, прохождение обучения в целях осуществления диверсионной деятельности и участие в диверсионном сообществе. При этом отметим, что новая конструкция имеет двойственную направленность, а именно несовершеннолетний получает повышенную уголовно-правовую защиту от вербовщика и одновременно в большем числе случаев может сам выступать субъектом ответственности за последующее общественно опасное поведение.

Такая двойственность, несомненно, имеет принципиальное значение для квалификации, поскольку один и тот же подросток в конкретной преступной ситуации способен быть лицом, в отношении которого осуществлялись склонение, вербовка или иное вовлечение, и одновременно субъектом совершенного им преступления. Необходимо отметить, что данные статусы не исключают друг друга, повышенная ответственность взрослого вербовщика обусловлена возрастной уязвимостью объекта воздействия, тогда как ответственность самого несовершеннолетнего зависит от достижения установленного возраста, вменяемости, фактической способности осознавать характер поведения и содержания его собственного умысла. Поэтому последующее привлечение подростка к ответственности за диверсию или террористическое преступление не устраняет квалифицирующий признак совершения вербовщиком соответствующего деяния в отношении несовершеннолетнего, тогда как иное решение лишало бы усиленной защиты именно тех подростков, преступное вовлечение которых оказалось результативным.

По нашему мнению, для правильного применения ст. 205.1 и 281.1 УК РФ необходимо учитывать содержание понятий «склонение», «вербовка» и «иное вовлечение». Так судебное толкование террористических составов исходит из того, что такие действия могут выражаться в уговорах, убеждении, предложениях, подкупе, угрозах, поиске лиц, распространении адресованных им материалов и иных формах воздействия, направленных на вовлечение в определенную преступную деятельность. Для цифровой же среды особенно важно, что уголовно-правовое значение имеет не физический контакт, а целенаправленность коммуникации, когда одно прямое сообщение с предложением совершить поджог и продолжительная цепочка внешне нейтральных заданий способны обладать одинаковой конечной направленностью, если доказано стремление сформировать у несовершеннолетнего решение участвовать в соответствующем преступлении [7].

При этом, несомненно, нельзя смешивать индивидуальное вовлечение с распространением опасного контента неопределенному кругу лиц, так как публичное оправдание терроризма, призыв к противоправной деятельности и адресная вербовка различаются по юридической природе и признакам состава. Одновременно для ст. 205.1 и 281.1 УК РФ принципиально установить направленность действий на конкретное лицо либо определенную группу лиц, что может подтверждаться индивидуальной перепиской, передачей координат объекта, согласованием вознаграждения, выдачей инструкций, требованием фото- или видеоотчета, контролем передвижения и созданием закрытого канала связи. Хотя сам факт подписки несовершеннолетнего на деструктив-

ный ресурс или просмотра им противоправного материала не позволяет автоматически признать администратора ресурса его вербовщиком без установления дополнительных действий, направленных именно на данного подростка.

Особое значение имеет разграничение террористической и диверсионной направленности, где внешняя форма поведения может совпадать, к примеру, поджог, взрыв, повреждение транспорта, средств связи, энергетического или иного объекта. Однако уголовно-правовая квалификация определяется не бытовым обозначением действия, а всеми признаками конкретного состава, включая специальную цель. Так для диверсии закон связывает ответственность с направленностью на подрыв экономической безопасности и (или) обороноспособности Российской Федерации, террористический акт характеризуется иными обязательными целями, связанными с дестабилизацией деятельности органов власти или международных организаций либо воздействием на принятие ими решений. Следовательно, при оценке дистанционной вербовки необходимо установить, в какое именно преступление инициатор намеревался вовлечь несовершеннолетнего и какой характер предполагаемого посягательства охватывался его умыслом.

Сложнее ситуация, когда подростку раскрывается только бытовая сторона задания, ему могут предложить за вознаграждение поджечь технический объект, утверждая, что речь идет о споре хозяйствующих субъектов, проверке охраны или обычном повреждении имущества. В таких случаях для ответственности вербовщика по ст. 281.1 УК РФ при наличии остальных признаков достаточно его собственного умысла на вовлечение в диверсионную деятельность, фактическое доведение замысла до конца не требуется для признания соответствующей формы содействия оконченной. Однако действия несовершеннолетнего должны оцениваться самостоятельно, нельзя выводить его осознание специальной диверсионной цели только из свойств объекта или умысла куратора, иначе ответственность подростка будет фактически основана на объективном вменении.

Отметим так же и тот факт, что цифровое вовлечение нередко имеет ступенчатый характер, когда на первом этапе подростку предлагается действие, которое само по себе может выглядеть социально нейтральным, сфотографировать объект, проверить адрес, передать сообщение, приобрести предмет, перевести небольшую сумму. Затем формируется привычка выполнять задания, вводятся материальное вознаграждение и правила конспирации, после чего следует поручение, имеющее уже очевидный преступный характер. Очевидно, что такая модель позволяет вербовщику одновременно проверить управляемость лица и снизить его психологический барьер, вот почему для правовой оценки нельзя искусственно изолировать последнее сообщение от предыдущей коммуникации, совокупность действий здесь может образовывать единый процесс вовлечения, если она подчинена общей цели включения подростка в террористическую или диверсионную деятельность.

Криминологически данный механизм опирается на свойства цифровой среды, такие как возможность сохранять анонимность, быстро менять аккаунты, одновременно взаимодействовать со значительным числом потенциальных исполнителей, изучать открытые сведения об их интересах и уязвимостях, использовать автоматический перевод и персонализированный контент. В исследованиях преступности несовершеннолетних отмечается возрастающее значение социальных сетей, мессенджеров и цифровых следов для предупреждения и выявления противоправного поведения [2; 3; 4]. При этом профилактическая работа с несовершеннолетними и преступлениями, совершаемыми ими и в их отношении, традиционно является самостоятельным направлением деятельности органов внутренних дел. Соответствующие меры рассматривались, в частности, В. В. Шанько и А. В. Мацко применительно к практике территориального органа МВД [6, с. 172-175] и, несомненно, в современных условиях такая профилактика неизбежно должна учитывать цифровой канал преступного воздействия.

Считаем, что снижение возраста уголовной ответственности до четырнадцати лет повышает значение ч. 3 ст. 20 УК РФ, поскольку достижение формального возраста не освобождает следствие и суд от обязанности установить, мог ли конкретный несовершеннолетний вследствие уровня психического развития в полной мере осознавать фактический характер и общественную опасность поведения либо руководить им. Дистанционная вербовка в этом контексте способна специально эксплуатировать возрастную внушаемость, потребность в признании, дефицит жизненного опыта, зависимость от оценки группы, стремление к быстрому заработку или страх разглашения личной информации. Такие обстоятельства сами по себе не означают отставания в психическом развитии и не исключают ответственности, но они должны учитываться при установлении субъективной стороны и при назначении наказания.

Необходимо так же различать понимание фактического характера действия и осознание специальных уголовно-правовых признаков, так как подросток обычно способен понимать физические последствия поджога или взрыва, однако это еще не доказывает осознание цели подрыва экономической безопасности или обороноспо-

собности страны. Аналогично согласие передать сведения, сфотографировать объект или получить деньги не всегда свидетельствует о понимании участия в террористическом сообществе либо содействии терроризму. Вот почему в делах о дистанционном вовлечении центральным предметом доказывания становится содержание коммуникации, а именно какие сведения о цели передавал куратор, как подросток реагировал на них, какие вопросы задавал, что обсуждалось после выполнения задания и какие меры конспирации предпринимались.

В цифровой среде, несомненно, особую роль приобретают электронные доказательства, значимыми могут быть содержание и последовательность переписки, история изменения имен и аккаунтов, метаданные файлов, сведения о передаче координат и изображений, движение денежных средств, данные о попытках удалить сообщения, цифровые следы использования нескольких устройств. Однако, здесь необходимо обратить внимание на тот факт, что отдельный цифровой фрагмент не должен оцениваться вне контекста, так, к примеру, фраза о «работе», «задании» или «объекте» может иметь различное значение в зависимости от предыдущего общения. Следовательно, доказательственная модель должна восстанавливать весь процесс формирования преступного решения, а не только фиксировать конечное противоправное действие, что особенно важно, когда защита ссылается на введение несовершеннолетнего в заблуждение относительно реального назначения поручения.

В связи с чем, мы считаем, что для практики целесообразно использовать трехэлементный критерий цифрового вовлечения. Первый элемент - это адресность, когда необходимо доказать, что воздействие направлено на определенного несовершеннолетнего либо индивидуализированную группу. Второй — преступная направленность, а именно содержание коммуникации в совокупности должно свидетельствовать о цели включить лицо в конкретную террористическую или диверсионную деятельность. И третий это субъективная дифференциация, когда умысел вербовщика и умысел вовлекаемого устанавливаются отдельно, без автоматического переноса знания одного лица на другое. Такой подход позволит одинаково избежать как неоправданного расширения ст. 205.1 и 281.1 УК РФ, так и недооценки сложных многоэтапных схем, в которых прямое преступное предложение появляется только на завершающей стадии.

Представляется необходимым так же уточнение судебных разъяснений. Во-первых, следует прямо указать, что склонение, вербовка и иное вовлечение могут полностью осуществляться посредством информационно-телекоммуникационных сетей и не требуют личной встречи. Во-вторых, повышенная ответственность за деяние в отношении несовершеннолетнего должна применяться независимо от того, совершил ли подросток последующее преступление и подлежит ли он за него уголовной ответственности. В-третьих, разграничение террористической и диверсионной направленности следует проводить по содержанию преступной цели, а не только по виду объекта воздействия. В-четвертых, последовательность внешне нейтральных микрозаданий может оцениваться как единый процесс вовлечения, если доказана их общая преступная направленность. И, в-пятых, при квалификации действий самого несовершеннолетнего необходимо отдельно устанавливать осознание им специальных признаков соответствующего состава.

Уголовно-правовое воздействие, несомненно, должно дополняться профилактикой, поскольку наказание реагирует уже на сформировавшуюся опасную ситуацию, эффективная модель предполагает взаимодействие органов внутренних дел, подразделений по делам несовершеннолетних, образовательных организаций, органов системы профилактики и цифровых платформ в пределах установленных законом полномочий. Приоритетными нам представляются обучение подростков распознаванию типовых приемов социальной инженерии, понятные способы безопасного сообщения о попытках вербовки, быстрое сохранение цифровых следов после такого обращения, адресная работа с лицами группы риска и информирование родителей и педагогов. В этом контексте профилактический материал должен объяснять не только суровость ответственности, но и сам сценарий вовлечения, то есть обещание легкого заработка, просьбу сохранить тайну, переход в закрытый мессенджер, постепенное усложнение поручений, получение компрометирующей информации и угрозы после выполнения первого задания.

Вопрос о моменте окончания вовлечения также нуждается в единообразном понимании, поскольку для квалификации действий вербовщика принципиально не то, согласился ли несовершеннолетний выполнить задание, а направленность совершенных действий на формирование соответствующего преступного решения. К примеру, если закон признает склонение или вербовку оконченными с момента самого воздействия, последующий отказ подростка либо пресечение коммуникации не устраняют уже содеянного, хотя это и не означает, что любое неудачное общение является оконченным преступлением, необходимо доказать, что действия объективно были обращены к вовлечению в предусмотренную законом преступную деятельность. Общая политическая дискуссия, провокационная реплика или неопре-

деленное предложение без связи с конкретным преступным поведением должны отграничиваться от целенаправленной вербовки.

Не менее важным нам представляется правильно оценивать роль совершеннолетнего посредника, который не общается с несовершеннолетним непосредственно, но передает его данные куратору, предоставляет средства связи, денежные средства или иным образом обеспечивает вовлечение. Поскольку такая деятельность может получать оценку по правилам соучастия, если доказано понимание характера основного преступления и желание содействовать ему. Однако сам факт знакомства с подростком либо передачи его контакта не позволяет автоматически выводить умысел на террористическое или диверсионное вовлечение, здесь вновь действует общий принцип, когда технологическая и организационная связь должна дополняться психической связью между участниками. Для цифровых же схем это особенно актуально, поскольку коммуникация часто распределена между несколькими аккаунтами и лицами.

Криминологическая профилактика должна учитывать и различие между универсальными и адресными мерами, когда универсальный уровень охватывает правовое просвещение, цифровую грамотность и информирование о способах манипуляции, адресный уровень необходим, когда выявлены конкретные признаки вовлечения, резкое появление необъяснимых денежных поступлений, секретность новых онлайн-контактов, получение заданий, связанных с объектами инфраструктуры, требование удалять переписку или скрывать маршрут. При этом отметим, что такие признаки не являются доказательством преступления и не должны вести к стигматизации подростка, но могут служить основанием для своевременной профилактической беседы и проверки обстоятельств уполномоченными органами в законных пределах. То есть мы видим, что эффективная профилактика тем самым сочетает безопасность с уважением частной жизни несовершеннолетнего.

Отдельное значение имеет реабилитационный компонент, поскольку несовершеннолетний, который оказался объектом вербовки, но своевременно отказался от исполнения поручения или сообщил о происходящем взрослым и правоохранительным органам, должен воспринимать обращение за помощью как безопасный и социально одобряемый выбор. Чрезмерно репрессивная публичная риторика здесь способна, напротив, усиливать зависимость подростка от куратора, если он уверен, что после первого контакта уже неизбежно будет наказан, в связи с чем профилактическая коммуникация должна четко объяснять различие между фактом получения опасного предложения, добровольным отказом от него и сознательным участием в преступлении. По нашему мнению, такой подход создает дополнительные условия для раннего пресечения вовлечения до причинения вреда.

Так же мы считаем, что следует учитывать и межотраслевое значение проблемы, поскольку установление уголовной ответственности не может подменять меры, предусмотренные законодательством о профилактике безнадзорности и правонарушений несовершеннолетних, об образовании и об информации. Так, после выявления попытки вовлечения необходимо не только пресечь конкретную коммуникацию, но и устранить условия, которые сделали подростка уязвимым, такие как социальная изоляция, конфликт в семье или образовательной среде, долговая зависимость, вовлечение в закрытые онлайн-сообщества. В противном случае блокирование одного аккаунта лишь временно разрывает контакт, не снижая вероятность повторной вербовки другим лицом, поэтому уголовно-правовая защита становится эффективнее, когда включена в систему индивидуальной профилактики, а не рассматривается как единственный инструмент реагирования.

В научном же плане дальнейшее исследование должно быть ориентировано на накопление обезличенных данных о способах цифрового вовлечения, возрасте и мотивации несовершеннолетних, формах обмана и характере их осведомленности о конечной цели. Поскольку без такой эмпирической базы существует риск строить уголовную политику на наиболее резонансных случаях, не отражающих всю структуру явления, ведь для выработки устойчивых рекомендаций необходимы сопоставление судебных решений, анализ прекращенных дел, материалов профилактического учета и результатов психологических исследований, что позволит точнее определить, какие признаки действительно свидетельствуют о сформированном преступном умысле подростка, а какие характеризуют прежде всего его уязвимость перед манипулятивным воздействием.

Таким образом, мы видим, что цифровая вербовка несовершеннолетних требует сочетания строгой уголовно-правовой оценки и индивидуализированного подхода к самому подростку. Новеллы 2025 г., несомненно, усилили охрану несовершеннолетнего и расширили его собственную ответственность, что делает особенно важным разграничение умысла вербовщика и вовлекаемого. И, предлагаемый нами трехэлементный критерий — адресность воздействия, преступная направленность коммуникации и самостоятельное установление субъективной стороны каждого участника — позволяет учитывать специфику многоэтапной социальной инженерии и одновременно сохранять действие принципа вины. Прак-

тическая задача же состоит не в дальнейшем механическом расширении санкций, а в формировании единообразных правил квалификации, доказательственных стандартов и ранней профилактики цифрового вовлечения.

Список литературы:

[1] Легушенко Д. А. Вовлечение несовершеннолетних в террористическую деятельность как элемент механизма совершения преступления // Вестник Калининградского филиала Санкт-Петербургского университета МВД России. 2025. № 3. С. 72-78.

[2] Горковенко И. А. Цифровая трансформация оперативно-разыскного противодействия органов внутренних дел преступности несовершеннолетних // Вестник Калининградского филиала Санкт-Петербургского университета МВД России. 2026. № 1 (83). С. 55-63.

[3] Букалерова Л. А., Остроушко А. В., Криез О. Преступления против информационной безопасности несовершеннолетних, совершаемые посредством информационно-телекоммуникационных сетей (включая сеть Интернет) // Вестник Санкт-Петербургского университета. Право. 2021. Т. 12. № 1. С. 17-35.

[4] Лебедева В. С. Влияние социальных медиа на формирование преступного поведения несовершеннолетних // Вопросы российской юстиции. 2024. Вып. 31. С. 310-319.

[5] Гайворонская И. Б., Фомина Т. Ф., Аманжолова Б. А. Вербовка в экстремистские и террористические организации посредством сети Интернет // Психология и право. 2020. Т. 10. № 4. С. 152-165.

[6] Мацко А. В., Шанько В. В. О мерах, принимаемых ГУ МВД России по Ставропольскому краю, по профилактике преступлений, совершенных несовершеннолетними и в их отношении // Ставрополь - город межэтнического согласия и межконфессионального диалога: материалы ежегодной городской научно-практической конференции. 2014. С. 172-175.

[7] Кудрявцев В. Л. «Склонение, вербовка или иное вовлечение лица» как альтернативные действия объективной стороны содействия террористической деятельности // Адвокат. 2012. № 5. С. 21-25.

[8] Коркмазов А. В. Современные тенденции цифрового экстремизма и терроризма // Пробелы в российском законодательстве. 2023. Т. 16. № 4. С. 208-212. EDN PLMEVN.

References:

[1] Legushenko D.A. Involvement of minors in terrorist activities as an element of the mechanism for committing a crime // Bulletin of the Kaliningrad branch of the St. Petersburg University of the Ministry of Internal Affairs of Russia. 2025. № 3. S. 72-78.

[2] Gorkovenko I. A. Digital transformation of operational-search counteraction of juvenile crime bodies // Bulletin of the Kaliningrad branch of the St. Petersburg University of the Ministry of Internal Affairs of Russia. 2026. № 1 (83). S. 55-63.

[3] Bukalerova L. A., Ostroushko A. V., Kriez O. Crimes against the information security of minors committed through information and telecommunication networks (including the Internet) // Bulletin of St. Petersburg University. Right. 2021. VOL. 12. № 1. S. 17-35.

[4] Lebedeva V. S. Influence of social media on the formation of criminal behavior of minors // Issues of Russian justice. 2024. No. 31. S. 310-319.

[5] Gayvoronskaya I.B., Fomina T.F., Amanzholova B.A. Recruitment to extremist and terrorist organizations via the Internet // Psychology and Law. 2020. T. 10. № 4. S. 152-165.

[6] Matsko A.V., Shanko V.V. On the measures taken by the Main Directorate of the Ministry of Internal Affairs of Russia for the Stavropol Territory to prevent crimes committed by and against minors // Stavropol is a city of interethnic harmony and interfaith dialogue: materials of the annual city scientific and practical conference. 2014. S. 172-175.

[7] Kudryavtsev V. L. "Declination, recruitment or other involvement of a person" as alternative actions of the objective side of facilitating terrorist activities // Lawyer. 2012. № 5. S. 21-25.

[8] Korkmazov A. V. Current trends in digital extremism and terrorism // Gaps in Russian legislation. 2023. T. 16. № 4. S. 208-212. EDN PLMEVN.