

ПРАВООБРАЗОВАНИЕ И ПРАВОТВОРЧЕСТВО

Дата поступления рукописи в редакцию: 05.07.2026 г.

Дата принятия рукописи в печать: 23.08.2026 г.

ГОНЧАР Владимир Владимирович,

доцент кафедры информационных технологий и
организации расследования киберпреступлений
Московская академия Следственного комитета
Российской Федерации имени А.Я. Сухарева,
e-mail: vg0778@bk.ru

ПАСЮКОВ Сергей Эдуардович,

сотрудник УВД по САО г. Москвы,
e-mail: spasukov2@yandex.ru

НЕКОТОРЫЕ АСПЕКТЫ НОРМАТИВНО-ПРАВОВОГО РЕГУЛИРОВАНИЯ ПРОТИВОДЕЙСТВИЕ ПРЕСТУПЛЕНИЯМ, СОВЕРШАЕМЫМ В ПСЕВДОДОМЕННЫХ ЗОНАХ СЕТИ ИНТЕРНЕТ

Аннотация. В данной статье рассматриваются научные, организационные и практические подходы к нормативно-правовому регулированию противодействия преступлениям, совершаемым с использованием анонимных торговых площадок.

Ключевые слова: анонимные торговые площадки, псевдодоменная зона, зона .onion, сеть Tor, классификация анонимных торговых площадок, темный Интернет, нормативное регулирование борьбы с киберпреступлениями.

GONCHAR Vladimir Vladimirovich,

Associate Professor, Department of Information Technologies
and Organization of Cybercrime Investigations,
A.Ya. Sukharev Moscow Academy of the
Investigative Committee of the Russian Federation

PASYUKOV Sergey Eduardovich,

Officer, Directorate of Internal Affairs for the
Northern Administrative District of Moscow

CERTAIN ASPECTS OF REGULATORY AND LEGAL REGULATION OF COUNTERING CRIMES COMMITTED IN PSEUDODOMAIN AREAS OF THE INTERNET

Annotation. This article examines scientific, organizational, and practical approaches to the regulatory and legal regulation of countering crimes committed using anonymous marketplaces.

Key words: anonymous marketplaces, pseudo-domain zone, .onion zone, Tor network, classification of anonymous marketplaces, the dark web, regulatory framework for combating cybercrime.

Правовое регулирование деятельности, связанной с функционированием анонимных торговых площадок в зоне .onion, осуществляется в рамках общей системы законодательства об информации и уголовно-правовых норм. Конституция Российской Федерации гарантирует право на неприкосновенность частной жизни, тайну переписки и переговоров, однако данные гарантии

могут быть ограничены в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

Именно на этом конституционном балансе строится правоприменительная практика при проведении оперативно-розыскных мероприятий в отношении скрытых интернет-ресурсов.

Основной нормативный акт, определяющий статус информационных ресурсов и порядок обращения с ними - Федеральный закон от 27 июля 2006г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

Данный закон устанавливает принципы правового регулирования отношений в сфере информации, но не содержит прямых указаний на псевдодоменные зоны или оверлейные (наложенные) сети.

На практике ресурсы .onion относят к информационным системам и сайтам в сети Интернет, распространяя на них общие требования о блокировке противоправного контента, предоставлении информации владельцами ресурсов и взаимодействии с уполномоченными органами.

Федеральный закон от 7 июля 2003г. № 126-ФЗ «О связи» регулирует отношения в области оказания услуг связи, включая услуги передачи данных.

С точки зрения противодействия анонимным площадкам, нормативное значение имеют положения об обязанности операторов связи хранить трафик иметаданные, а также предоставлять их по запросам правоохранительных органов.

Архитектура Tor изначально проектировалась для обхода традиционных точек перехвата трафика, что создает техническое противоречие с законодательными требованиями к провайдерам. В результате стандартные механизмы контроля связи оказываются малоэффективными при работе с .onion-сервисами, что вынуждает искать альтернативные правовые основания для получения информации.

Федеральный закон от 12 августа 1995г. № 144-ФЗ «Об оперативно-розыскной деятельности». Статья 6 перечисляет мероприятия, которые могут проводиться в отношении лиц, подозреваемых в совершении преступлений с использованием анонимных площадок: наблюдение, контроль почтовых отправлений, телеграфных и иных сообщений, снятие информации с технических каналов связи. Применение данных мероприятий к даркнет-среде требует специальной технической подготовки и процессуального оформления, поскольку стандартные схемы взаимодействия с операторами связи здесь неприменимы.

Законодательство допускает использование специальных технических средств, негласно получаемых информации, однако их применение должно строго соответствовать принципам законности и соразмерности, что накладывает дополнительную ответственность на должностных лиц.

Уголовный кодекс Российской Федерации не содержит специальной нормы, напрямую квалифицирующей создание или администрирование анонимной торговой площадки как самостоятельный состав преступления. При квалификации подобных преступлений правоприменительная практика опирается на совокупность статей, а именно:

ст. 138.1 УК РФ предусматривает ответственность за незаконный оборот специальных технических средств, предназначенных для негласного по-

лучения информации. Данная норма применяется к разработчикам и распространителям инструментов деанонимизации.

ст. 228.1 УК РФ (незаконное производство, сбыт или пересылка наркотических средств). Значительная доля транзакций в зоне .onion связана именно с оборотом запрещенных веществ. Следователи квалифицируют действия организаторов площадок как пособничество или организацию сбыта, в зависимости от степени их вовлеченности в логистические цепочки. Постепенно формируется подход - предоставление инфраструктуры для незаконного оборота может расцениваться как соучастие, даже при формальном нейтралитете оператора ресурса.

ст. 159 УК РФ (мошенничество) применяется в случаях, когда площадки выступают гарантом сделок, но присваивают средства пользователей (так называемые exit scam). Доказывание умысла и причинно-следственной связи в таких ситуациях осложняется анонимностью бенефициаров и использованием криптовалют. Практика привлечения к ответственности по данной норме постепенно расширяется.

ст. 187 УК РФ (неправомерный оборот средств платежных карт) и 172.1 УК РФ (незаконная организация и проведение азартных игр) также находят применение в зависимости от профиля конкретной площадки.

Международно-правовое регулирование играет ключевую роль в противодействии транснациональной преступности в Даркнет. Серверная инфраструктура, разработчики, администраторы и пользователи анонимных площадок часто находятся в разных юрисдикциях. Конвенция Совета Европы о киберпреступности (Будапештская конвенция 2001 г.) остается основным международным документом, устанавливающим стандарты криминализации компьютерных преступлений и механизмы международного сотрудничества.

Россия не является участницей данной конвенции. Но значительная часть её положений нашла отражение в российском законодательстве. Что позволяет применять схожие правовые механизмы в рамках двусторонних международных договоров.

Большое значение для международного сотрудничества имеют резолюции Генеральной Ассамблеи ООН, направленные на борьбу с транснациональной организованной преступностью и незаконным оборотом наркотических средств. Также многосторонние соглашения в рамках СНГ по вопросам информационной безопасности. Активно используются двусторонние договоры о правовой помощи по уголовным делам, которые предусматривают процедуры направления запросов о предоставлении доказательств, экстрадиции лиц и проведения совместных расследований.

Однако на практике применение этих механизмов сопряжено с серьезными трудностями. Средний срок ответа на запрос о международной правовой помощи составляет несколько месяцев. Такие задержки становятся критическими: площад-

ки успевают сменить домены, перенести серверы на новые локации или полностью прекратить свою деятельность.

Деятельность Интерпол и Европол координирует усилия национальных подразделений по борьбе с киберпреступностью. Совместные операции, такие как DisrupTor или Operation Bayonet, демонстрируют эффективность синхронизированных действий при одновременных задержаниях в нескольких странах. Правовая основа таких операций - соглашения о взаимном признании ордеров, упрощенные процедуры обмена разведывательной информацией и создание совместных следственных групп.

Но различия нормативно-правового регулирования в различных странах, особенно в вопросах допустимости цифровых доказательств и защиты персональных данных, создают барьеры для оперативного сотрудничества.

Особую сложность представляет вопрос юрисдикции. Согласно статье 12 УК РФ: российское уголовное законодательство распространяется на лиц, совершивших преступления на территории РФ, а также на граждан РФ и лиц без гражданства, постоянно проживающих в РФ, совершивших преступления вне пределов страны. Определение «место совершения преступления» весьма затруднительно. Сервер может находиться в Нидерландах, администратор - в Бразилии, разработчик - в Германии, а пользователи - по всему миру. В таких ситуациях следует регламентироваться профильными разъяснениями Верховного суда РФ.

Процессуальное оформление материалов, полученных при работе с анонимными торговыми площадками, регулируется Уголовно-процессуальным кодексом РФ.

В соответствии со статьёй 81 УПК РФ вещественными доказательствами признаются предметы, которые использовались при совершении преступления или сохранили на себе его следы. В сфере высоких технологий к таким предметам относятся серверы, жёсткие диски, USB-накопители, а также файлы и другие электронные данные.

Статья 164.1 УПК РФ специально регулирует проведение следственных действий с использованием информационных технологий. Она предусматривает порядок осмотра электронных носителей, изъятия информации и обязательную видеотекстовую фиксацию хода этих действий.

Особую сложность вызывает вопрос о доказательственном значении данных блокчейна и метаданных сети Tor. Записи в криптовалютных реестрах (Bitcoin, Monero и других) сами по себе не указывают напрямую на конкретного человека. Это всего лишь последовательность транзакций, которая становится доказательством только когда её сопоставляют с другими материалами дела. Суды всё чаще принимают такие данные, но только после компьютерно-технической экспертизы, которая подтверждает их подлинность и неизменность.

Согласно статье 80 УПК РФ в качестве доказательств может использоваться и заключение специ-

алиста. Благодаря этому следователи привлекают экспертов для разбора криптографических данных, восстановления удалённой информации и выявления связей между участниками преступной деятельности.

20 февраля 2026 г. УПК РФ дополнен новой статьёй - ст.164.2. закрепляет особенности изъятия цифровой валюты при производстве следственных действий.

При этом крайне важно строго соблюдать порядок получения электронных доказательств. Если информация получена с нарушением закона - например, через негласные мероприятия, не предусмотренные УПК, - суд может признать её недопустимой. Особенно остро этот вопрос стоит при работе с Даркнет. Оперативники нередко используют социальную инженерию, фишинг или вредоносное программное обеспечение, чтобы установить личность администраторов площадок. Судебная практика по оценке таких методов пока неоднородна: в одних случаях действия признаются законными, в других — нет. Чётких правил на этот счёт в законодательстве до сих пор нет.

Не менее внимательно нужно подходить к фиксации содержимого анонимных сайтов. Простые скриншоты без дополнительных мер защиты легко оспариваются стороной защиты. Поэтому лучше использовать специальные программы для сохранения веб-страниц, которые автоматически создают хеш-суммы и временные метки, и обязательно привлекать специалиста для составления протокола осмотра.

В целом нормативная база в этой сфере содержит определенные пробелы. В нормативно-правовых актах до сих пор нет официальных определений терминов «Даркнет», «скрытый сервис» и «псевдодоменированная зона .onion». Из-за этого возникают разночтения и сложности с квалификацией преступлений.

Регулирование криптовалют также остаётся довольно поверхностным. Федеральный закон «О цифровых финансовых активах» даёт только общие рамки, но почти не затрагивает вопросы контроля за миксерами, P2P-обменниками и децентрализованными биржами, через которые часто отмываются деньги с анонимных площадок.

Кроме того, отсутствует четкий механизм признания цифровых следов (блокчейн-транзакций, логов Tor, метаданных кошельков) самостоятельными доказательствами без дополнительной верификации через традиционные источники [1].

Возможные направления совершенствования законодательства включают: введение специального определения анонимных торговых площадок в 149-ФЗ, установление упрощенной процедуры экстренного взаимодействия с иностранными регистраторами доменов и хостинг-провайдерами, закрепление статуса цифровых следов как допустимых доказательств при соблюдении технических стандартов фиксации, а также развитие института совместных следственных групп с правом оперативного обмена данными в реальном времени [2].

Понимание пробелов национального регулирования логически подводит к необходимости изучения зарубежного опыта. Многие страны уже столкнулись с аналогичными вызовами и выработали собственные подходы к правовому регулированию, техническому контролю и международному сотрудничеству.

Анализ этих решений позволит сформулировать конкретные методические рекомендации, которые будут рассмотрены в следующей главе настоящей работы.

Список литературы:

[1] Тисен О.Н. Механизм совершения преступлений с использованием криптовалют: по результатам

анализа следственной и судебной практики// Российский следователь. 2024, №5. С. 7-11.

[2] Тисен О.Н. Субъекты досудебного соглашения о сотрудничестве// Судебная власть и уголовный процесс. 2013, №2, С. 91-95.

References:

[1] Tisen O.N. Mechanism of committing crimes involving cryptocurrencies: based on an analysis of investigative and judicial practice // Russian Investigator. 2024, No. 5. Pp. 7–11.

[2] Tisen O.N. Parties to a pre-trial cooperation agreement // Judicial Power and Criminal Process. 2013, No. 2, Pp. 91–95.