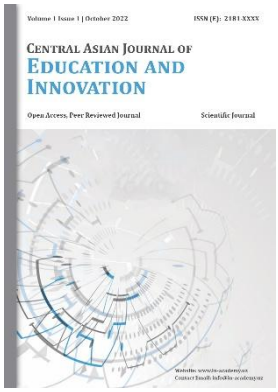

УГОЛОВНО-ПРАВОВАЯ ХАРАКТЕРИСТИКА ЦИФРОВОГО ПРЕСЛЕДОВАНИЯ: ПРОБЛЕМЫ КВАЛИФИКАЦИИ И ДОКАЗЫВАНИЯ

Сапарбаева Шахноза Рустем кызы
Базовый докторант Каракалпакского государственного университета имени Бердаха
https://doi.org/10.5281/zenodo.20655236

ARTICLE INFO

Qabul qilindi: 08-iyun 2026 yil
Ma'qullandi: 10- iyun 2026 yil
Nashr qilindi: 12- iyun 2026 yil

KEY WORDS

цифровое преследование, кибersталкинг, уголовное право, квалификация преступлений, электронные доказательства, неприкосновенность частной жизни, информационная безопасность, киберпреступность, психологическое насилие.

ABSTRACT

В представленной статье исследуется феномен цифрового преследования (кибersталкинга) как новой, стремительно развивающейся формы посягательства на личность, ее психологическую неприкосновенность и частную жизнь в условиях глобальной цифровизации. Анализируются ключевые уголовно-правовые признаки данного деяния, а также выявляются существенные пробелы в действующем уголовном законодательстве Республики Узбекистан, препятствующие эффективной квалификации таких преступлений. Особое внимание уделяется специфике собирания и оценки цифровых доказательств, проблемам деанонимизации преступников и трансграничному характеру киберпреступности. На основе проведенного анализа формулируется концепция комплексного противодействия цифровому преследованию, включающая законодательные, технологические и процессуальные модули.

Стремительное развитие информационно-коммуникационных технологий и повсеместное внедрение сети Интернет во все сферы общественной жизни привели не только к беспрецедентному расширению возможностей для коммуникации, но и к появлению новых, высокотехнологичных форм криминального поведения. В рамках реализации стратегии «Цифровой Узбекистан – 2030» вопросы обеспечения информационной безопасности граждан приобретают первостепенное значение.[1] Одной из наиболее латентных и психологически разрушительных угроз современности стало цифровое преследование, или кибersталкинг — целенаправленное, систематическое использование электронных средств связи для запугивания, контроля, домогательства или причинения серьезного беспокойства другому лицу. [2]

Актуальность темы исследования обусловлена резким ростом числа инцидентов, связанных с угрозами в социальных сетях, популярных мессенджерах, массовой рассылкой оскорбительных сообщений, а также

несанкционированным сбором и распространением личных данных. В отличие от традиционного физического преследования, кибersталкинг позволяет преступнику действовать анонимно, дистанционно и круглосуточно, что многократно усиливает чувство незащищенности у жертвы. Несмотря на высокую общественную опасность деяния, выражающуюся в причинении глубоких психологических травм и разрушении социальных связей потерпевших, правоохранительные органы сталкиваются с серьезными теоретическими и практическими трудностями при квалификации содеянного, а также на этапе сбора и закрепления цифровых доказательств.

Цифровое преследование представляет собой комплексное деяние, ядром которого является систематичность, навязчивость и прямой умысел виновного на причинение психологического дискомфорта или страха. Специфика заключается в обязательном использовании информационно-коммуникационных технологий в качестве орудия преступления. Однако ввиду отсутствия в Уголовном кодексе Республики Узбекистан (УК РУз) специальной нормы, устанавливающей ответственность непосредственно за преследование (сталкинг), правоприменители вынуждены прибегать к квалификации действий кибersталкеров по смежным статьям. [3] Это неизбежно приводит к искусственному дроблению единого преступного умысла.

Зачастую цифровое преследование сопровождается запугиванием, что формально подпадает под признаки статьи 112 УК РУз (Угроза убийством или применением насилия). Основная проблема правоприменения в данном случае кроется в требовании реальности угрозы. В цифровой среде, когда сталкер скрывается за анонимным аккаунтом (фейком) и физически может находиться за пределами страны, доказать, что потерпевший имел достаточные основания опасаться осуществления этой угрозы, крайне сложно. Следственная практика показывает, что угрозы, высказанные исключительно в виртуальном пространстве без подкрепления физическими действиями, часто расцениваются как малозначительные.

Другим аспектом кибersталкинга является незаконный сбор и распространение информации о жертве. Подобные действия квалифицируются по статье 141-1 УК РУз (Нарушение неприкосновенности частной жизни). Пробел здесь заключается в том, что закон защищает лишь сведения, составляющие личную или семейную тайну. Современные сталкеры активно используют методы разведки по открытым источникам (OSINT), систематизируя легально доступную информацию (фотографии, геолокации, данные о месте работы) с целью создания атмосферы тотального контроля. Формально нарушения тайны не происходит, однако ущерб психологической безопасности жертвы наносится колоссальный. [4]

Кроме того, инструментом цифровой травли нередко выступает распространение заведомо ложных, порочащих сведений, что охватывается статьей 139 УК РУз (Клевета). Тем не менее, данная норма неприменима в ситуациях, когда преследователь массово рассылает правдивую, но глубоко компрометирующую информацию интимного характера или изводит жертву сотнями бессмысленных сообщений, не содержащих ни угроз, ни клеветы, но носящих откровенно терроризирующий характер. Таким образом, действующий уголовный закон реагирует лишь на отдельные, фрагментарные проявления кибersталкинга, оставляя без должной правовой оценки сам факт целенаправленного психологического преследования в цифровой среде.

Процесс доказывания по делам рассматриваемой категории сталкивается с комплексом препятствий процессуального и технического свойства. Фундаментальной проблемой является анонимизация и идентификация субъекта преступления. Использование злоумышленниками VPN-сервисов, прокси-серверов, теневого сегмента сети Интернет и виртуальных телефонных номеров сводит на нет стандартные методы оперативно-розыскной деятельности. Даже при успешном установлении IP-адреса устройства, с которого осуществлялись противоправные действия, следствию предстоит доказать, что устройством управлял конкретный подозреваемый, а не третье лицо или вредоносная программа.

Не менее острой является проблема волатильности (изменчивости) электронных доказательств. Цифровые следы подвержены быстрому уничтожению или модификации. Во многих современных мессенджерах предусмотрена функция бесследного удаления переписки для обеих сторон. Потерпевшие, как правило, пытаются фиксировать факт преследования с помощью снимков экрана (скриншотов), однако с точки зрения уголовно-процессуального законодательства их доказательственная сила уязвима, так как подобные изображения легко фальсифицируются. Для легализации таких данных требуются длительные и сложные компьютерно-технические экспертизы. [5]

Дополнительные трудности вызывает доказывание систематичности и умысла на причинение страданий. В виртуальной среде грань между назойливым вниманием и уголовно наказуемым сталкингом крайне тонка. Отсутствуют унифицированные методики судебно-психологической экспертизы, которые позволили бы объективно оценить степень моральных страданий и обоснованность чувства страха жертвы, вызванного исключительно электронными сообщениями.

Наконец, нельзя игнорировать трансграничный характер подобных преступлений. Серверы глобальных социальных сетей и провайдеров услуг связи находятся в различных юрисдикциях. Процедура направления международных запросов об оказании правовой помощи занимает длительное время, что критически недопустимо в ситуациях, требующих немедленного вмешательства для защиты жизни и здоровья жертвы.

Для преодоления сложившейся ситуации и обеспечения надежной защиты граждан необходим концептуально новый подход. Оптимальным решением видится создание комплексной архитектуры противодействия цифровому преследованию, условно объединяющей три взаимосвязанных модуля: законодательный, технологический и процедурный. Подобный механизм мог бы стать своеобразным «кибер-щитом» (Cyber-Qalqon) для защиты прав личности в информационном пространстве.

В рамках законодательного модуля первоочередной задачей является криминализация сталкинга. Предлагается дополнить Уголовный кодекс Республики Узбекистан новой статьей, криминализирующей систематическое преследование. Диспозиция должна охватывать целенаправленные действия по поиску, слежке и установлению нежелательного контакта, вызывающие у потерпевшего обоснованный страх за свою безопасность. В этой же статье необходимо предусмотреть квалифицирующий признак — совершение деяния с использованием информационно-

телекоммуникационных сетей, а также специальных технических средств негласного получения информации, что позволит адекватно оценивать повышенную общественную опасность киберсталкинга.

Процедурный модуль должен быть направлен на реформирование уголовно-процессуального законодательства. [6] Ключевым нововведением должно стать внедрение института защитных (охранных) ордеров, выдаваемых судом в ускоренном порядке. Такой ордер должен не только запрещать физическое приближение к потерпевшему, но и содержать строгий запрет на любые формы электронной коммуникации, включая взаимодействие через третьих лиц в социальных сетях. Кроме того, требуется разработка детализированных методических рекомендаций для органов дознания и следствия по фиксации цифровых следов, а также упрощение процедуры признания электронных документов допустимыми доказательствами.

Технологический модуль предполагает налаживание оперативного взаимодействия правоохранительных органов с IT-сектором. Необходимо нормативно закрепить механизмы экстренного реагирования интернет-провайдеров и администраторов цифровых платформ на запросы следствия по делам, связанным с непосредственной угрозой безопасности личности. Внедрение передовых программных решений для мониторинга и блокировки вредоносного трафика позволит пресекать действия сталкеров еще на этапе покушения.

Заключение

Цифровое преследование в современных реалиях представляет собой серьезное посягательство на конституционные права граждан, их психологическую неприкосновенность и личную безопасность. Отсутствие прямого уголовного запрета на сталкинг создает иллюзию безнаказанности у правонарушителей и оставляет потерпевших без надлежащей государственной защиты. Практика применения разрозненных норм действующего уголовного законодательства демонстрирует свою неэффективность, не позволяя охватить всю полноту и систематичность данного преступного явления.

Решение проблемы требует незамедлительной модернизации правовой базы путем прямой криминализации преследования с выделением его цифровой формы в качестве отягчающего обстоятельства. Наряду с этим, критически важно внедрять комплексные правовые и технологические инструменты, совершенствовать криминалистические методики работы с электронными доказательствами. Только системный подход позволит обеспечить адекватную защиту прав граждан и неотвратимость наказания за посягательства на личность в условиях развивающегося цифрового общества.

Список использованной литературы:

1. Указ Президента Республики Узбекистан от 05.10.2020 г. № УП-6079 «Об утверждении Стратегии «Цифровой Узбекистан - 2030» и мерах по ее эффективной реализации».
2. Смирнов А. В. Киберсталкинг: понятие, формы и проблемы уголовно-правовой квалификации // Российский следователь. – 2022. – № 4. – С. 38-42.

3. Уголовный кодекс Республики Узбекистан (утвержден Законом РУз от 22.09.1994 г. № 2012-XII) // Национальная база данных законодательства.
4. Васюков В. Ф. Особенности изъятия электронных носителей информации при расследовании преступлений // Уголовный процесс. – 2019. – № 11. – С. 54-59.
5. Русскевич Е. А. Уголовное право и цифровая преступность: проблемы и решения. – Москва: ИНФРА-М, 2020. – 224 с.
6. Уголовно-процессуальный кодекс Республики Узбекистан (утвержден Законом РУз от 22.09.1994 г. № 2012-XII) // Национальная база данных законодательства.