

*Левин Д.С.,
Следователь*

*Следственное управление Следственного комитета Российской
Федерации по Тюменской области
Российская Федерация, г. Тюмень*

*магистр,
ФГБОУ ВО «Челябинский Государственный Университет», кафедра
уголовно-правовых дисциплин, факультет заочного и дистанционного
обучения*

Научный руководитель: Дробот С.А.

ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННО- ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ «ИНТЕРНЕТ» КАК СПОСОБ СОВЕРШЕНИЯ ПРЕСТУПЛЕНИЯ: УГОЛОВНО-ПРАВОВЫЕ И КРИМИНАЛИСТИЧЕСКИЕ АСПЕКТЫ

***Аннотация.** Рассмотрены уголовно-правовые и криминалистические аспекты использования сети «Интернет» при совершении преступлений. Раскрыты разграничение мошенничества по статьям 159 и 159.6 УК РФ, значение цифровых следов и процессуальные условия получения электронных доказательств. Обозначены проблемы квалификации деяний и установления лица, совершившего преступление.*

***Ключевые слова:** сеть «Интернет», информационно-телекоммуникационные технологии, киберпреступность, мошенничество, цифровые следы, электронные доказательства, криминалистика, уголовная ответственность.*

***Abstract.** The article examines the criminal law and forensic aspects of using the Internet to commit crimes. It discusses the distinction between fraud under*

Articles 159 and 159.6 of the Criminal Code of the Russian Federation, the significance of digital traces, and the procedural requirements for obtaining electronic evidence. It identifies problems in the legal classification of offences and the identification of offenders.

Keywords: *Internet, information and telecommunications technologies, cybercrime, fraud, digital traces, electronic evidence, forensic science, criminal liability.*

В 2023 г. российские органы внутренних дел зарегистрировали свыше 677 тыс. преступлений в сфере информационных технологий. В 2022 г. зарегистрировано 522 тыс. таких деяний, а доля преступлений цифрового характера выросла с 26,5 до 34,8 %. Число преступлений, совершенных с использованием сети «Интернет», увеличилось с 381,1 до 526,7 тыс. [1, с. 105]. Статистика отражает изменение способа преступного поведения: лицо получает возможность действовать дистанционно, использовать несколько учетных записей, привлекать посредников и одновременно воздействовать на потерпевших в разных регионах.

Сеть «Интернет» не образует самостоятельный состав преступления. Уголовная ответственность возникает при наличии признаков конкретного преступления, предусмотренного Особенной частью УК РФ. Интернет может выполнять функцию средства связи, места размещения информации, канала передачи данных, инструмента воздействия на компьютерную систему или способа сокрытия личности. Такое разграничение связано с принципом законности, закрепленным в ст. 3 УК РФ, и запретом расширительного толкования уголовного закона. М. В. Арзамасцев связывает квалификацию интернет-деяний с необходимостью учитывать цифровые права и не переносить уголовно-правовые запреты на электронные ресурсы без прямого указания закона [2, с. 12].

Статья 159 УК РФ охватывает хищение имущества или приобретение права на имущество путем обмана либо злоупотребления доверием. Размещение фиктивного объявления о продаже товара, создание копии сайта магазина, рассылка сообщения от имени банка или должностного лица образуют обман, если потерпевший передает деньги под влиянием ложных сведений. Пункт 21 постановления Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48 разъясняет: распространение заведомо ложных сведений в информационно-телекоммуникационной сети, включая создание поддельных сайтов и использование электронной почты, квалифицируется по ст. 159 УК РФ, а не по ст. 159.6 УК РФ.

Статья 159.6 УК РФ применяется при хищении, связанном с вмешательством в функционирование средств хранения, обработки или передачи компьютерной информации. Пленум Верховного Суда связывает такое вмешательство с целенаправленным воздействием программных или программно-аппаратных средств на сервер, компьютер, смартфон либо сеть, которое нарушает установленный процесс обработки, хранения или передачи данных и позволяет завладеть имуществом. Если потерпевший сам вводит реквизиты карты на поддельном сайте, состав ст. 159.6 УК РФ отсутствует, поскольку компьютерная система не подвергалась такому воздействию.

Уголовная политика учитывает новые способы обмана, включая синтез голоса, изображения и автоматическую рассылку сообщений. Е. В. Зотина указывает, что в 2023 г. каждое третье преступление совершалось с использованием информационно-телекоммуникационных технологий, а число видеодипфейков выросло втрое, аудиодипфейков почти в восемь раз по сравнению с 2022 г. [3, с. 75]. Автор предлагает учитывать использование искусственного интеллекта как квалифицирующий признак в ст. 159, 159.3 и 159.6 УК РФ, поскольку технология позволяет одновременно персонализировать обращение и увеличить число потерпевших.

Отдельную группу образуют преступления против личности, общественной безопасности и общественной нравственности, при которых Интернет обеспечивает публичность действия. Ю. С. Пестерева и С. Е. Тимошенко исследуют «треш-стримы» и указывают, что действующее уголовное законодательство не содержит самостоятельного состава за такую трансляцию. Ответственность наступает по статьям о преступлениях против личности, а запись уже совершенного насилия может образовывать постпреступное поведение при наличии самостоятельных признаков состава [4, с. 600].

Виртуальный след возникает при каждом действии в цифровой среде: авторизации, передаче сообщения, изменении файла, входе в интернет-банк, подключении устройства, оплате домена и переводе денежных средств. Е. С. Переверзева и А. В. Комов связывают механизм слеδοобразования с преобразованием действий пользователя в записи, которые сохраняются на устройстве, сервере, в сетевом оборудовании и информационной системе [5, с. 130]. След может быть видимым для пользователя или скрытым в системном журнале, метаданных и резервной копии.

В. Б. Вехов и А. Б. Смушкин описывают цифровой отпечаток устройства как производное значение параметров аппаратного и программного обеспечения. К таким параметрам относятся версия операционной системы, браузер, конфигурация устройства и иные технические признаки. Авторы указывают, что подделка совокупного отпечатка практически невозможна, поэтому его сопоставление с серверными журналами повышает вероятность установления устройства, с которого совершались действия [6, с. 393].

Обыск и выемка электронных носителей требуют соблюдения ст. 164.1 УПК РФ. Изъятие допускается, когда на носителе содержится информация, которой владелец не вправе распоряжаться, когда сведения могут использоваться для новых преступлений либо когда копирование способно привести к утрате или изменению данных. Закон предусматривает

копирование информации на другой носитель с участием специалиста и отражение технических действий в протоколе.

А. В. Кутузов указывает на отсутствие единого законодательного определения цифровых следов и цифровых доказательств. По его позиции, электронная информация нуждается в закреплении признаков происхождения, целостности, доступности для проверки и связи с обстоятельствами уголовного дела [7, с. 68]. Для суда важен не цифровой формат сам по себе, а возможность установить источник, способ получения и неизменность представленных сведений.

Электронно-цифровые следы получают доказательственное значение после проверки их достоверности. В. А. Родивилина и В. В. Коломинов связывают такую проверку с единообразием извлечения, копирования, хранения и исследования данных. Авторы обосновывают необходимость национального регламента работы с электронно-цифровыми следами, поскольку нарушение процедуры создает риск признания сведений недопустимыми [8, с. 214].

Первую проблему создает смешение понятий «преступление в сфере компьютерной информации» и «преступление с использованием Интернета». Глава 28 УК РФ охраняет общественные отношения в сфере компьютерной информации. Статьи 159, 163, 205.2, 280 и 282 УК РФ охраняют иные объекты, а сеть используется в качестве средства совершения или распространения деяния. Ошибка в разграничении приводит к неправильному определению состава, предмета доказывания и подследственности.

Вторую проблему образует установление лица, которое фактически использовало учетную запись или устройство. Регистрация на паспортные данные, привязка номера телефона и наличие банковской карты не исключают передачи доступа другому человеку. Н. И. Валькирия указывает, что цифровые следы дают сведения о свойствах и поведении неизвестного лица, но требуют соединения первичной информации с дополнительными данными,

полученными при помощи специальных знаний [9, с. 60]. Поэтому идентификация строится на совокупности сетевых, финансовых, технических и поведенческих признаков.

3. И. Харисова предлагает кодировать преступления в сфере компьютерной информации с учетом примененного средства, способа воздействия, объекта и оставленных следов. Кодирование связывается с формированием единообразных методик расследования и использованием технико-криминалистических средств при появлении новых способов атаки [10, с. 166]. Практический результат такого подхода возможен при условии, что код не заменяет юридическую квалификацию и не используется как самостоятельное основание уголовной ответственности.

Использование сети «Интернет» изменяет способ подготовки и совершения преступления, однако само по себе не образует состава преступления. При размещении ложных сведений и создании поддельного сайта применяется ст. 159 УК РФ. При воздействии на процесс обработки компьютерной информации применяется ст. 159.6 УК РФ, а при наличии самостоятельных признаков возможна совокупность со ст. 272, 273 или 274.1 УК РФ. Такой вывод следует из п. 21 постановления Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48.

Криминалистическое расследование строится на ранней фиксации сетевых и электронных данных. IP-адрес, сведения об учетной записи, цифровой отпечаток устройства, журналы авторизации, переписка и банковские операции приобретают доказательственное значение при установлении источника, целостности и связи с событием преступления. Статьи 164.1 и 164.2 УПК РФ задают процессуальные условия работы с электронными носителями, а заключение специалиста или эксперта дополняет протокол следственного действия.

Данные МВД России о росте числа IT-преступлений с 522 тыс. в 2022 г. до свыше 677 тыс. в 2023 г. подтверждают необходимость точного

разграничения составов и единообразной фиксации цифровых следов. Научные предложения А. В. Кутузова, В. А. Родивилиной, В. В. Коломинова, З. И. Харисовой и Н. И. Валькирии относятся к процедурам получения, проверки и сопоставления данных. Их практическая ценность связана с тем, что суд получает проверяемую связь между цифровым действием, конкретным лицом и последствием, указанным в уголовном законе.

Библиографический список:

1. Малышева Ю. Ю. Мошеннические проявления фейков и дипфейков: проблемы противодействия // Российско-Азиатский правовой журнал. 2025. № 1. С. 105–112.
2. Арзамасцев М. В. Конституционные основы ответственности за преступления, совершаемые с использованием сети «Интернет» // Криминалистика. 2024. № 2 (47). С. 10–18.
3. Зотина Е. В. Уголовно-правовой аспект предупреждения мошенничества с использованием информационно-телекоммуникационных технологий и приемов социальной инженерии // Вестник Казанского юридического института МВД России. 2024. Т. 15, № 3 (57). С. 73–82.
4. Пестерева Ю. С., Тимошенко С. Е. Уголовно-правовые, криминологические, криминалистические аспекты публичной демонстрации преступлений против личности в информационно-телекоммуникационной сети «Интернет» // Сибирское юридическое обозрение. 2024. Т. 21, № 4. С. 596–608.
5. Переверзева Е. С., Комов А. В. Механизм слепообразования виртуальных следов // Вестник Санкт-Петербургского университета МВД России. 2022. № 1 (93). С. 128–133.
6. Вехов В. Б., Смушкин А. Б. Криминалистическое исследование цифровых отпечатков компьютерных устройств // Всероссийский криминологический журнал. 2024. Т. 18, № 4. С. 390–397.

7. Кутузов А. В. Цифровые следы и доказательства: необходимость теоретического и нормативного определения в условиях цифровизации // Legal Concept = Правовая парадигма. 2024. Т. 23, № 3. С. 67–72.

8. Родивилина В. А., Коломинов В. В. Электронно-цифровые следы как доказательства при расследовании интернет-мошенничества: криминалистические и процессуальные аспекты // Вестник Восточно-Сибирского института МВД России. 2026. № 1. С. 214–227.

9. Валькирия Н. И. Использование цифровых следов в деятельности по установлению лица, совершившего преступление // Криминалистика: вчера, сегодня, завтра. 2023. № 4 (28). С. 56–66.

10. Харисова З. И. Криминалистическая кодификация преступлений в сфере компьютерной информации и ее роль в унификации процесса расследования // Вестник Санкт-Петербургского университета МВД России. 2025. № 4. С. 164–172.