

Научная статья

<https://doi.org/10.24412/2220-2404-2026-8-5>

УДК 343.13



Attribution

cc by

ОПРЕДЕЛЕНИЕ ТЕРРИТОРИАЛЬНОЙ ПОДСУДНОСТИ ПО УГОЛОВНЫМ ДЕЛАМ
О ПРЕСТУПЛЕНИЯХ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ
ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Исмаилов М.И.

Московский государственный юридический университет им. Кутафина

Аннотация. Цель статьи – систематизировать критерии определения территориальной подсудности по ИТТ-преступлениям и предложить практико-ориентированный алгоритм действий для следствия, прокурора и суда. Цифровой способ совершения преступлений (Интернет, мессенджеры, дистанционное банковское обслуживание) размывает традиционные критерии «места совершения преступления», что затрудняет определение территориальной подсудности и порождает споры о компетентном суде. На основе ст. 32 УПК РФ и разъяснений Пленума Верховного Суда РФ (15.12.2022 № 37; 30.11.2017 № 48; 27.06.2023 № 22) предлагаются критерии выбора суда в делах о преступлениях, совершенных с использованием ИТТ, а также алгоритм локализации действий лица по цифровым следам. Выводы иллюстрируются примером из практики автора: хищение средств организации путем формирования платежных поручений в системе «Банк-клиент» и подтверждения операций по СМС-коду с последующим перечислением денег на подконтрольные счета.

Ключевые слова: подсудность, место совершения преступления, информационно-телекоммуникационные технологии, Интернет, дистанционное банковское обслуживание, мошенничество, безналичные денежные средства.

Финансирование: инициативная работа.

Original article

DETERMINATION OF TERRITORIAL JURISDICTION IN CRIMINAL CASES OF CRIMES
COMMITTED USING INFORMATION AND TELECOMMUNICATION TECHNOLOGIES

Magamed I. Ismailov

Moscow State Law University named after Kutafina

Abstract. The purpose of the article is to systematize the criteria for determining territorial jurisdiction for ITT crimes and to propose a practice-oriented algorithm of actions for the investigation, the prosecutor and the court. The paper addresses territorial jurisdiction in criminal cases involving offences committed through ICT (Internet, messengers, remote banking). Relying on Article 32 of the Russian Criminal Procedure Code and the Supreme Court Plenum's guidance (15.12.2022 No. 37; 30.11.2017 No. 48; 27.06.2023 No. 22), the author proposes criteria for locating the 'place of crime' via digital traces and demonstrates them with a practical case of misappropriation through a remote banking system.

Keywords: territorial jurisdiction, place of crime, ICT, Internet, remote banking, fraud; non-cash funds.

Funding: Independent work.

Введение.

Рост преступлений, совершаемых с использованием информационно-телекоммуникационных технологий, стал одним из ключевых вызовов для уголовного судопроизводства. Для таких дел характерны «дистанционность» действий, использование мобильных устройств и распределение событий преступления между несколькими территориями (регион пребывания виновного, место нахождения потерпевшего, банк, серверная инфраструктура).

Территориальная подсудность выступает не технической формальностью, а гарантийным институтом: неверное определение компетентного суда затрагивает конституционное право на рассмотрение дела законным судом и приводит к процессуальным издержкам (передача дела, отмена судебных решений, затягивание сроков).

Материалы.

Общее правило территориальной подсудности закреплено в ч. 1 ст. 32 УПК РФ: уголовное дело рассматривается по месту совершения преступления. Если преступление начато в одном месте, а окончено в другом, применяется ч. 2 ст. 32 УПК РФ (по месту окончания). При множественности эпизодов, совершенных в разных местах, действует ч. 3 ст. 32 УПК РФ (по месту совершения большинства преступлений либо наиболее тяжкого из них). Порядок передачи дела по подсудности и изменения подсудности раскрыт в ст.ст. 34-35 УПК РФ.

Постановление Пленума Верховного Суда РФ от 27.06.2023 № 22 подчеркивает, что установленный законом порядок определения и изменения подсудности исключает произвольный выбор суда и гарантирует рассмотрение дела компетентным и беспристрастным составом. Следовательно, установление

«места совершения преступления» приобретает доказательственное значение (п. 1 ч. 1 ст. 73 УПК РФ) и должно быть мотивировано в обвинении и проверяемо судом на стадии подготовки к судебному заседанию.

Постановление Пленума Верховного Суда РФ от 15.12.2022 № 37 закрепило общий ориентир для преступлений, совершенных с использованием электронных или информационно-телекоммуникационных сетей (включая Интернет): местом совершения признается место совершения лицом действий, входящих в объективную сторону состава преступления. Пленум отдельно обращает внимание на то, что доступ к сети осуществляется, в том числе, с переносных устройств, что делает необходимым установление фактического местонахождения пользователя в момент совершения действий.

Для имущественных преступлений, где результат выражается в причинении ущерба, на практике долгое время спорным оставался вопрос о том, следует ли связывать территорию преступления с местом «нахождения» безналичных денег (банка) либо с местом действий виновного. Специальное разъяснение дано Постановлением Пленума ВС РФ от 30.11.2017 № 48 (в ред. 15.12.2022): мошенничество с безналичными денежными средствами считается оконченным с момента их изъятия с банковского счета владельца (причинения ущерба), а место совершения - как правило, место совершения действий, связанных с обманом или злоупотреблением доверием и направленных на незаконное изъятие средств.

В п. 5.1 названного Постановления Пленума прямо указано, что территориальная подсудность дел о мошенничестве с безналичными денежными средствами определяется по месту совершения лицом действий, направленных на незаконное изъятие средств, а при наличии нескольких территорий - по правилам ч.ч. 2-4 и 5.1 ст. 32 УПК РФ. Таким образом, современная модель Верховного Суда РФ строится на приоритете локализации действий виновного, а не технической инфраструктуры.

Обсуждение.

Правоприменительная практика показывает, что наибольшие сложности возникают в трех типовых ситуациях.

Во-первых, при «формальных» интернет-составах (публичные призывы, распространение запрещенной информации), где объективная сторона исчерпывается размещением/рассылкой сведений: подсудность определяется по месту, где лицо использовало устройство для размещения или рассылки [11].

Во-вторых, при дистанционных хищениях (звонки, мессенджеры, фишинг, удаленный доступ), где действия по обману и действия по списанию средств могут быть пространственно разнесены: ориентиром выступает место действий виновного, направленных на незаконное изъятие имущества (в том числе подтверждение перевода).

В-третьих, при многоэтапных схемах, когда отдельные элементы объективной стороны совершены на разных территориях: применяется ч. 2 ст. 32 УПК

РФ (по месту окончания - последнего действия), а при множественности эпизодов - ч. 3 ст. 32 УПК РФ.

Обсуждение. Результаты.

Практический алгоритм установления подсудности в ИТТ-делах может быть сформулирован следующим образом:

1) определить состав и выделить действия, образующие объективную сторону;

2) установить территорию каждого действия по цифровым следам (IP-адреса и журналы входов, идентификаторы устройств, данные базовых станций и детализация соединений, логи банковских систем, сведения о доставке и подтверждении СМС-кодов);

3) если действия совершены на разных территориях - применить ч. 2 ст. 32 УПК РФ (место окончания) либо ч. 3 ст. 32 УПК РФ (большинство/наиболее тяжкое);

4) обеспечить отражение выбранного критерия в обвинении и возможность его проверки судом;

5) при выявлении ошибки использовать механизм передачи дела по подсудности (ст. 34 УПК РФ) либо, при наличии оснований, изменения подсудности (ст. 35 УПК РФ).

Переориентация подсудности на место совершения действий в сети неизбежно делает центральным вопрос доказывания такой «локализации». Если для традиционных составов место преступления часто следует из обстановки и материальной обстановки события, то в ИТТ-делах оно устанавливается через цифровые следы. При этом место совершения преступления продолжает входить в предмет доказывания как элемент события преступления (п. 1 ч. 1 ст. 73 УПК РФ), а значит, должно подтверждаться допустимыми и относимыми доказательствами.

К ключевым источникам сведений о месте действий относятся:

(а) журналы и метаданные информационных систем (IP-адреса входа, время сессий, идентификаторы устройств, сведения о браузере/ОС, токены);

(б) данные операторов связи (номера и координаты базовых станций, обслуживавших абонентское устройство в момент соединения);

(в) банковские логи дистанционного обслуживания (входы в «Банк-клиент», сведения о доставке и подтверждении одноразовых паролей, последовательность операций);

(г) данные из изъятых устройств (история подключений, геолокация, переписка, кэш приложений) [9].

Практически значимым является сопоставление разнородных источников: например, IP-адрес и время входа в систему «Банк-клиент» соотносятся с детализацией оператора связи и данными геолокации мобильного устройства.

Процессуальная форма получения и фиксации таких сведений также влияет на их доказательственное значение. Сведения банка и операторов связи, как правило, поступают в виде документов и могут приобщаться к делу как «иные документы» (ст. 84 УПК РФ),

однако, в зависимости от способа получения, применимы также выемка и осмотр документов и электронных носителей. Для получения у оператора связи сведений о соединениях между абонентами и (или) абонентскими устройствами предусмотрено специальное следственное действие (ст. 186.1 УПК РФ), осуществляемое по судебному решению (ст. 165 УПК РФ). Именно эта процессуальная конструкция позволяет законно получить данные о базовых станциях и тем самым «привязать» абонентское устройство к территории.

На стадии направления дела в суд важно избегать безальтернативной формулировки «находясь в неустановленном месте» там, где локализация объективно возможна. Если же установить место совершения действий не удалось, в обвинении целесообразно мотивировать, какие меры были приняты для установления территории (запросы, осмотры, экспертизы), какие сведения получены и почему выбран конкретный «замещающий» критерий подсудности. Такой подход повышает проверяемость выводов, снижает риск передачи дела по подсудности уже в суде и соответствует гарантийной природе института подсудности.

В моей адвокатской практике встречалось уголовное дело, в котором ключевым оказался именно вопрос территориальной подсудности (данные обезличены). Генеральный директор коммерческой организации К. оформил на супругу Н. доверенность с полномочиями дистанционного управления расчетным счетом организации и предоставил ей доступ к системе «Банк-клиент». Подтверждение операций осуществлялось одноразовыми СМС-кодами, поступавшими на номер телефона, находившийся в пользовании Н.

В последующем Н., используя полученный доступ и злоупотребляя доверием, сформировала и подписала платежные поручения на перечисление денежных средств со счета организации на подконтрольный ей счет. В назначении платежа отражались сведения о работах/услугах, фактически не выполнявшихся. По делу было установлено несколько эпизодов списания денежных средств (в том числе переводы по 120 000 руб.). Потерпевший описывал ситуацию предельно просто: «она переводила деньги на свои нужды».

Сложность заключалась в том, что в обвинении было указано: точное место, где Н. использовала устройство для входа в «Банк-клиент», формирования и подтверждения платежных поручений, в ходе расследования не установлено. При этом банк и потерпевшая организация находились на территории одного субъекта РФ. Возник спор: считать ли территорией преступления место нахождения банка/счета (как место списания средств и причинения ущерба) или добиваться установления места нахождения Н. в момент совершения действий в системе.

С учетом разъяснений Пленума ВС РФ (№ 37; № 48), приоритетным является установление территории совершения действий виновного. Поэтому для правильного решения вопроса о подсудности в подобных делах принципиально важно получать у банка сведения о времени и IP-адресах входа в систему, об

устройствах и каналах подтверждения операций, а также данные оператора связи о местонахождении абонентского номера (базовые станции) в соответствующие даты и время. Именно эти материалы позволяют обосновать место совершения действий, входящих в объективную сторону, и тем самым - законный суд [13].

Ключевая практическая проблема - случаи, когда локализовать место совершения действий в сети объективно невозможно (утрата логов, использование средств анонимизации, недостаточность данных у оператора связи). В такой ситуации правоприменитель фактически вынужден выбирать «замещающий» критерий, чаще всего ориентируясь на место списания средств со счета потерпевшего либо место открытия счета, что позволяет хотя бы обеспечить проверяемость вывода о подсудности. Представляется, что выбранная привязка должна быть прямо мотивирована в обвинении и подтверждена документально (материалами банка), иначе возрастает риск последующей отмены судебных актов из-за нарушения подсудности.

ИТТ-преступления нередко носят серийный характер и охватывают эпизоды в разных субъектах РФ. В этих случаях значение приобретает ч. 3 ст. 32 УПК РФ, а также разъяснение Пленума № 22: если прокурор направил дело в суд с соблюдением одного из альтернативных правил (например, по месту совершения большинства эпизодов), передача дела на основании другого альтернативного правила той же нормы не допускается [15]. Дополнительным «стабилизатором» является ч. 2 ст. 34 УПК РФ: если суд уже приступил к разбирательству и установил подсудность другому суду того же уровня, он вправе (с согласия подсудимого) оставить дело в своем производстве.

Для снижения правовой неопределенности *de lege ferenda* (законодательное предположение) возможно обсуждение точечного дополнения ст. 32 УПК РФ резервным правилом на случай, когда место совершения действий в сети не может быть установлено даже при принятии исчерпывающих мер. В качестве таких критериев могут рассматриваться место обнаружения признаков преступления либо место окончания предварительного расследования. Подобная норма не отменяла бы приоритет «места действий», но позволила бы единообразно решать дела, где цифровые следы по объективным причинам недоступны.

Заключение.

Разъяснения Пленума Верховного Суда РФ последних лет сформировали единый ориентир для определения территориальной подсудности по ИТТ-преступлениям: ключевым является место совершения действий, входящих в объективную сторону, в том числе совершенных дистанционно с использованием мобильных устройств. Для мошенничеств и иных хищений безналичных денежных средств эта логика дополнительно закреплена в Постановлении Пленума № 48.

Практика показывает, что правильное решение вопроса о подсудности в значительной степени за-

висит от качества собираемых цифровых доказательств, позволяющих локализовать действия пользователя (банковские журналы, IP-данные, сведения опе-

раторов связи). Устранение «слепых зон» при невозможности установить место совершения действий в сети требует дальнейшего развития судебной практики и обсуждения точечных законодательных изменений.

Конфликт интересов

Не указан.

Рецензия

Все статьи проходят рецензирование в формате double-blind peer review (рецензенту неизвестны имя и должность автора, автору неизвестны имя и должность рецензента). Рецензия может быть предоставлена заинтересованным лицам по запросу.

Conflict of Interest

None declared.

Review

All articles are reviewed in the double-blind peer review format (the reviewer does not know the name and position of the author, the author does not know the name and position of the reviewer). The review can be provided to interested persons upon request.

Список источников:

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок).
2. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (в действующей редакции).
3. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (в действующей редакции).
4. Постановление Пленума Верховного Суда РФ от 15.12.2022 № 37 "О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть Интернет".
5. Постановление Пленума Верховного Суда РФ от 30.11.2017 № 48 "О судебной практике по делам о мошенничестве, присвоении и растрате" (в ред. постановления Пленума ВС РФ от 15.12.2022 № 38).
6. Постановление Пленума Верховного Суда РФ от 27.06.2013 № 22 "О применении судами норм Уголовно-процессуального кодекса Российской Федерации, регламентирующих подсудность уголовного дела".
7. Архипов А.В. Проблемы определения места совершения мошенничества в отношении безналичных денежных средств // Уголовное право. - 2016. - № 3. - С. 4-10. EDN: WHWTNV
8. Бадзгарадзе Г.Д. Вопросы установления места совершения мошенничества, осуществленного с использованием информационных технологий: криминалистический и уголовно-процессуальный аспекты // Сибирское юридическое обозрение. - 2022. - Т. 19, № 2. - С. 156-164. DOI: 10.19073/2658-7602-2022-19-2-156-164 EDN: DYEXOW
9. Баранов А.М. Электронные доказательства: иллюзия уголовного процесса XXI в. // Уголовная юстиция. - 2019. - № 13. - С. 64-69. DOI: 10.17223/23088451/13/12 EDN: PJCJXL
10. Воронин М.И. Электронные доказательства в УПК: быть или не быть? // Lex Russica. - 2019. - № 7. - С. 74-84. DOI: 10.17803/1729-5920.2019.152.7.074-084 EDN: JZBDUT
11. Довгань М.А. Уголовные дела о мошенничестве, связанном с хищением безналичных денежных средств: вопросы подсудности и подследственности // Электронное приложение к "Российскому юридическому журналу". - 2022. - № 1. - С. 67-71. DOI: 10.34076/22196838_2022_1_67 EDN: BICHVO
12. Дорошова А.А. Электронные "доказательства" в уголовном судопроизводстве Российской Федерации // Право и практика. - 2019. - № 4. - С. 203-208. EDN: RAVFWA
13. Корешников Д.С. Проблемы определения территориальной подследственности и подсудности "дистанционных" преступлений // Правопорядок: история, теория, практика. - 2024. - № 3 (42). - С. 162-166. DOI: 10.47475/2311-696X-2024-42-3-162-166 EDN: AOQKYS
14. Мецкерский А.С., Дрокин В.С., Карпенко Д.Ю. Определение места совершения хищения денежных средств с использованием безналичных расчетов // Законность. - 2016. - № 10. - С. 58-60. EDN: XAAGCN
15. Стельмах В.Ю. Получение информации о соединениях между абонентами и (или) абонентскими устройствами // Lex Russica. - 2017. - № 3. - С. 141-153. DOI: 10.17803/1729-5920.2017.124.3.141-153 EDN: YJGGTF
16. Степанова М.А., Царев Е.В. Проблемы определения места совершения хищения денежных средств с использованием информационно-телекоммуникационных технологий // Вестник Белгородского юридического института МВД России имени И.Д. Путилина. - 2021. - № 1. - С. 12-16. EDN: COYGXC

References:

1. The Constitution of the Russian Federation (adopted by popular vote on December 12, 1993) (as amended).
2. The Criminal Code of the Russian Federation dated June 13, 1996, No. 63-FZ (as currently amended).
3. The Criminal Procedure Code of the Russian Federation dated December 18, 2001, No. 174-FZ (as currently amended).
4. Resolution of the Plenum of the Supreme Court of the Russian Federation dated 12/15/2022 No. 37 "On certain issues of judicial practice in criminal cases of crimes in the field of computer information, as well as other crimes committed using electronic or information and telecommunication networks, including the Internet."
5. Resolution of the Plenum of the Supreme Court of the Russian Federation dated 11/30/2017 No. 48 "On judicial practice in cases of fraud, embezzlement and embezzlement" (as amended by Resolution of the Plenum of the Supreme Court of the Russian Federation dated 12/15/2022 No. 38).
6. Resolution of the Plenum of the Supreme Court of the Russian Federation dated 06/27/2023 No. 22 "On the application by Courts of the norms of the Criminal Procedure Code of the Russian Federation regulating the jurisdiction of a criminal case".
7. Arkhipov A.V. Problems of Determining the Place of Commission of Fraud Involving Non-Cash Funds // Criminal Law. - 2016. - No. 3. - Pp. 4-10. EDN: WHWTNV
8. Badzgaradze G.D. Issues of Establishing the Place of Commission of Fraud Committed Using Information Technologies: Forensic and Criminal Procedure Aspects // Siberian Legal Review. - 2022. - Vol. 19, No. 2. - Pp. 156-164. DOI: 10.19073/2658-7602-2022-19-2-156-164 EDN: DYEXOW
9. Baranov A.M. Electronic Evidence: An Illusion of the 21st-Century Criminal Process // Criminal Justice. - 2019. - No. 13. - Pp. 64-69. DOI: 10.17223/23088451/13/12 EDN: PJCJXL

-
10. Voronin M.I. *Electronic evidence in the Criminal Procedure Code: to be or not to be?* // *Lex Russica*. – 2019. – No. 7. – Pp. 74–84. DOI: 10.17803/1729-5920.2019.152.7.074-084 EDN: JZBDUT
11. Dovgan M.A. *Criminal cases involving fraud related to the embezzlement of non-cash funds: issues of jurisdiction and investigative competence* // *Electronic supplement to the "Russian Legal Journal"*. – 2022. – No. 1. – Pp. 67-71. DOI: 10.34076/22196838_2022_1_67 EDN: BICHVO
12. Dorosheva A.A. *Electronic "evidence" in criminal proceedings of the Russian Federation* // *Law and Practice*. – 2019. – No. 4. – Pp. 203–208. EDN: RAVFWA
13. Koreshnikov D.S. *Problems of determining territorial jurisdiction and venue for "remote" crimes* // *Law and Order: History, Theory, Practice*. – 2024. – No. 3 (42). – Pp. 162-166. DOI: 10.47475/2311-696X-2024-42-3-162-166 EDN: AOQKYS
14. Meshchersky A.S., Drokin V.S., Karpenko D.Yu. *Determining the location where a theft of funds was committed using non-cash payments* // *Legality*. – 2016. – No. 10. – Pp. 58-60. EDN: XAAGCN
15. Stelmakh V.Yu. *Obtaining information about connections between subscribers and (or) subscriber devices* // *Lex Russica*. – 2017. – No. 3. – Pp. 141-153. DOI: 10.17803/1729-5920.2017.124.3.141-153 EDN: YJGGTF
16. Stepanova M.A., Tsarev E.V. *Problems of determining the location where the theft of funds was committed using information and telecommunications technologies* // *Bulletin of the Belgorod Law Institute of the Ministry of Internal Affairs of Russia named after I.D. Putilin*. – 2021. – No. 1. – Pp. 12-16. EDN: COYGXC

Информация об авторе:

Исмаилов Магамед Исмаил оглы, аспирант, Московский государственный юридический университет им. Кутафина (МГЮА) г. Москвы, Адвокат, КА «Московский юридический центр», Россия, Москва, E-mail: advocateimi@mail.ru
Magamed I. Ismailov, PhD student, Moscow State Law University named after Kutafina (MGUA), Moscow, Lawyer, Moscow Law Center, Moscow, Russia.

Статья поступила в редакцию / The article was submitted 26.04.2026;
Одобрена после рецензирования / Approved after reviewing 01.07.2026;
Принята к публикации / Accepted for publication 20.08.2026.
Автором окончательный вариант рукописи одобрен.