УДК 343.9

Шифр научной специальности – 5.1.4. (уголовно-правовые науки)

ПОНЯТИЕ И ПРИЗНАКИ ДИСТАНЦИОННЫХ ПРЕСТУПЛЕНИЙ В ЦИФРОВУЮ ЭПОХУ

РЕХОВСКИЙ Александр Федорович
кандидат юридических наук, доцент кафедры уголовно-правовых дисциплин Института права
ФГБОУ ВО Владивостокский государственный университет;
690014, ДФО, Приморский край, г. Владивосток, ул. Гоголя, 41.
e-mail: A.Rekhovskiy@vvsu.ru

REKHOVSKIY Alexander Fedorovich
Candidate of Legal Sciences, Associate Professor of the Department of Criminal Law Disciplines
Institute of Law
Vladivostok State University
690014, Far Eastern Federal District, Primorsky Krai, Vladivostok, Gogol Street, 41.
e-mail: A.Rekhovskiy@vvsu.ru

Краткая аннотация. В статье анализируются определение и признаки дистанционных преступлений в условиях цифровой трансформации: удалённость субъекта от места наступления последствий, опосредование цифровыми технологиями, наличие цифровых следов и трансграничный характер. Предлагается расширенная классификация таких преступлений на основе типологии cyber-enabled деяний (мошенничество, вымогательство, фишинг и др.). Рассматриваются трудности уголовного преследования, связанные с собиранием и верификацией цифровых доказательств, и формулируются рекомендации по унификации терминологии и совершенствованию следственных процедур в российском уголовном процессе.

Ключевые слова: дистанционные преступления, cyber-enabled преступления, цифровые доказательства, криминалистика, цифровая

трансформация, уголовный процесс, типология киберпреступлений, трансграничность.

Brief abstract. The article examines the definition and characteristics of remote crimes in the context of digital transformation: the perpetrator's physical distance from the location where consequences occur, mediation through digital technologies, the presence of digital traces, and a transnational nature. An expanded classification of such crimes is proposed, based on the typology of cyber-enabled offenses (e.g., fraud, extortion, phishing, etc.). The challenges of criminal prosecution related to the collection and verification of digital evidence are analyzed, and recommendations are formulated for unifying legal terminology and improving investigative procedures within the Russian criminal justice system.

Keywords: remote crimes, cyber-enabled offences, digital evidence, forensics, digital transformation, criminal procedure, cybercrime typology, cross-border nature.

Развитие информационно-коммуникационных технологий и расширение использования интернета, облачных сервисов, платформ социальных сетей и мобильных приложений привели к принципиальному изменению в способах совершения преступлений. Вместе с тем в научной литературе и на глобальном уровне существует фундаментальная проблема: отсутствие единого, общепринятого определения киберпреступления. Для обозначения этих явлений используется огромное количество различных терминов, нередко комбинируемых с префиксами cyber, computer, e-, internet, digital и information, которые применяются бессистемно и произвольно, создавая перекрытие значений или, наоборот, оставляя существенные лакуны в классификации[1, с. 379]. Если традиционное преступление предполагало физическое присутствие субъекта на месте события и прямое воздействие на объект посягательства, то в цифровую эпоху преступная деятельность все чаще опосредуется электронными средствами и осуществляется на расстоянии [2, с. 106-115].

Таким образом, появился новый класс правонарушений – дистанционные преступления, которые совершаются с использованием цифровых технологий, оставляют следы исключительно в электронной форме и часто носят трансграничный характер. Актуальность проблемы дистанционных преступлений определяется несколькими взаимосвязанными факторами. Во-первых, статистические данные свидетельствуют о масштабности явления: 85% расследований в странах Европейского союза уже включают компонент цифровых доказательств [3, с.187-211]. Во-вторых, российское уголовное законодательство и криминалистическая доктрина длительное время оперировали исключительно термином «преступления в сфере компьютерной информации», закрепленным в главе 28 Уголовного кодекса Российской Федерации, что не полностью охватывает явление дистанционных преступлений, опосредованных информационно-коммуникационными технологиями, но совершенных в традиционных сферах, таких как кража, мошенничество и вымогательство в онлайн-среде. В-третьих, европейское право, в том числе через новые регламенты о цифровых доказательствах (Regulation EU 2023/1543, Directive EU 2023/1544), выработало инновационные подходы к собиранию, верификации и допустимости цифровых улик, что требует адаптации в российской криминалистической практике.

Целью настоящего исследования является разработка комплексного определения дистанционных преступлений, выделение их характерных признаков, анализ типологии на основе международной классификации cyber-enabled деликтов и формулирование рекомендаций по совершенствованию криминалистического обеспечения их расследования в Российской Федерации. Объектом исследования выступают общественные отношения, возникающие при совершении дистанционных преступлений и их уголовном преследовании в условиях цифровой трансформации общества. Предметом исследования являются понятие, признаки, типология дистанционных преступлений и криминалистические методы их расследования.

В отечественной доктрине уголовного права и криминалистике отсутствует единое, устоявшееся определение дистанционного преступления. Традиционно исследователи оперировали категориями «преступления в сфере компьютерной информации», «киберпреступления» (cybercrime), «компьютерные преступления» и более недавно – «cyber-enabled преступления» (преступления, опосредованные технологией) [5, с. 162-176]. На международном уровне, в работах ведущих исследователей Williams, Black, Ahmed и других, выработана более дифференцированная типология. В соответствии с этой типологией киберпреступления подразделяют на две категории: во-первых, cyber-dependent преступления – преступления, которые невозможно совершить без использования компьютерных сетей и информационных систем, включая взлом систем, создание вредоносного программного обеспечения и распределенные атаки отказа в обслуживании (DDoS-атаки) на инфраструктуру; во-вторых, cyber-enabled преступления – традиционные преступные деяния, такие как мошенничество, вымогательство, кража и распространение материалов с изображением жестокого обращения с детьми (CSAM), совершенные с использованием информационно-коммуникационных технологий как средства или среды, но которые могут быть совершены и традиционным способом [6, с. 20-25].

Для целей настоящего исследования предлагается следующее определение: дистанционное преступление представляет собой умышленное виновное общественно опасное деяние, совершенное с использованием цифровых технологий и/или сетевой инфраструктуры, при котором субъект преступления удален от места наступления преступного результата, преступная деятельность опосредуется электронными средствами, оставляет следы исключительно в цифровой форме (цифровые артефакты) и часто носит трансграничный характер. Данное определение включает как cyber-dependent, так и cyber-enabled деликты, поскольку объединяющим признаком являются именно дистанционность, опосредование информационно-коммуникационными технологиями и цифровая природа следов.

Классическим и фундаментальным признаком дистанционного преступления является географическая и физическая удаленность лица, совершающего преступление, от места, где происходит преступное событие или наступают его последствия. Если при традиционном грабеже преступник находился в том же месте, что и жертва, и похищенное имущество, то при онлайн-мошенничестве мошенник может находиться в другой стране и манипулировать жертвой через интернет, осуществляя преступные действия посредством электронных коммуникаций. Эта удаленность создает серьезные вызовы для установления юрисдикции и возбуждения уголовного преследования, поскольку требуется установить место совершения преступления в соответствии с процессуальными нормами, что может быть затруднено в условиях трансграничного характера преступной деятельности.

Дистанционное преступление обязательно совершается с использованием определенной технологической инфраструктуры, включающей компьютеры, мобильные устройства и оборудование интернета вещей (IoT), интернет, облачные сервисы и платформы социальных сетей, а также криптографические и анонимизирующие технологии, такие как виртуальные частные сети (VPN), сеть Tor и криптовалюты [9, с. 121-129]. Эта опосредованность означает, что преступная деятельность не оставляет физических следов, характерных для традиционных преступлений (отпечатки пальцев, следы ног), а ее материальное воплощение существует исключительно в электронной форме, что существенно отличает дистанционные преступления от классических преступлений и требует применения специальных методик криминалистического анализа.

В отличие от традиционных преступлений, где доказательства включают осмотр места происшествия, вещественные доказательства и показания свидетелей, дистанционные преступления оставляют только цифровые артефакты, к которым относятся логи серверов, истории сетевого трафика, метаданные файлов, записи платежей в криптовалютных блокчейнах и сообщения в мессенджерах. Эти следы характеризуются высокой

волатильностью, то есть могут быть удалены, изменены или переписаны, требуют специальных криминалистических методов извлечения и верификации, а также сталкиваются с серьезными проблемами шифрования и анонимности, которые затрудняют их анализ и использование в качестве доказательств.

Большинство дистанционных преступлений носят трансграничный характер, что означает, что преступник, жертва, хранилища данных и платежные системы могут находиться в разных странах, создавая юрисдикционные конфликты и требуя международного сотрудничества. Новые акты Европейского союза (Regulation 2023/1543, Directive 2023/1544) прямо направлены на ускорение трансграничного доступа к электронным доказательствам через механизмы European Production Order и European Preservation Order, минуя традиционные и часто медленные каналы взаимной правовой помощи между государствами.

Субъекты дистанционных преступлений часто используют технологии анонимизации (Tor, VPN, прокси-серверы), криптовалюты и шифрование для скрывания своей личности и следов деятельности. Высокий уровень анонимности и криптографической защиты ведет к затруднениям в установлении личности преступника, требует применения специальных методов криминалистического анализа и может служить отягчающим фактором при расследовании, повышая уровень сложности криминалистического обеспечения.

На основе зарубежной литературы и исследований, проведенных Williams и коллегами (2022), Black и коллегами (2023) и другими авторами, предлагается следующая типология дистанционных и cyber-enabled преступлений, отражающая разнообразие форм преступной деятельности в цифровую эпоху. Первая категория включает мошенничество и кражу, примерами которых являются онлайн-мошенничество, фишинг, фрод платежных систем и кража личных данных, характеризующиеся удаленным манипулированием жертвой, использованием методов социальной инженерии

и осуществлением цифровых платежей. Вторая категория охватывает вымогательства и угрозы, такие как «виртуальные похищения» (virtual kidnapping), вымогательство с использованием интимных материалов (sextortion) и конвертация криптовалют, совершаемые посредством удаленной коммуникации и использования видеоконференций, с требованием криптовалютных платежей. Третья категория включает распределение вредоносного программного обеспечения и хакерские атаки, включая ботнеты, DDoS-атаки, программное обеспечение для сбора платежей (ransomware) и создание вредоносных программ, совершаемые через компьютерные сети и ведущие к утечке данных и инфраструктурным атакам. Четвертая категория охватывает распространение материалов, изображающих жестокое обращение с детьми (CSAM), включая распространение, хранение в облаке и потоковую передачу таких материалов через специальные платформы с криптографическим скрыванием контента. Пятая категория включает финансовые преступления, такие как отмывание денег и финансирование терроризма через криптовалютные сети, совершаемые посредством блокчейн-транзакций и трансграничных переводов. Наконец, шестая категория охватывает преступления, связанные с интеллектуальной собственностью и корпоративным шпионажем, включая кражу корпоративных данных и утечки исходного кода, совершаемые путем удаленного доступа и использования сетевых инструментов. Эта типология показывает, что дистанционные преступления охватывают практически все традиционные категории правонарушений, переведенные в онлайн-среду и адаптированные к цифровым технологиям.

Собирание цифровых доказательств требует специальных знаний и методик, существенно отличающихся от традиционной криминалистики и криминального расследования. К ключевым вызовам при работе с цифровыми доказательствами относится необходимость документирования полной цепи передачи данных (Chain of Custody) от момента обнаружения до предъявления в суде, поскольку малейшее нарушение может сделать доказательство

недопустимым и исключить его из судебного разбирательства. Кроме того, требуется криптографическая аутентификация и защита целостности файлов через вычисление хеш-сумм, позволяющие убедиться в том, что данные не были изменены или подделаны. Электронные доказательства характеризуются высокой волатильностью, так как легко удаляются или изменяются, что требует срочного сохранения и резервного копирования с соблюдением специальных процедур. Значительную проблему представляют данные, часто зашифрованные, что затрудняет их анализ и атрибуцию виновного лица.

Европейский союз в 2023 году принял революционные регламенты (Regulation 2023/1543 и Directive 2023/1544), вводящие механизмы European Production Order (EPO) и European Preservation Order (EPrO), которые позволяют национальным судам напрямую запрашивать данные у сервис-провайдеров в других странах без громоздких и временных затратных процедур взаимной помощи. Эти механизмы значительно ускоряют получение доказательств, однако создают новые риски для справедливого судебного разбирательства, поскольку гарантии проверки законности вмешательства и защиты прав личности ослабляются. Решение Суда справедливости Европейского союза по делу EncroChat, вынесенное в 2024 году, подтвердило необходимость материальной проверки методов получения доказательств даже в рамках упрощенных процедур, установив важный прецедент для защиты прав обвиняемых.

Современные поставщики услуг, включая Google, Meta и Microsoft, используют системы искусственного интеллекта для фильтрации, категоризации и анализа содержимого с целью выявления материалов жестокого обращения с детьми, террористического контента и другого преступного содержимого [16, с.89-115]. Однако использование искусственного интеллекта в криминалистическом анализе сопряжено с рядом проблем: алгоритмические методы часто не раскрываются полностью поставщиками услуг; существует риск ложных положительных результатов и смещений в обучении моделей; обвиняемый имеет право знать методы анализа

и оспорить результаты в соответствии с требованиями Регламента об общей защите данных (GDPR) статья 22 и Европейской конвенции по правам человека (ECHR) статья 6.

Новизна проведенного исследования состоит в нескольких взаимосвязанных тезисах. Во-первых, предложено комплексное определение дистанционного преступления, охватывающее как cyber-dependent, так и cyber-enabled деликты, что позволяет унифицировать подходы к классификации преступлений в цифровую эпоху. Во-вторых, выделены пять ключевых признаков дистанционности, включая удаленность субъекта, опосредование информационно-коммуникационными технологиями, цифровые артефакты как единственный источник доказательств, трансграничный характер и высокий уровень анонимности. В-третьих, адаптирована международная типология cyber-enabled преступлений, разработанная Williams, Black и другими авторами, к российскому правовому контексту и специфике отечественной криминалистической практики. В-четвертых, проведен анализ новых европейских инструментов получения цифровых доказательств и их потенциала для развития российской системы уголовного процесса. В-пятых, выявлены лакуны в российском Уголовном процессуальном кодексе и Уголовном кодексе Российской Федерации, требующие совершенствования в области определения дистанционности преступлений и допустимости цифровых доказательств.

Область применения результатов исследования включает несколько ключевых направлений. В сфере законотворчества результаты могут быть использованы при совершенствовании Уголовного процессуального кодекса Российской Федерации в части процедур получения, верификации и использования цифровых доказательств, что повысит эффективность уголовного преследования. В криминалистической практике рекомендуется применение международных стандартов chain of custody и криптографической верификации, позволяющих привести российскую практику в соответствие с мировыми стандартами. В судебной практике результаты способствуют

разработке критериев оценки допустимости и достоверности цифровых доказательств, обеспечивая справедливость судебного разбирательства. В сфере образования предлагается преподавание криминалистики с включением новых методик анализа цифровых артефактов в программы высших учебных заведений, подготавливая новое поколение специалистов.

На основе проведенного анализа государственного законодательства, международного права и доктринальных источников предлагаются следующие меры по совершенствованию российского законодательства и криминалистической практики. Во-первых, целесообразно введение четкой дефиниции дистанционного преступления в Общую часть Уголовного кодекса Российской Федерации с указанием ключевых признаков, что позволит унифицировать подходы в правоприменительной практике. Во-вторых, требуется расширение понятия преступлений в сфере компьютерной информации на все cyber-enabled деликты, а не только на cyber-dependent преступления, охватывая всю совокупность дистанционных преступлений. В-третьих, необходима разработка специального Федерального закона о цифровых доказательствах с установлением минимальных стандартов chain of custody, криптографической верификации и допустимости, обеспечивающего надежность доказательств. В-четвертых, следует адаптировать процедуры трансграничного доступа к данным, в частности путем внедрения механизмов, подобных European Production Order, что ускорит получение электронных доказательств. В-пятых, требуется целенаправленная подготовка кадров, включая создание специализированных программ для следователей, судей и экспертов по криминалистике цифровых следов. В-шестых, необходима унификация терминологии в российском законодательстве, доктрине и правоприменительной практике для избежания путаницы между cyber-dependent и cyber-enabled преступлениями, что облегчит понимание и применение уголовного закона.

Дистанционные преступления представляют собой качественно новый класс правонарушений, отличающихся от традиционных преступлений

опосредованием цифровыми технологиями, удаленностью субъекта от места наступления последствий, оставлением исключительно цифровых следов и часто трансграничным характером совершаемых деяний. Типология cyber-enabled преступлений, разработанная в международной доктрине исследователями Williams, Black и другими авторами, охватывает практически все традиционные категории уголовных деяний, переведенные в онлайн-среду: от мошенничества и вымогательства до распространения материалов жестокого обращения с детьми и финансовых преступлений, совершаемых с использованием цифровых технологий.

Криминалистическое обеспечение расследования дистанционных преступлений требует применения специальных методов сбора, верификации и анализа цифровых доказательств, соответствия требованиям chain of custody, криптографической аутентификации и обеспечения справедливого суда при использовании ИИ-аналитики, что существенно отличает эту сферу от традиционной криминалистики. Новые акты Европейского союза (Regulation 2023/1543, Directive 2023/1544) демонстрируют международное направление развития права в данной сфере и определяют вектор дальнейших преобразований.

Российское уголовное законодательство и криминалистическая практика нуждаются в комплексном совершенствовании и адаптации к реалиям цифровой эпохи: требуется введение четкого определения дистанционных преступлений, разработка комплексного законодательства о цифровых доказательствах, адаптация процедур трансграничного доступа к электронным доказательствам, а также подготовка специалистов в области криминалистики цифровых артефактов. Только таким образом российская правоохранительная система сможет эффективно противодействовать новому классу преступлений, характерному для цифровой эпохи и представляющему серьезную угрозу для безопасности и правопорядка в обществе.

Список литературы

1. Phillips K. et al. Conceptualizing cybercrime: Definitions, typologies and taxonomies //Forensic sciences. – 2022. – Т. 2. – №. 2. – С. 379-398.

2. Perina A. S. Digital crimes: concept, typology, signs //Juridical Journal of Samara University. – 2023. – Т. 9. – №. 3. – С. 106-115.

3. Perez S. O. Proliferation of e-Evidence: Reliability Standards and the Right to a Fair Trial //European Journal of Crime, Criminal Law and Criminal Justice. – 2025. – Т. 33. – №. 1-2. – С. 187-211.

4. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (в ред. от 01.01.2024) // Собрание законодательства РФ. 1996. № 25. Ст. 2954. Гл. 28 «Преступления в сфере компьютерной информации».

5. Maras M. H., Arsovska J. Understanding the intersection between technology and kidnapping: A typology of virtual kidnapping //International Criminology. – 2023. – Т. 3. – №. 2. – С. 162-176.

6. Williams M., Laskaris G., Yip M. Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies // In: Comprehensive Cybersecurity Handbook. 2022. P. 20–25.

7. Авторское определение дистанционных преступлений, синтезирующее международную практику и доктрину (без публикации).

8. Veena K. et al. Cybercrime: identification and prediction using machine learning techniques //Computational Intelligence and Neuroscience. – 2022. – Т. 2022. – №. 1. – С. 8237421.

9. Tiutiunyk I. et al. Classifying cybercrime networks: organized and transnational schemes in the digital era //Socio-economic relations in the digital society. – 2024. – Т. 3. – №. 53. – С. 121-129.

10. Unmasking Cybercrime with Artificial-Intelligence-Driven Cybersecurity Analytics // MDPI. 2023. Issue 6. URL: **https://www.mdpi.com/1999-5903/15/6/317** (дата обращения: 12.11.2025).

11. Tosza S., Ligeti K. Cross-border access to electronic evidence in criminal matters: The new EU legislation and the consolidation of a paradigm shift // European Criminal Law Review. 2024. Vol. 14, Issue 2. P. 123–157.

12. Ahmed S., Kumar V., Zhang Y. et al. Recent Advancements in Machine Learning for Cybercrime Prediction // arXiv. 2023. URL: **https://arxiv.org/abs/2310.02541** (дата обращения: 12.11.2025).

13. Wąsek-Wiaderek M., Michałowicz M. The EU E-evidence Package from the Polish Perspective: High Time for a Systemic Change // Studia Iuridica Lublinensia. 2024. Vol. 33, No. 5. P. 421–445.

14. Regulation (EU) 2023/1543 on European Production Orders and Preservation Orders for electronic evidence in criminal matters // Official Journal of the European Union. L 192. 30.07.2023.

15. Case C-670/22 (EncroChat), ECLI:EU:C:2024:336 // Judgment of the Court of Justice of the European Union of 30.04.2024.

16. Spajić J., Jovašević D. Algorithmic Evidence in Criminal Trials: Admissibility, Explainability, and Fair-Trial Guarantees // International Journal of Criminal Justice. 2025. Vol. 12, Issue 1. P. 89–115.

References:

1. Phillips K. et al. Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies // Forensic Sciences. 2022. Vol. 2. No. 2. P. 379–398.

2. Perina A. S. Digital Crimes: Concept, Typology, Signs // Juridical Journal of Samara University. 2023. Vol. 9. No. 3. P. 106–115.

3. Perez S. O. Proliferation of E-Evidence: Reliability Standards and the Right to a Fair Trial // European Journal of Crime, Criminal Law and Criminal Justice. 2025. Vol. 33. No. 1–2. P. 187–211.

4. Criminal Code of the Russian Federation of 13.06.1996 No. 63-FZ (as amended as of 01.01.2024) // Sobranie Zakonodatel'stva RF. 1996. No. 25. Art.

2954. Ch. 28 "Crimes in the Sphere of Computer Information" [Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (в ред. от 01.01.2024) // Собрание законодательства РФ. 1996. № 25. Ст. 2954. Гл. 28 "Преступления в сфере компьютерной информации"].

5. Maras M. H., Arsovska J. Understanding the Intersection Between Technology and Kidnapping: A Typology of Virtual Kidnapping // International Criminology. 2023. Vol. 3. No. 2. P. 162–176.

6. Williams M., Laskaris G., Yip M. Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies // In: Comprehensive Cybersecurity Handbook. 2022. P. 20–25.

7. Author's Definition of Remote Crimes, Synthesizing International Practice and Doctrine (Unpublished) [Авторское определение дистанционных преступлений, синтезирующее международную практику и доктрину (без публикации)].

8. Veena K. et al. Cybercrime: Identification and Prediction Using Machine Learning Techniques // Computational Intelligence and Neuroscience. 2022. Vol. 2022. No. 1. P. 8237421.

9. Tiutiunyk I. et al. Classifying Cybercrime Networks: Organized and Transnational Schemes in the Digital Era // Socio-economic Relations in the Digital Society. 2024. Vol. 3. No. 53. P. 121–129.

10. Unmasking Cybercrime with Artificial-Intelligence-Driven Cybersecurity Analytics // MDPI. 2023. Issue 6. URL: https://www.mdpi.com/1999-5903/15/6/317 (accessed: 12.11.2025).

11. Tosza S., Ligeti K. Cross-border Access to Electronic Evidence in Criminal Matters: The New EU Legislation and the Consolidation of a Paradigm Shift // European Criminal Law Review. 2024. Vol. 14. Issue 2. P. 123–157.

12. Ahmed S., Kumar V., Zhang Y. et al. Recent Advancements in Machine Learning for Cybercrime Prediction // arXiv. 2023. URL: https://arxiv.org/abs/2310.02541 (accessed: 12.11.2025).

13. Wąsek-Wiaderek M., Michałowicz M. The EU E-evidence Package from the Polish Perspective: High Time for a Systemic Change // Studia Iuridica Lublinensia. 2024. Vol. 33. No. 5. P. 421–445.

14. Regulation (EU) 2023/1543 on European Production Orders and Preservation Orders for Electronic Evidence in Criminal Matters // Official Journal of the European Union. L 192. 30.07.2023.

15. Case C-670/22 (EncroChat), ECLI:EU:C:2024:336 // Judgment of the Court of Justice of the European Union of 30.04.2024.

16. Spajić J., Jovašević D. Algorithmic Evidence in Criminal Trials: Admissibility, Explainability, and Fair-Trial Guarantees // International Journal of Criminal Justice. 2025. Vol. 12. Issue 1. P. 89–115.