Дата поступления рукописи в редакцию: 02.12.2025 г. DOI: 10.24412/3034-4395-2025-4-92-95
Дата принятия рукописи к печати: 03.12.2025

***ДЕНИСОВ Максим Денисович,***
*магистр*
*Тамбовского государственного университета имени Г.Р. Державина,*
*e-mail: maksim.denisov.1999@list.ru*

# ПОНЯТИЕ И ВИДЫ КОМПЬЮТЕРНОГО МОШЕННИЧЕСТВА: ТЕОРЕТИЧЕСКИЕ ПОДХОДЫ И КЛАССИФИКАЦИИ

**Аннотация.** *Статья посвящена теоретическому анализу понятия и видов компьютерного мошенничества, рассматриваемого в контексте уголовного законодательства Российской Федерации. Рассматриваются современные подходы к классификации данного вида преступлений, выделяются механизмы совершения мошеннических действий в цифровой среде, а также анализируются особенности правовой квалификации деяний в рамках ст. 159 УК РФ и смежных норм.*

**Ключевые слова:** *компьютерное мошенничество, киберпреступность, ст. 159 УК РФ, электронные платежные системы, фишинг, информационная безопасность, классификация преступлений, криминологический подход.*

***DENISOV Maksim Denisovich,***
*Master's student*
*of the Tambov State University named after G. R. Derzhavin*

# CONCEPT AND TYPES OF COMPUTER FRAUD: THEORETICAL APPROACHES AND CLASSIFICATIONS

**Annotation.** *The article is devoted to a theoretical analysis of the concept and types of computer fraud, considered in the context of the criminal legislation of the Russian Federation. Modern approaches to the classification of this type of crime are examined, the mechanisms of committing fraudulent actions in the digital environment are highlighted, and the features of the legal qualification of acts under Article 159 of the Criminal Code of the Russian Federation and related provisions are analyzed.*

**Key words:** *computer fraud, cybercrime, Article 159 of the Criminal Code of the Russian Federation, electronic payment systems, phishing, information security, crime classification, criminological approach.*

Компьютерное мошенничество представляет собой одну из наиболее актуальных форм преступной деятельности в условиях стремительного развития информационных технологий. Оно характеризуется использованием средств вычислительной техники, сетевых коммуникаций и программного обеспечения для совершения действий, направленных на незаконное завладение чужим имуществом либо получением иных имущественных выгод. Теоретическое понимание этого явления формируется на стыке криминологии, информационной безопасности и права, что обуславливает необходимость комплексного подхода к его изучению.

С точки зрения юридической науки, компьютерное мошенничество подпадает под определение, установленное в рамках уголовного законодательства Российской Федерации, в частности ст. 159 УК РФ, где мошенничество рассматривается как хищение чужого имущества или приобретение права на имущество путём обмана или злоупотребления доверием. Современная трактовка

криминалистической практики расширяет это понятие, учитывая, что использование информационных технологий позволяет скрывать источники преступной деятельности, изменять или подделывать электронные данные и документы, а также обеспечивать анонимность субъекта преступления. Важной особенностью компьютерного мошенничества является его потенциальная масштабность и быстрота воздействия на многочисленные объекты одновременно, что отличает его от традиционных форм мошенничества [1].

Классификационные подходы к компьютерному мошенничеству в научной литературе строятся на основе анализа механизмов совершения преступления, используемых технологий и способов воздействия на потерпевшего. Среди выделяемых категорий исследователи различают мошенничество с использованием электронных платежных систем, фишинговые атаки, мошенничество в сфере онлайн-торговли, а также программы-вымогатели и кибершпионаж, предполагающий извлечение денежных средств под угрозой распространения конфиденциальной информации. Классификация также может опираться на субъектную характеристику преступления, разделяя действия, совершаемые индивидуальными пользователями, организованными группами и киберпреступными сообществами, что имеет значение для прогнозирования рисков и разработки профилактических мер.

Теоретические подходы к изучению компьютерного мошенничества включают криминологический, юридический и социально-психологический аспекты. Криминологический подход концентрируется на выявлении факторов, способствующих совершению преступлений в информационном пространстве, таких как техническая подкованность субъектов, доступность цифровых ресурсов и уязвимость информационных систем. Юридическая перспектива направлена на уточнение состава преступления, определение объективной и субъективной стороны деяния, а также соотношение с действующими нормами УК РФ и международными стандартами кибербезопасности. Социально-психологический анализ акцентирует внимание на мотивации преступников, влиянии сетевых культур и особенностях взаимодействия с потенциальными жертвами [2].

На основе совокупного анализа теоретических подходов формируется понимание необходимости комплексного регулирования компьютерного мошенничества, которое включает как совершенствование уголовного законодательства, так и развитие технологических и организационных мер защиты информации. В российской правоприменительной практике наблюдается постепенное расширение норм УК РФ, направленных на охрану имущественных и нематериальных интересов граждан в цифровой среде, что отражает динамику информационного общества и возрастающие требования к безопасности электронных коммуникаций.

Современное компьютерное мошенничество характеризуется высокой динамичностью и адаптивностью, что отражает развитие цифровых технологий и изменение моделей поведения пользователей в информационном пространстве. Преступные действия в этой сфере нередко скрываются за сложными алгоритмами, автоматизированными системами и криптографическими средствами, что создаёт дополнительные трудности для правоохранительных органов. В этой связи ключевой задачей криминологической науки является не только идентификация видов и методов мошенничества, но и анализ структурных закономерностей его возникновения, а также выявление факторов, способствующих распространению преступлений в цифровой среде.

Одним из существенных аспектов является соотношение компьютерного мошенничества с традиционными формами хищений. Если классическое мошенничество опирается на прямое взаимодействие между преступником и потерпевшим, то в цифровой среде зачастую отсутствует физический контакт, а воздействие осуществляется через манипуляцию информацией, программное обеспечение и дистанционные каналы связи. Это требует корректировки юридической квалификации деяний и применения ст. 159 УК РФ с учётом особенностей электронных доказательств и цифровых следов, что подтверждается судебной практикой последних лет [3].

В научной литературе выделяется несколько методологических подходов к системати-

зации компьютерного мошенничества. Одни авторы акцентируют внимание на объекте посягательства, выделяя имущественные и нематериальные виды ущерба, включая незаконное присвоение денежных средств, интеллектуальной собственности и персональных данных. Другие исследователи предлагают классификацию, ориентированную на используемые технические средства и программные методы, что позволяет выделять фишинг, кейлоггинг, социальную инженерию, применение вредоносного ПО и схемы финансовых манипуляций через электронные платформы. Такой подход обеспечивает понимание не только самого факта преступления, но и механизмов его реализации, что важно для профилактики и расследования [4].

С точки зрения уголовного права, актуальность исследования определяется необходимостью точного разграничения понятий «мошенничество», «компьютерное преступление» и «киберпреступление». Хотя термин «компьютерное мошенничество» в УК РФ напрямую не выделен, его действия квалифицируются через ст. 159, а также в ряде случаев в совокупности с нормами о незаконном доступе к компьютерной информации (ст. 272 УК РФ), распространении вредоносных программ (ст. 273 УК РФ) и хищении средств с использованием электронных платежных систем (ст. 159.6 УК РФ). Это позволяет правоприменителям учитывать специфику цифровой среды и формировать комплексные меры правовой защиты.

Важно отметить, что превентивная функция законодательства в области компьютерного мошенничества предполагает не только установление уголовной ответственности, но и стимулирование разработки технологических стандартов безопасности, образовательных программ по киберграмотности и внутреннего контроля организаций. Современные исследования подчеркивают необходимость интеграции юридических, технических и социально-психологических мер для эффективного противодействия киберпреступности, что отражает глобальную тенденцию перехода к многоуровневой модели защиты информации [5].

Таким образом, компьютерное мошенничество следует рассматривать как многоплановое явление, включающее правовые, криминологические и технические аспекты. Ключевым элементом в изучении и классификации данного феномена является учет механизмов воздействия на объекты преступления, мотивации и организационной структуры субъектов, а также особенностей современного информационного общества. Комплексный подход, объединяющий теоретические исследования и практику уголовного права, позволяет создавать эффективные стратегии предупреждения и расследования преступлений в цифровой среде, соответствующие как требованиям УК РФ, так и международным стандартам информационной безопасности.

***Список литературы:***

*[1] Алексеев, Д. С. Мошенничество в сфере компьютерной информации: особенности квалификации и конкуренции со смежными составами преступлений / Д. С. Алексеев // Аллея науки. – 2022. – Т. 1, № 2(65). – С. 508-518.*

*[2] Долженко, Н. И. Мошенничество в сети Интернет / Н. И. Долженко, С. О. Тарасова // Актуальные вопросы борьбы с преступлениями. – 2023. – № 2. – С. 34-37.*

*[3] Модонов, Н. В. Мошенничество в сфере компьютерной информации: понятие и виды / Н. В. Модонов // Молодой ученый. – 2024. – № 50(549). – С. 319-321.*

*[4] Мустаев, В. И. Проблема квалификации преступлений в сфере компьютерной информации / В. И. Мустаев // Следственная деятельность: проблемы, их решение, перспективы развития : Материалы VII Всероссийской молодёжной научно-практической конференции, Москва, 27 ноября 2023 года. – Москва: Московская академия Следственного комитета Российской Федерации, 2024. – С. 163-167.*

*[5] Урванцев, Е. В. Вопросы квалификации преступлений в сфере компьютерной информации / Е. В. Урванцев // Научное образование. – 2023. – № 3(20). – С. 161-165.*

***Spisok literatury:***

*[1] Alekseev, D. S. Moshennichestvo v sfere komp'iuternoi informatsii: osobennosti kvalifikatsii i konkurentsii so smezhnymi sostavami prestuplenii / D. S. Alekseev // Alleia nauki. – 2022. – T. 1, № 2(65). – S. 508-518.*

*[2] Dolzhenko, N. I. Moshennichestvo v seti Internet / N. I. Dolzhenko, S. O. Tarasova // Aktual'nye voprosy bor'by s prestupleniiami. – 2023. – № 2. – S. 34-37.*

*[3] Modonov, N. V. Moshennichestvo v sfere komp'iuternoi informatsii: poniatie i vidy / N. V. Modonov // Molodoi uchenyi. – 2024. – № 50(549). – S. 319-321.*

*[4] Mustaev, V. I. Problema kvalifikatsii prestuplenii v sfere komp'iuternoi informatsii / V. I. Mustaev // Sledstvennaia deiatel'nost': problemy, ikh reshenie, perspektivy razvitiia : Materialy VII Vserossiiskoi molodezhnoi nauchno-prakticheskoi konferentsii, Moskva, 27 noiabria 2023 goda. – Moskva: Moskovskaia akademiia Sledstvennogo komiteta Rossiiskoi Federatsii, 2024. – S. 163-167.*

*[5] Urvantsev, E. V. Voprosy kvalifikatsii prestuplenii v sfere komp'iuternoi informatsii / E. V. Urvantsev // Nauchnoe obrazovanie. – 2023. – № 3(20). – S. 161-165.*