

УДК 343.985.7

# Современные возможности расследования мошенничества, совершенного с использованием высоких технологий<sup>1</sup>

Савельева Ирина Сергеевна, магистрант, Владимирский государственный университет имени А. Г. и Н. Г. Столетовых, savelevaira97@bk.ru

В статье рассматриваются современные возможности расследования мошенничества, совершенного с использованием высоких технологий. Отмечается, что основной характеристикой дистанционного мошенничества в данной сфере является способ его совершения. Анализируются способы совершения мошенничества с использованием высоких технологий и излагаются рекомендации по его предупреждению.

Ключевые слова: мошенничество, наказание, уголовное право, высокие технологии, злоупотребление доверием.

В последние годы цифровые технологии развиваются стремительными темпами, что облегчает коммуникацию, социализацию, ведение бизнеса и повседневную жизнь. Однако вместе с этим растут и угрозы преступности, совершаемой с использованием высоких технологий. Дистанционное мошенничество — одна из наиболее заметных и вредоносных форм преступной деятельности. В 2025 г. эта проблема усугубилась как по масштабам, так и по технической сложности. В статье представлены современные тенденции дистанционного мошенничества, его виды и меры противодействия.

В последние годы в целях повышения эффективности борьбы с преступлениями, совершаемыми с использованием телекоммуникационных и компьютерных сетей, существенные изменения претерпели отдельные положения Уголовного кодекса Российской Федерации. Так, в составы отдельных статей УК РФ введен квалифицирующий признак совершения преступления «с использованием средств массовой информации, в т. ч. информационно-телекоммуникационных сетей (включая сеть Интернет)», а также квалифицирующий признак совершения преступления «с использованием информационно-телекоммуникационных сетей (включая сеть Интернет)». Отдельное правовое закрепление также получили составы «высокотехнологичных» видов мошенничества (ст. 159.3, 159.6 УК РФ) [1].

Между тем, как показывает практика деятельности правоохранительных органов, данные меры являются необходимыми, но не исчерпывающими в вопросах предупреждения как преступлений, совершаемых в сфере информационно-телекоммуникационного пространства в целом, так и мошенничества, совершаемого с использованием телекоммуникационного и компьютерного оборудования, в частности.

Следует также отметить, что особую актуальность теме исследования придает рост числа зарегистрированных преступлений в данной сфере. Преступления, совершаемые с использованием современных компьютерных технологий и средств связи, имеют существенную специфику, которая порождает сложности как в обнаружении фактических действий злоумышленника, так и в определении потенциальной возможности совершения преступления. Общий ущерб в России за 2024 г. уже превысил 170–200 млрд руб. Также зарегистрировано более 640 тыс. случаев дистанционного мошенничества; за десять месяцев 2025 г. — более 564 тыс. преступлений в информационно-коммуникационной

сфере, что на 15,3 % больше по сравнению с аналогичным периодом 2024 г. Количество обращений пострадавших за десять месяцев 2025 г. выросло на 31 % [2].

В настоящее время наиболее распространены следующие способы мошенничества в сфере высоких технологий:

1. Телефонное мошенничество. Мошенники звонят от имени банков, государственных служб, налоговых органов и вводят жертв в заблуждение посредством угроз или обещаний.

2. Фишинг и клонирование аккаунтов. Используются поддельные сайты и приложения для кражи персональных данных; все чаще применяются технологии искусственного интеллекта для создания реалистичных подложных ресурсов.

3. Мошенничество на торговых платформах и в социальных сетях. Продажа несуществующих товаров, обман покупателей на маркетплейсах.

4. Использование искусственного интеллекта в мошеннических целях. Автоматизация атак с помощью чат-ботов, клонирование голоса, создание дипфейков (технологии синтеза медиаконтента с помощью алгоритмов искусственного интеллекта) и персонализированных фишинговых сообщений.

5. Мошенничество с криптовалютами. Фиктивные инвестиционные платформы, кражи из электронных кошельков и с бирж [3, с. 65–67].

Мошенничество в сети Интернет характеризуется прямым умыслом, направленным на незаконное получение чужого имущества или приобретение права на него путем обмана или злоупотребления доверием, возникшим до совершения названных действий, а также корыстной целью. Перечисленные факторы указывают на необходимость выработки специфических мер предупреждения преступлений данного вида и определяют основные направления противодействия им.

## Рекомендации по усилению защиты

Регулярное обучение и информирование пользователей по вопросам распознавания мошеннических схем.

Внедрение многофакторной аутентификации и комплексных систем безопасности с мониторингом.

Законодательное усиление ответственности за мошенничество с использованием искусственного интеллекта.

Объединение усилий бизнеса, государства и общества в целях формирования культуры цифровой безопасности [4].

Таким образом, можно отметить, что дистанционное мошенничество эволюционирует, используя новые технологии и становясь

<sup>1</sup> Научный руководитель: Головинская Ирина Викторовна — профессор кафедры уголовно-правовых дисциплины, Владимирский государственный университет имени А. Г. и Н. Г. Столетовых, профессор кафедры конституционного и муниципального права, Владимирский филиал Российской академии народного хозяйства и государственной службы при Президенте РФ, доктор юридических наук, профессор.

более изощренным. Решение данной проблемы требует комплексного подхода, предусматривающего применение технических, образовательных и правовых мер.

#### **Примечания**

1. Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ // Собрание законодательства РФ. 1996. N 25. Ст. 2954.
2. Статистические сведения о состоянии преступности в Российской Федерации. URL: <https://мвд.рф/dejatelnost/statistics> (дата обращения: 13.11.2025).
3. Евтушенко И. И., Венедиктов А. А. Дистанционные хищения: понятие и признаки // Гуманитарные, социально-экономические и общественные науки. 2020. N 12-2.
4. Майтесян А. М. Мошенничество в сети интернет и способы защиты от него // Международный журнал гуманитарных и естественных наук. 2020. N 5-4.

#### **English version**

Contemporary possibilities for investigating fraud committed using high technologies

Save'eva Irina Sergeevna, master's student, Vladimir State University named after A. G. and N. G. Stoletovs

This article examines contemporary possibilities for investigating fraud committed using high technologies. It is noted that the principal characteristic of remote fraud in this area is the method by which it is committed. The article analyzes methods of committing fraud using high technologies and presents recommendations for its prevention.

Keywords: fraud, punishment, criminal law, high technologies, abuse of trust.