

- ресурс]. — Режим доступа: <https://www.amazon.com/Blockchain-Revolution-Technology-Changing-Business/dp/1101980133> (дата обращения 08.03.2021).
6. Михайлов А.В. Проблемы становления цифровой экономики и вопросы развития предпринимательского права / А.В. Михайлов // Актуальные проблемы российского права. — 2018. — №11(96). — С. 68–70.
7. Сушкова О.В. Влияние интеллектуальных систем на развитие условий реализации экономических прав граждан в цифровой среде / О.В. Сушкова // Правовая защита интеллектуальной собственности: проблемы теории и практики: сб. материалов IX Междунар. юридич. форума (IP Форума). — М.: ИЦ Ун-та им. О.Е. Кутафина (МГЮА), 2021. — С. 282–287.

## МОШЕННИЧЕСТВО В ИННОВАЦИОННОЙ СРЕДЕ

## FRAUD IN AN INNOVATIVE ENVIRONMENT

### Костюк Михаил Федорович

*Доктор юридических наук, профессор, профессор кафедры экономических и финансовых расследований ВШГА МГУ имени М. В. Ломоносова*



### Kostjuk Mihail Fedorovich

*Doctor of Law, Professor, Professor of the Department of Economic and Financial Investigations of the Higher School of Economics, Lomonosov Moscow State University*

### Василихина Юлия Владимировна

*Студентка 2-го курса Высшей школы государственного аудита Московский государственный университет имени М.В. Ломоносова*



### Vasilihina Julija Vladimirovna

*2nd year student of the Graduate School of State Audit, Moscow State University named after M.V. Lomonosov*

**Аннотация:** развитие компьютерных и информационно-телекоммуникационных технологий имеет положительные стороны, но в то же время порождает и негативные последствия, выраженные в возникновении новых видов мошенничества, посредством использования технологических достижений современности. В связи с чем возникает необходимость криминализации противоправных деяний, причиняющих вред объекту посягательства и внесения изменений в законодательные положения, которые позволят правоприменителю едино толковать существующие уголовно-правовые нормы, посвященные мошенничеству, что надлежит рассмотреть в данной статье.

**Ключевые слова:** мошенничество, информационные технологии, инновационное мошенничество.

**Abstract:** The development of computer and information and telecommunication technologies has positive aspects, but at the same time generates negative consequences, expressed in the emergence of new types of fraud, through the use of modern technological achievements. In this connection, it becomes necessary to criminalize unlawful acts that harm the object of encroachment and amend the legislative provisions that will allow the law enforcement officer to unify the interpretation of the existing criminal law norms on fraud, which should be considered in this article.

**Keywords:** fraud, information technology, innovative fraud.

Развитие инновационных технологий в современном обществе имеет значительную роль, поскольку позволяет улучшить качественные показатели жизнедеятельности человека. Однако, стоит отметить, что прогресс в той или иной сфере имеет и обратную сторону. Развитие инновационных, а в частности, компьютерных и информационно — телекоммуникационных технологий является основной для зарождения ранее не существовавших преступных посягательств. Важным является замечание и о том, что «высокие

технологии» — это не только лишь компьютеры, но и иные специальные технологии, предоставляющие возможность негласного получения информации, развитие и внедрение которых имеет значительные темпы, что расширяет возможности их использования в преступных целях [1]. Исключением тому не стало и мошенничество, что породило необходимость криминализации его квалифицированных видов в уголовном законодательстве Российской Федерации.

До 29 ноября 2012 года данная сфера правоотношений оставалась законодательно неурегулированной, в следствие чего мошенничество в сфере компьютерной информации квалифицировалось по статье 159 УК РФ как «хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием», что не соответствовало характеру и степени общественной опасности преступления и личности виновного, а то есть противоречило целям наказания, применяемого к лицу, совершившему преступления в соответствии с положениями ст. 43 УК РФ [2]. Однако Федеральным законом от 29.11.2012 № 207 «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» [3] в уголовное законодательство были внесены изменения, направленные на дифференциацию различных видов мошенничества, в том числе в сфере экономической деятельности. В частности, уголовный закон был дополнен ст. 159<sup>1</sup> — 159<sup>6</sup> УК РФ, которые предусмотрели ответственность за мошенничество, совершаемое в сфере кредитования, предпринимательской деятельности, страхования, компьютерной информации, а также при получении выплат или использования платежных карт [4], что позволило правоприменителю производить более точную уголовно-правовую оценку конкретного общественно-опасного деяния, но вместе с тем вызвало острую дискуссию в научном сообществе, в силу отсутствия устойчивой и однородной правоприменительной практики.

Особое значение для данного исследования имеет ст. 159<sup>6</sup>, посвященная мошенничеству в сфере компьютерной информации, а то есть «хищению чужого имущества или приобретению права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации или информационно-телекоммуникационных сетей», состав которого для полноты исследования следует рассмотреть далее.

Диспозиция ст. 159<sup>6</sup> имеет бланкетный характер и требует привлечения дополнительной информации из сопутствующего законодательства РФ для установления признаков состава преступления. Основным непосредственным объектом рассматриваемого преступления выступают общественные отношения, связанные с отношениями собственности независимо от ее формы, дополнительным — правоотношения обеспечивающие информационную безопасность. Предметом данного преступления является чужое имущество, право на чужое имущество, а также компьютерная информация, используя которую виновное лицо достигает преступных целей. В свою очередь «компьютерной информацией» согласно примечанию к ст. 272 УК РФ являются «сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи». Объективная сторона выражена общественно опасными деяниями в виде хищения чужого имущества или приобретения прав на него, общественно-опасным последствием в качестве при-

чинения имущественного ущерба собственнику и причинно-следственной связью между ними. Дополнительным признаком объективной стороны выступает способ совершения преступления, характеризующийся альтернативно как: ввод, удаление, блокирование, модификация компьютерной информации, а также вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей [5]. Следовательно, по конструкции объективной стороны состав является материальным. Согласно п. 5 Постановления Пленума Верховного суда РФ № 48 от 30.11.2017 «О судебной практике по делам о мошенничестве, присвоении и растрате» преступление считается оконченным с момента, «когда имущество поступило в незаконное владение виновного или других лиц и они получили реальную возможность пользоваться или распорядиться им по своему усмотрению». Субъективная сторона характеризуется прямым умыслом и корыстным мотивом, а то есть стремлением получить материальную выгоду. Субъектом преступления выступает вменяемое физическое лицо, достигшее возраста шестнадцати лет.

Важным является замечание о том, что данные преступные деяния являются наиболее распространенными в преступной среде, чему свидетельствуют статистические данные преступности, приведенные Министерством внутренних дел за январь-февраль 2021 года. Так, за данный отчетный период число преступлений, совершенных мошенническим путем в сфере компьютерной информации возросло на 51,9%, в том числе — на 48,3% с использованием сети «Интернет» и на 32,6% с использованием средств мобильной связи по сравнению с показателями предшествующего периода [6]. Актуальность данной нормы обусловлена и наличием проблем в квалификации преступлений, совершенных путем мошенничества в сфере компьютерной информации, а также отсутствием единообразного подхода в применении судами нормы, предусматривающей ответственность за данное преступление, что вызывает острые дискуссии в научной среде.

Так, М.В. Андрианов считает необоснованным необходимость выделения данного состава преступления, поскольку рассматриваемое деяние является лишь одним из способов совершения мошенничества [7]. Противоположного мнения придерживается В.М. Елина, которая считает необходимым криминализацию компьютерного мошенничества, поскольку это дает возможность Российской Федерации принимать участие в мировых интеграционных процессах в сфере борьбы с киберпреступностью. Ряд авторов придерживается мнения о том, что данная норма должна предусматривать ответственность за хищение вне зависимости от способа, если при этом используется несанкционированное вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей [8]. Другие же

ученые, в частности И.А. Александрова считает, что данное деяние следует квалифицировать как кражу, поскольку компьютер — не физическое лицо, а фактически устройство, как и банкомат [9].

Не имеет единообразного подхода в применении данной нормы и правоприменитель, который сталкивается с определенными трудностями в квалификации хищения с использованием компьютерной информации, в следствие чего однородным преступным деяниям даются различные правовые оценки в виде кражи, общего мошенничества или мошенничества в сфере компьютерной информации, подтверждением чему судебная практика.

Так, согласно обвинительному приговору Октябрьского районного суда Ханты-мансийского автономного округа от 17 декабря 2013 года, лицо, используя забытый пассажиром в салоне мобильный телефон и содержащуюся в нем систему «Телекард», перечислило денежные средства, находящиеся на балансе счета потерпевшего, открытого в ОАО «Газпром», на баланс своего мобильного телефона и на свой электронный кошелек «Яндекс.Деньги», в следствие чего было признано судом виновным по ч.1 ст. 158 УК РФ [10].

В то же время, Железногорский городской суд Курской области, квалифицировал деяния лица, которое используя мобильный телефон, посредством услуги «Мобильный банк», подключенной предыдущим владельцем ФИО7 для доступа к банковскому счету ПАО «Сбербанк» и посредством отправления специального сообщения на номер «900», незаконно осуществило снятие со счета банковской карты, оформленной на ФИО7, денежных средств, которые посредством услуги «Мобильный банк» были автоматически зачислены на счет виновного по ч.2 ст.159.6 УК РФ [11].

Подводя итоги всему вышесказанному, становится очевидным, что рассматриваемая норма требует должного внимания со стороны законодателя, поскольку существует ряд проблем в ее применении, поскольку зачастую суды однородные преступные деяния квалифицирует различно, как общее мошенничество, кражу или мошенничество в сфере компьютерной информации. Также остается неразрешенным вопросом о том, что считать вмешательством в функционировании средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей. Негативная тенденция в правоприменительной практике подлежит устранению, так как отсутствие единого подхода в применении нормы, предусматривающей ответственность за совершение мошенничества в сфере компьютерной информации, в том числе неблагоприятно влияет на авторитет судебной системы Российской Федерации. Вследствие чего, видится воз-

можным, разрешить данную ситуацию посредством более подробных разъяснений Верховного суда РФ о критериях отграничения данного состава от смежных составов преступления, а в частности, путем внесения их в Постановление Пленума Верховного суда РФ № 48 от 30.11.2017 «О судебной практике по делам о мошенничестве, присвоении и растрате».

### Список литературы

1. Мазуров А.В. Преступность в сфере высоких технологий: понятие, общая характеристика, тенденции / А.В. Мазуров // Вестник Томского государственного университета. — 2007. — № 2. — С. 151–154.
2. Федосенко В. Цена высоких технологий. Гендиректор подозревается в присвоении двух миллионов евро / В. Федосенко // Российская газета. — 2008. — 22 апр.
3. Федеральный закон от 29.11.2012 № 207 «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» // СПС «Консультант плюс».
4. Обзор судебной практики по применению ФЗ от 29.11.2012 № 207-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» и постановления Государственной Думы Федерального Собрания РФ от 02.07.2013 № 2559 ГД «Об объявлении амнистии» // СПС «Консультант плюс».
5. Журавлева Г.В. Мошенничество в сфере компьютерной информации: спорные вопросы теории и практики / Г.В. Журавлева, Н.А. Карпова // Вестник москов. ун-та МВД России. 2017. С. 153–158.
6. МВД РФ, ФКУ «Главный информационно-аналитический центр» Состояние преступности в России за январь-февраль 2021 года [Электрон. ресурс]. — Режим доступа: <https://мвд.рф/>.
7. Андрианов М.В. Новые способы мошенничества в УК РФ / М.В. Андрианов // Вестник ВлГУ. — 2013. — № 9. — С. 63.
8. Иванченко Р.Б. Проблемы квалификации мошенничества с использованием информационных технологий / Р.Б. Иванченко, А.Н. Малышев // Уголовное право. — 2015. — № 5. — С. 131–134.
9. Александрова И.А. Новое уголовное законодательство о мошенничестве / И.А. Александрова // Юридическая наука и практика. Вестник Нижегородской академии МВД России. — 2013. — № 21. — С. 54–62.
10. Обвинительный приговор Октябрьского районного суда Ханты-Мансийского автономного округа от 17.12.2013 [Электрон. ресурс]. — Режим доступа: <https://sudact.ru/>.
11. Обвинительный приговор Железногорского городского суда Курской области по делу № 1-243/2014 от 21.10.2014 г. [Электрон. ресурс]. — Режим доступа: <https://sudact.ru/>.