3. Аменицкая Н. А. Взаимодействие следователя и органов, осуществляющих оперативно-розыскную деятельность в раскрытии и расследовании преступлений (в ОВД) : автореф. дис. ... канд. юрид. наук. Н. Новгород, 2016. 32 с.

4. Быков В. М. Психологические аспекты взаимодействия следователя и органа дознания. Омск, 1976. 42 с.

5. Гусев А. В. Организационно-правовые проблемы взаимодействия следователя с лицом, обладающим специальными знаниями // Юристъ-Правоведъ. 2011. № 3. С. 34–38.

6. Косимов О. А. Проблемы взаимодействия следователя с органами дознания на стадии возбуждения уголовного дела по материалам оперативно-розыскной деятельности // Российский следователь. 2011. № 12. С. 31–36.

7. Кругликов А. П. Следственная и следственно-оперативная группы: проблемы взаимодействия следователей и органов дознания при их функционировании // Уголовное право. 2010. № 6. С. 77–84.

УДК 343.3/.7

Белехова Виктория Евгеньевна,
студент, Костромской государственный университет, г. Кострома
viktoriya98000@icloud.com

Belekhova Victoria Evgenievna,
student, Kostroma State University, Kostroma

СОВРЕМЕННЫЕ ПРОБЛЕМЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ С ИСПОЛЬЗОВАНИЕМ КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ

MODERN PROBLEMS OF LEGAL REGULATION OF CRIMES RELATED TO THE USE OF COMPUTER TECHNOLOGIES

В настоящей статье исследуются вопросы мошенничества в сфере компьютерной информации с использованием компьютерных технологий и предлагаются пути решения путем дополнения Уголовного кодекса Российской Федерации новой статьей 165[1].

This article examines the issues of fraud in the field of computer information using computer technology and suggests solutions by supplementing the Criminal code of the Russian Federation with a new article 165[1].

Мошенничество, мошенничество в сфере компьютерной информации с использованием компьютерных технологий, цифровые имущественные преступления, имущественные преступления в сфере цифровой экономики.

Fraud, fraud in the field of computer information using computer technology, digital property crimes, property crimes in the digital economy.

Современный мир характеризуется стремительным развитием информационных отношений, информационно-коммуникационных технологий, а также тотальной компьютеризацией общества. По данным Судебного департамента при Верховном суде Российской Федерации, за преступления в сфере компьютерной информации в 2020 г. осуждено 165 человек, в 2021 г. – 137, а в 2022 г. – уже 225 человек. В 2019 г. число осужденных за преступления, где использование Интернета вменяется как признак, составило 6041 человек, в 2020 г. – 5696, а в 2021 г. – 6726 человек. Президент Российской Федерации В. В. Путин в своем выступлении на сессии онлайн-форума «Давосская повестка дня 2021», организованного Всемирным экономическим форумом, справедливо указал, что в начавшемся третьем десятилетии XXI века трудно не заметить глубинных перемен и коренных трансформаций в глобальной экономике, социальной жизни, технологиях. В то жк время все более значимую роль в жизни общества начинают играть современные технологические и прежде всего цифровые гиганты [4].

Как справедливо замечено в доктрине, общественная опасность – необходимое, неотъемлемое свойство, атрибут преступления, его определяющее качество; ее природа заключена в том, что преступление приносит вред социуму, выступает как «вредоносное посягательство на жизненные условия общества» [5, с. 72]. Не является исключением здесь и «компьютерное» мошенничество – сравнительно новый вид имущественного преступления в области цифровой экономики, информационно-телекоммуникационных сетей, компьютерной информации, имеющее ряд социально-правовых особенностей, отличающих его от традиционного мошенничества как корыстного преступления против собственности.

Следует отметить, что преступления, совершенные с использованием IT-технологий, составляют все большую долю в общей структуре преступности: сегодня она достигла 25 %. Динамика ежегодного прироста фиксируется последние несколько лет. Так, в 2021 г. зарегистрировано более 294 тыс. преступлений, совершенных с использованием информационно-телекоммуникационных технологий, что на 70 % больше, чем за 2020 г. Половина таких преступлений совершается с использованием сети Интернет, а более трети – посредством мобильной связи. Четыре таких преступления (80,0 %) из пяти совершаются путем кражи или мошенничества – 235,5 тыс. (+83,2 %) [6, с. 21].

Федеральным законом от 29 ноября 2012 г. № 207-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» [2] введена статья 159^6 «Мошенничество в сфере компьютерной информации». Федеральным законом от 23 апреля 2018 г. № 111-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации» [3] пункт «в» ч. 3 ст. 159^6 УК РФ изложен в следующей редакции: мошен-

ничество в сфере компьютерной информации, совершенное с банковского счета, а равно в отношении электронных денежных средств.

Эти изменения в уголовном законодательстве России не получили однозначной оценки в науке. Многие исследователи признают несовершенство конструкции ст. 159^6 Уголовного кодекса Российской Федерации (далее – УК РФ, УК) [1], именно поэтому в доктрине можно отметить различные подходы относительно судьбы «компьютерного» мошенничества: выделить в самостоятельный состав, преобразовать или вовсе исключить из уголовного закона, признав квалифицированным видом кражи, предусмотренной п. «г» ч. 3 ст. 158, наконец, переместить в другую главу Особенной части УК.

Согласно позиции отдельных исследователей целесообразно отнести преступление, предусмотренное ст. 159^6, к разновидности мошенничества, уточнив в уголовном законе содержание его объективной стороны и рассматривая использование компьютера лишь как вещественный элемент поражаемых отношений. К примеру, с точки зрения Т. А. Кули-Заде, в составе преступления, описанного в ст. 159^6, целесообразно в качестве основных признаков указать «обман или злоупотребление доверием» [6, с. 23].

Ряд исследователей считают более обоснованным не установление уголовной ответственности за самостоятельный вид преступления «мошенничество в сфере компьютерной информации», а обеспечение дифференциации уголовной ответственности за мошенничество и некоторые другие преступления в сфере экономики путем установления такого квалифицирующего (особо квалифицирующего) обстоятельства, как совершение соответствующего преступления в сфере компьютерной информации или с использованием информационно-телекоммуникационных технологий и сетей.

Так, Т. Ю. Орешкина полагает, что уголовно-правовая норма об ответственности за мошенничество в сфере компьютерной информации является неудачной, и правильнее было бы, исключив ст. 159^6, предусмотреть способ, связанный с вводом, удалением, блокировкой, модификацией компьютерной информации, иным вмешательством в функционирование средств хранения, обработки или передачи компьютерной информации, в качестве квалифицирующего признака «классического» мошенничества [7, с. 187].

Суть хищения, совершаемого с использованием средств электронной техники, состоит в модификации автоматизированной обработки данных компьютерной системы, в результате чего происходит воздействие на результат вводимой и выводимой информации, и, как следствие, видоизменяется информация о переходе имущества либо прав на имущество собственника или иного законного владельца.

Такого рода модификация представляет собой: а) изменение информации, обрабатываемой в компьютерной системе, хранящейся на материальных носителях (машинных, пластиковых) или передаваемой по сетям передачи данных; б) введение в компьютерную систему заведомо ложной информации.

Представляется, что понятие «хищение чужого имущества, совершенное с использованием высоких технологий» в сфере цифровых имущественных отношений неуместно. Использование категории «хищение чужого имущества» подразумевает, что тайность, открытость, удержание, обман и злоупотребление доверием становятся возможными способами совершения компьютерных имущественных преступлений. Однако это далеко не так, потому что компьютерные преступления против собственности обладают другими особенностями и свойствами, совершаются с помощью иных способов и средств.

На наш взгляд, «мошенничество в сфере компьютерной информации с использованием компьютерных технологий» следовало бы считать самостоятельным видом «цифровых» имущественных преступлений (а в будущем возможно даже самостоятельной группой).

В современный период представляется более реалистичным для эффективного уголовно-правового противодействия преступлениям против собственности в сфере компьютерной информации дополнение УК РФ новой статьей 165^1 «Причинение имущественного ущерба путем неправомерного воздействия на объекты в сфере информационно-телекоммуникационной сети и компьютерной информации» и изложение ее в следующей редакции:

«Статья 165^1. «Причинение имущественного ущерба путем неправомерного воздействия на объекты в сфере информационно-телекоммуникационной сети и компьютерной информации»

Причинение имущественного ущерба путем неправомерного воздействия на объекты в сфере информационно-телекоммуникационной сети и компьютерной информации, совершенного с корыстной целью путем использования технических и программных (электронных) средств или устройств, а равно в отношении электронных денежных средств, –

наказывается штрафом в размере до ста двадцати тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного года, либо обязательными работами на срок до трехсот шестидесяти часов, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на срок до трех лет.

То же деяние, совершенное группой лиц по предварительному сговору, а равно с причинением значительного ущерба гражданину, –

наказывается штрафом в размере до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до двух лет, либо обязательными работами на срок до четырехсот восьмидесяти часов, либо исправительными работами на срок до двух лет, либо принудительными работами на срок до пяти лет с ограничением свободы на срок до одного года или без такового, либо лишением свободы на срок до пяти лет с ограничением свободы на срок до одного года или без такового.

Деяния, предусмотренные частями первой или второй настоящей статьи, совершенные:

а) лицом с использованием своего служебного положения;

б) в крупном размере;

в) с банковского счета, –

наказываются штрафом в размере от ста тысяч до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до трех лет, либо принудительными работами на срок до пяти лет с ограничением свободы на срок до двух лет или без такового, либо лишением свободы на срок до шести лет со штрафом в размере до восьмидесяти тысяч рублей или в размере заработной платы или иного дохода осужденного за период до шести месяцев либо без такового и с ограничением свободы на срок до полутора лет либо без такового.

Деяния, предусмотренные частями первой, второй или третьей настоящей статьи, совершенные:

а) организованной группой;

б) путем компьютерной атаки;

в) в особо крупном размере, –

наказываются лишением свободы на срок до десяти лет со штрафом в размере до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период до трех лет либо без такового и с ограничением свободы на срок до двух лет либо без такового.

Основной состав представленной модели преступления (ч. 1) отнесен к категории небольшой тяжести, альтернативное наказание за совершение которого не превышает трех лет лишения свободы. Квалифицированные виды этого преступления (ч. 2) следует признать преступлениями средней тяжести, а особо квалифицированные виды (ч. 3 и 4) – тяжкими преступлениями.

Предложенная конструкция материального состава в отношении указанного выше преступления, момент окончания которого должен быть привязан к зачислению переведенных (списанных) денежных средств на счет виновного или другого лица либо получению виновным иной реальной возможности распоряжаться чужим денежными средствами или иным имуществом по своему усмотрению, в том числе путем обналичивания, оплаты товара, работ или услуг либо совершения других имущественных действий. Как видно, названный момент окончания преступлений соединен с причинением имущественного ущерба, что характерно, повторимся, для конструкции материального состава преступлений. Как видно из проекта, с отнесением конструкции к материальному составу нами одновременно предлагается усилить уголовное наказание за основной и квалифицированные составы анализируемых преступлений.

Покушением на причинение имущественного ущерба путем неправомерного воздействия на объекты в сфере информационно-телекоммуникационной сети и компьютерной информации следует признать, в частности, списание (перевод) безналичных денежных средств с банковского счета независимо от зачисления списанных средств на счет (банковский счет, оператору электронных денежных средств и др.) виновного или иного лица либо получения ука-

занными лицами реальной возможности распоряжаться поступившими средствами по своему усмотрению.

Следует отметить, что мошенничество в сфере компьютерной информации с использованием компьютерных технологий» следует считать самостоятельным видом «цифровых» имущественных преступлений (а в будущем возможно даже самостоятельной группой). С углублением цифровизации назревает потребность в реформировании главы 21 УК РФ путем выделения в последней ряда составов имущественных преступлений в сфере цифровой экономики.

Таким образом, совершенствование уголовного законодательства России, в случае принятия ст. 165^{1} УК РФ, повлечет исключение из УК РФ положений, содержащихся в п. «г» ч. 3 ст. 158 об ответственности за кражу, совершенную с банковского счета, а равно в отношении электронных денежных средств, ст. 159^{3} УК РФ о мошенничестве с использованием электронных средств платежа, а также ст. 159^{6} УК РФ о мошенничестве в сфере компьютерной информации.

СПИСОК ИСТОЧНИКОВ

1. Уголовный кодекс Российской Федерациот 13.06.1996 года№ 63-ФЗ (в редакции от 24.09.2022 года) // Официальный интернет-портал правовой информации. Информационно-правовая система «Законодательство России». URL: www.pravo.gov.ru (дата обращения: 20.09.2022).

2. Федеральный закон Российской Федерации от 29 ноября 2012 года № 207-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельныезаконодательные акты Российской Федерации» // Официальный интернет-портал правовой информации. Информационно-правовая система «Законодательство России». URL: www.pravo.gov.ru (дата обращения: 20.10.2022).

3. Федеральный закон Российской Федерации от 23 апреля 2018 года № 111-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации». URL: www.pravo.gov.ru (дата обращения: 20.10.2022).

4. Давосская повестка дня 2021. URL: http://www.kremlin.ru/events/president/news/64938 (дата обращения: 20.09.2022).

5. Дурманов Н. Д. Понятие преступления. М. : АН СССР, 1948. 311 с.

6. Кули-Заде Т. А. Проблемы квалификации мошенничества в сфере компьютерной информации // Российская юстиция. 2021. № 3. С. 21–25.

7. Орешкина Т. Ю. Преступления в сфере экономики: дифференциация-без границ Уголовное право в эпоху финансово-экономических перемен // Материалы IX Российского Конгресса уголовного права, состоявшегося 29–30 мая 2014 г. / отв. ред. докт. юрид. наук, проф. В. С. Комиссаров. М. : Норма, 2014. С. 186–190.