МОШЕННИЧЕСТВО В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ: УГОЛОВНО-ПРАВОВОЙ И КРИМИНОЛОГИЧЕСКИЙ АСПЕКТ

Савенко Ирина Алексеевна
к.ю.н., доцент, доцент кафедры уголовного права и криминологии Краснодарского университета МВД России, полковник полиции

Бикмашев Виталий Абдулхаевич
к.ю.н., доцент, доцент кафедры уголовного права и криминологии Краснодарского университета МВД России

«Каждый мошенник расчитывает на плохую память того, кто должен быть обманут»
Ю. Фучик [8]

Аннотация. В статье авторами рассмотрены особенности специального состава мошенничества в сфере компьютерной информации, способы совершения, вопросы квалификации и предупреждения.

Ключевые слова: мошенничество, компьютерная информация, электронные средства платежа, блокирование, модификация, IT-технологии

В современном мире все большее значение приобретает развитие IT-технологий, новые технологии и разработки повсеместно внедряются в различные сферы общества и повышают эффективность их функционирования.

Глобализация информационных технологий, создание общего IT-пространства открыло возможности его использования, как для всего общества в целом, так и для каждого человека.

Массовый переход общества на дистанционное банковское обслуживание создал благоприятную среду для развития мошенничества с использованием IT-технологий с целью лоббирования своих корыстных интересов путем вторжения в сферу безналичных взаиморасчетов.

Незаконное списание электронных средств платежа с цифрового кошелька стало распространенным явлением. Отсутствие практики надежного страхования электронных кошельков клиентов банка и взыскания с виновных лиц

похищенных денег повышает риск стать жертвой мошенников. В настоящее время банки ограничиваются только размещением в сети Интернет превентивных мер, сводящихся к запрету сообщения посторонним лицам кода и номера платежных банковских карт, но как показывает практика, они не совершенны.

Развитие IT-технологий открыло новые возможности для преступников, позволило использовать ранее не изученные методы и средства для осуществления преступной деятельности направленной на завладение электронными денежными средствами граждан, вследствие чего правоохранительные органы сталкиваются со значительными трудностями не только в раскрытии и расследовании преступлений, но и в их квалификации.

Введение в Уголовный кодекс нормы, предусматривающей ответственность за мошенничество в сфере компьютерной информации [3], породило различные подходы ученых в оценке признаков состава данного преступления.

Место расположения рассматриваемого вида мошенничества (159[6] УКРФ) в разделе VIII «Преступления в сфере экономики» УК РФ, определило содержание родового объекта – это общественные отношения по потреблению, перераспределению материальных благ в сфере экономической деятельности, в качестве видового – в сфере собственности, что на наш взгляд не вызывает споров.

Однако, вопрос о непосредственном объекте мошенничества в сфере компьютерной информации является дискуссионным благодаря новой редакции статьи. По мнению одних ученых преступление относится к двуобъектному, поскольку кроме общественных отношений, охраняющих собственность необходимо рассматривать вопрос об уголовно-правовой охране отношений, связанных с областью компьютерной информации. Другие же считают, что в данном составе возник «конфликт интересов» между традиционным понятием объекта, как конкретной формы собственности, так и сферой компьютерной информации. [5]

Третьи остаются на позициях традиционного подхода к определению непосредственного объекта мошенничества и полагают, что указание законодателем на неправомерный доступ и модификацию компьютерной информации не означает его исключительную роль в совершении преступления. Например, по мнению Т.М. Лопатиной при совершении рассматриваемого

вида мошенничества интересы сферы компьютерной информации не нарушаются и образуют отношения, регулируемые факультативным объектом. [7]

Анализ судебной практики и разъяснения Верховного Суда, указывают, что мошенничество в сфере компьютерной информации, совершается именно посредством вмешательства в функционирование средств хранения, обработки и передачи компьютерной информации и как результат нарушается их процесс и создается условие для завладения чужим имуществом. Следовательно, основным объектом будут являться отношения собственности независимо от формы, а дополнительным - отношения, обеспечивающие информационную безопасность.

Не менее дискуссионным является отнесение электронных денежных средства к предмету данного преступления. Согласно статье 128 ГК РФ к объектам гражданских прав относятся: безналичные денежные средства, бездокументарные ценные бумаги и цифровые права, [4], обладающие стоимостным показателем[2].

Согласно позиции Министерства юстиции РФ «криптовалюта может быть рассмотрена как объект гражданских прав в качестве «иного имущества», так как она способна к обособлению и имеет имущественную ценность»[6], однако, российское законодательство рассматривает криптовалюту, как объект инвестирования, но не как средство платежа [1].

Таким образом, можно сделать вывод, что предметом данного преступления являются электронные денежные средства и ценные бумаги.

Мошенничество в сфере компьютерной информации в отличие от традиционного вида мошенничества имеет свои специфические способы, обеспечивающие переход права на чужое имущество либо непосредственное завладение имуществом в виде электронных денежных средств: ввода, удаления, блокирования, модификации компьютерной информации.

Рассмотрим каждый из указанных способов.

Ввод необходимо понимать как введение новой информации посредством использования специальных устройств (клавиатуры, мыши) в базу данных.

Блокирование проявляется в преднамеренном создании ограничений, которые будут препятствовать доступу к информации, находящейся на

компьютере для другого пользователя, при этом информация, несмотря на блокирование, сохраняется.

Под модификацией необходимо понимать любое видоизменение первоначальной информации, как интеллектуальное, так и физическое изменение ее объема с использованием компьютерных технологий.

Законодатель кроме вышеуказанных способов указал «иное вмешательство» в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей [3], однако не раскрыл его содержание. Анализ различных мнений авторов научных статей позволил прийти к выводу, что оно может осуществляться путем любого воздействия с применением различных технологий на проводимые в отношении информации процессы, препятствующие ее нормальному использованию, чаще всего путем ввода, однако могут быть использованы и другие способы [4].

Первый типичный способ совершения преступления заключается в применении злоумышленниками вредоносных программных средств, с помощью которых они взламывают считывающие устройства банкоматов, электронные базы данных. Например, «Осуществил ввод компьютерной информации, а именно привнесение новых последовательных электронных сигналов в систему хранения информации с помощью средств ввода, а именно: клавиатуры и соответствующей программы считывания графической информации» [8].

Второй способ связан с применением продуктов новых технологий. Например, технологическая сим-карта с момента внесения в нее данных абонентского номера, открывает доступ к управлению электронным «Киви» кошельком привязанном к номеру телефона, то есть становится сим-картой «двойником».

Приведем пример из судебной практики: Сидоров А.А. используя технологическую карту, зная, что оригинальная карта заблокирована, отправил команду на сервер ЗАО «Киви банк» о снятии денежных средств с расчетного счета Фомина К.К., информация была автоматически обработана и деньги поступили на лицевой счет сим-карты двойника. Таким образом, по вине Сидорова А.А была произведена модификация компьютерной

информации, при помощи которой он получил доступ к управлению электронным «Киви» кошельком и завладел деньгами Фомина К.К. [11]

Количество пользователей в Интернете повышается, онлайн-пространство начинает осваивать даже самое возрастное поколение.

К распространенному способу можно отнести создание «фишинг сайтов», то есть электронных ресурсов внешне схожих с официальными электронными ресурсами платежных систем и популярных социальных сетей, которые содержат вредоносные программы. Например, «посредством рассылки на используемые номера поступило sms сообщение определенного вида со ссылкой для перехода на сайт «Интернет» - ресурс специального вредоносного сайта.

Рассматриваемый вид мошенничества по отношению к общему составу мошенничества, является специальной нормой и может совершаться без присутствия потерпевшего, однако с помощью принадлежащей ему информации путем воздействия на нее посредством компьютерных технологий. С другой стороны, обман здесь присутствует, однако, воздействию подвергается не потерпевший, а определенная система, выбранная по усмотрению злоумышленника.

По законодательной конструкции рассматриваемый состав относится к материальному, поскольку для привлечения лица к уголовной ответственности важно наступление именно общественно опасных последствий, то есть причинения потерпевшему ущерба.

Оконченным такое преступление считается в тот момент, когда произошло, например, списание денежных средств со счета потерпевшего.

Привлечь к ответственности за совершение мошенничества в сфере компьютерной информации, можно только то лицо, которое уже достигло возраста шестнадцати лет. Как правило, такие лица обладают компьютерной грамотностью или непосредственно имеют доступ к информационным базам о банковских счетах, либо используют общедоступные сведения и методом исследования компьютерной информации удаленно, без непосредственного контакта с владельцами денежных средств, завладевают ими. При этом злоумышленник стремится не только изъять, но и обратить имущество в свою пользу либо передать другим лицам, круг которых не ограничен.

Субъективная сторона характеризуется умышленной формой вины.

Субъективную сторону мошенничества в сфере компьютерной информации образует прямой умысел на завладение чужим имуществом с использованием специфических способов незаконного вторжения в область функционирования компьютерной информации.

Несмотря на длительность существования рассматриваемого вида мошенничества среди норм уголовного законодательства на практике до сих пор допускаются ошибки при квалификации, когда действия виновного квалифицируются по ст. 159⁶ УК РФ и дополнительная квалификация по ст. ст. 272 УК РФ не применяется либо наоборот излишне вменяется. Обращаясь к разграничению ст. 159⁶ и ч. 2 ст. 272 УК РФ, предусматривающей неправомерный доступ к компьютерной информации, совершенный с корыстными целями, можно сказать, что на первый взгляд объективная сторона рассматриваемых составов имеет сходства.

Как показывает анализ судебной практики, мошенничество в сфере компьютерной информации чаще совершается способами (блокирования, модификации, копирования, удаления) с целью непосредственного завладения денежными средствами. Однако, при конструировании законодателем объективной стороны ст. 272 УК РФ эти способы представлены в качестве конечного результата преступной деятельности и лицо только в будущем намеревается получить выгоду от использования такой информации. Стоит отметить, что одним из последствий деяния, предусмотренного ст. 272 УК РФ, выступает именно уничтожение информации, а в диспозиции ст. 159⁶ УК РФ закреплен способ удаления информации. В судебной практике уничтожение и удаление рассматривается, как создание условий, делающих невозможным дальнейшее использование информации. Однако уравнивание удаления и уничтожения информации видится необоснованным, поскольку в некоторых случаях удаленная информации может быть восстановлена. С юридической точки зрения, для одной статьи УК РФ удаление – это способ совершения деяния, а для другой уничтожение – это последствие преступного посягательства.

Таким образом, мошенничество в сфере компьютерной информации, совершенное путем неправомерного доступа к ней или посредством создания, использования и распространения вредоносных компьютерных программ, требует дополнительной квалификации по ст. 272, 273 или 274¹ УК РФ.

Эффективность борьбы с мошенничеством в сфере компьютерной информации, по нашему мнению, обеспечивается в первую очередь не уголовно-правовыми мерами, а профилактикой совершения данного вида преступлений.

В статистическом сборнике «Цифровая экономика 2022», подготовленном Министерством цифрового развития, связи и массовых коммуникаций совместно с Федеральной службой государственной статистики и Национальным исследовательским университетом «Высшая школа экономики» отмечается, что ежедневная аудитория Интернета в России достигла почти 77% взрослого населения и более 80% детей от 3 до 14 лет. По итогам 2021 года было совершено 517 722 таких преступления, а их удельный вес достиг 25,8%, и повысило показатели 2020г. на 1.4 %.[13]

По данным МВД России, в 2022 г. количество преступлений, совершенных с помощью информационных технологий только по итогам шести месяцев 2022 г. составило 249 тыс. [14], несмотря на высокий уровень латентности.

В судебной практике зафиксированы случаи способствования совершению преступления со стороны работников, имеющих доступ к конфиденциальной информации. Например, В., обладая знаниями в сфере информационных технологий, самостоятельно изучил алгоритм необходимых действий, направленных на практически одномоментное копирование сим-карты абонента и блокирования ее оригинала, тем самым получал беспрепятственный доступ к управлению денежными средствами, которые находились на банковских счетах абонентов.

С целью реализации преступной корыстной цели он приобрел клиентскую базу данных, содержащую все сведения об абонентах сотовой связи (номера телефонов, их паспортные данные), и при невыясненных обстоятельствах получил сведения о счетах, привязанных к номерам телефонов. [12]

Учитывая, что преступления в сфере компьютерной информации совершаются как без участия потерпевшего, так и посредством его активных действий, считаем необходимым:

-разработать комплекс технических мер, направленных на повышение уровня защиты информации о денежных средствах граждан и организаций;

-более тщательно проводить отбор специалистов, работающих в кредитно-финансовой сфере, с различными базами клиентов, содержащих их персональные данные, в том числе о финансовом состоянии;

-повысить уровень достаточной правовой грамотности и знаний, среди населения касающихся обеспечения информационной безопасности;

-более активно предупреждать виктимное поведение жертв в сфере компьютерной информации путем информационного обеспечения через средства массовой информации.

Создать систему государственных органов, в правомочия которых будет включена возможность запроса и получения от кредитных организаций информации, которая имеет статус банковской тайны, в определенные сроки и в конкретной форме. Такая разработка позволит сократить проблемы, возникающие в процессе взаимодействия правоохранительных органов и банковских структур.

Необходимо обратить внимание на усовершенствование не только нормативной базы, регламентирующей вопросы мошенничества, ответственности за совершение этих деяний и способов взаимодействия в процессе разбирательств по делу органов государственной власти, но и на обеспечение высокого уровня технического оснащения правоохранительных органов.

Литература:

1. Федеральный закон «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» от 31 июля 2020 г. N 259-ФЗ [Электронный ресурс] Режим доступа: https://www.consultant.ru/(дата обращения 12.05.2023).
2. Федеральный закон от 27 июня 2011 г. N 161-ФЗ (ред. от 22 декабря 2020 г.) «О национальной платежной системе» (с изм. и доп., вступ. в силу с 28.12. 2022) //https://base.garant.ru (дата обращения 15.05.2023)
3. Уголовный кодекс Российской Федерации. Москва: Проспект, 2023. 384с.
4. Гражданский кодекс Российской Федерации (часть первая): федер. закон от 30 нояб. 1994 г. № 51-ФЗ: (ред. от 16 апреля. 2022 г.) // https://base.garant.ru/10164072/ (дата обращения 20.01.2023)
5. Гладких В. И. Компьютерное мошенничество: а были ли основания его криминализации? // Российский следователь. 2014. № 22. С. 25 - 31

6. Егорова М. А., Кожевина О. В. Место криптовалюты в системе объектов гражданских прав // Актуальные проблемы российского права. — 2020. — Т. 15. — № 1. — С. 81—91, с 85.
7. Лопатина Т. М. Проблемы уголовно- правовой защиты сфер компьютерной информации: современный взгляд на мошенничество // Право и безопасность. 2013. №3-4 (45). С.93.
8. Степанова К.В. Мошенничество в сфере компьютерной информации: российский и зарубежный опыт // Актуальные проблемы уголовного права, уголовного процесса и криминалистики. 2019. С. 32-38
9. Юлиус Фучик (1903-1943) - журналист, литературный и театральный критик, публицист [Электронный ресурс] Режим доступа: // https://theocrat.ru
10. Постановление Пленума Верховного Суда РФ от 15.12.2022 N 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей включая сеть «Интернет» [Электронный ресурс] //www.consultant.ru (дата обращения 19.05.2023)
11. Приговор Видновского городского суда Московской области Дело № 1-183/2020 от 28 июля 2020 г. № 1-243/2020 [Электронный ресурс] // ГАС «Правосудие» URL: https://bsr.sudrf.ru/bigs/portal.htm (дата обращения 19.05.2023 г).
12. Приговор № 1-341/2022 от 24 ноября 2022 г. по делу № 1-341/2022 Шатурского городского суда Московской области [Электронный ресурс] Режим доступа: // https://sudact.ru (дата обращения 20.05.2023).
13. Цифровая экономика 2022. Краткий статистический сборник [Электронный ресурс] URL: https://issek.hse.ru/mirror/pubs/share/552091260 (дата обращения: 21.01.2023).
14. Официальный сайт МВД России [Электронный ресурс] // URL: https://мвд.рф (дата обращения: 15.05.2023.)

FRAUD IN THE FIELD OF COMPUTER INFORMATION: CRIMINAL LAW AND CRIMINOLOGICAL ASPECT

Savenko I.A.
Candidate of Law, Associate Professor, Associate Professor of the Department of Criminal Law and Criminology of the Krasnodar University of the Ministry of Internal Affairs of Russia, Police Colonel

Bikmashev V. A.
Candidate of Law, Associate Professor, Associate Professor of the Department of Criminal Law and Criminology of the Krasnodar University of the Ministry of Internal Affairs of Russia

Annotation. In the article, the authors consider the features of the special composition of fraud in the field of computer information, methods of commission, issues of qualification and prevention.

Key words: fraud, computer information, electronic means of payment, blocking, modification, IT technologies

Հոդվածը գրախոսվել է՝ 27. 06.2023թ.:
Ներկայացվել է տպագրության՝ 27.06.2023թ.: