Научная статья
УДК 343.721
DOI 10.33184/vest-law-bsu-2021.12.11

Ситдикова Гузель Зуфаровна
Башкирский государственный университет,
Уфа, Россия, g40773@yandex.ru

К ВОПРОСУ О КВАЛИФИКАЦИИ МОШЕННИЧЕСТВА, СОВЕРШЕННОГО С ИСПОЛЬЗОВАНИЕМ МОБИЛЬНОГО УСТРОЙСТВА

Аннотация. Мошенничества, совершаемые с использованием мобильных устройств, являются наиболее распространенными, о чем свидетельствуют общие статистические показатели преступности. Вместе с тем законодатель не придает самостоятельной общественной опасности деяниям, при свершении которых использованы в качестве предмета преступления мобильные устройства. В данной статье предлагаются результаты исследования отдельных проблем квалификации мошенничества, совершенного с использованием мобильных устройств.

Ключевые слова: мошенничество, мобильное устройство, квалификация преступления, электронные средства платежа, компьютерные преступления

Для цитирования: Ситдикова Г.З. К вопросу о квалификации мошенничества, совершенного с использованием мобильного устройства // Вестник Института права Башкирского государственного университета. 2021. № 4. С. 107–112. DOI 10.33184/vest-law-bsu-2021.12.11.

Original article

Sitdikova Guzel Zufarovna
Bashkir State University,
Ufa, Russia, g40773@yandex.ru

ON THE FRAUD CLASSIFICATION COMMITTED WITH A MOBILE DEVICE

Abstract. Frauds committed with mobile devices are the most common, as evidenced by general crime statistics. At the same time, the legislator does not

impose an independent public danger on acts in which mobile devices are used as the object of a crime. This article presents the results of a study of some problems of fraud classification committed by using mobile devices.

Keywords: fraud, mobile device, qualification of a crime, electronic means of payment, computer crimes

For citation: Sitdikova G.Z. On the Fraud Classification Committed with a Mobile Device. *Vestnik Instituta prava Bashkirskogo gosudarstvennogo universiteta = Bulletin of the Institute of Law of the Bashkir State Uversity,* 2021, no. 4, pp. 107–112. DOI 10.33184/vest-law-bsu-2021.12.11. (In Russian).

Цифровизация общественных отношений способствует активному использованию современных технологий в социально значимых сферах жизни и одновременно вызывает большой интерес у субъектов преступной деятельности как способ совершения общественно опасных деяний.

Последние поколения мобильных устройств предлагают широкий спектр сетевых функций в рамках определенных стандартов, включая регистрацию абонента, передачу информации, шифрование, роуминг и ряд различных услуг, предоставляемых абоненту. Они стали не только средством вербального общения, но и средством управления, офисной работы, финансовых операций, удаленной работы и обучения. Эти обстоятельства являются предпосылкой для использования мобильного устройства в различных общественных отношениях в рамках правового поля, охраняемого законом. В то же время эти же обстоятельства создают предпосылки для совершения противоправных деяний с использованием мобильных устройств. Одно из самых распространенных преступлений сегодня – мобильное мошенничество.

В 2019 г. с платежных карт граждан России мошенническим путем было похищено около 6,5 млрд руб. 69 % трансакций без согласия клиентов были совершены с использованием методов социальной инженерии – в результате побуждения клиента к совершению трансакции или из-за недобросовестных злоупотреблений[1].

Мобильные устройства – телефоны, смартфоны и др., используемые клиентами кредитных организаций для денежных переводов, – стали одним из основных компонентов финансовых трансакций. В то же время уровень латентности преступлений, совершаемых путем мошенничества или злоупотребления доверием с использованием таких устройств, весьма высок.

[1] Банк России. Обзор операций, совершенных без согласия клиентов финансовых организаций за 2019 г. [Электронный ресурс]. URL: https://cbr.ru/Collection/Collection/File/32189/Review_of_transactions_2019.pdf (дата обращения: 06.12.2021).

Мобильные устройства связи, мобильные телефоны, смартфоны являются одним из распространенных способов оплаты через электронные системы. Электронное средство платежа означает средство или метод, который позволяет клиенту банка или другой кредитной организации поручить перечисление денежных средств в рамках применяемых форм безналичных расчетов с использованием информационно-коммуникационных технологий, электронных носителей, в том числе платежных карт, и других технических устройств. При этом ситуации, когда владелец мобильного устройства, который также является абонентом сотовой связи, из-за материальных или иных личных интересов становится участником мошеннической схемы, впоследствии имеют проблемы в квалификации. Они возникают из-за обмана абонента сотовой связи и побуждения его к определенным действиям.

Поиск желающих получить некую выгоду осуществляется с помощью методов социальной инженерии, таких как компьютерная программа Randomizer, которая выбирает случайные числа, составляющие группу чисел номеров телефона для конкретной страны. Социальные сети Instagram, Vk.com, Twitter способствуют поиску, располагая подробной информацией о подписчике, его месте жительства, профессиональной деятельности, близких родственниках. В результате мобильный абонент получает сообщение от известной организации, компании или неизвестного номера с предложением выбрать комбинацию цифр на клавиатуре или голосом подтвердить свое участие в социологическом исследовании, акции, розыгрыше призов, благотворительном марафоне и др. Набранная комбинация цифр или сказанное «Да» в дальнейшем используются для подтверждения операции списания средств с банковского счета абонента.

Такие преступные схемы должны иметь четкие правовые нормы для применения уголовной ответственности. Кроме того, уголовные преступления, предусмотренные ст. 159.3 или ст. 159.6 УК РФ, неоднозначно применимы к рассматриваемым обстоятельствам общественно опасного деяния. К тому же ст. 159.6 УК РФ предусматривает в диспозиции вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей, то есть умышленное воздействие программного или программного и аппаратного обеспечения на серверы, компьютерное оборудование, в том числе портативное – ноутбуки, планшеты, смартфоны, оснащенные соответствующим программным обеспечением, или в информационных и телекоммуникационных сетях. Озвученное добровольное согласие на участие в акции, розыгрыше или набранная комбинация цифр абонентом сотовой связи вызывает спорную квалификацию о постороннем вмешательстве в функционирование средств хранения, обработки или передачи компьютерной информации.

Для общения с потенциальной жертвой «мобильные» мошенники используют: 1) телефонный звонок – позволяет манипулировать человеком во время разговора; 2) SMS-сообщения – это «слепая» рассылка; такие сообщения рассылаются в больших количествах в поиске доверчивого получателя. Основная цель «мобильных» мошенников – заставить жертву добровольно набрать цифры или озвучить подтверждение [1, с. 53].

За последние полгода более 57 % россиян получали звонки от телефонных мошенников, а 19 % – SMS-сообщения. Среди наиболее частых причин для звонков или текстовых сообщений от мошенников предложения банковских услуг (38 %), банковских карт (27 %), кредитов (8 %), предложения о переводе денег (5 %), а также информация о выигрышных призах или акциях на медицинские услуги (по 3 %)[1].

Очевидно, что количество таких преступлений растет, а их латентность позволяет преступникам разрабатывать новые схемы мошенничества и способы совершения деяний, принимать меры по сокрытию их следов. Кроме того, распространенность подобных преступлений свидетельствует о высокой степени уязвимости граждан перед криминальным вмешательством в сфере информационных технологий и мобильных услуг.

Одним из способов контроля за криминальными методами социальной инженерии М.Н. Кузбагаров и Е.В. Кузбагарова предлагают активное внедрение Единой биометрической системы и Единой системы идентификации и аутентификации в банковскую сферу, которые рекомендуется рассматривать как средство обеспечения безопасности банковских операций с использованием сети Интернет, созданных на основе современных инженерных, технических и программных разработок [2, с. 210].

В настоящее время наиболее распространенными в криминальной среде схемами телефонного мошенничества являются: 1) побуждение открыть ссылку с последующим разъяснением причин; 2) ошибочный перевод средств; 3) ложный выигрыш в лотерею; 4) сообщение о перечислении родственнику или другу; 5) сообщение о блокировке банковской карты, за которым следует инструкция по набору определенных цифр; 6) запрос конкретной суммы на счете продавца перед продажей товара на сайтах объявлений и др. Это позволяет сделать вывод о том, что нынешняя ситуация с распространенностью мошенничества с использованием мобильных устройств оп-

[1] Аналитический обзор. Всероссийский центр изучения общественного мнения (ВЦИОМ): телефонное мошенничество: масштабы и потери [Электронный ресурс]. URL: https://wciom.ru/analytical-reviews/analiticheskii-obzor/telefonnoe-moshennichestvo-masshtaby-i-poteri (дата обращения: 06.12.2021).

равдывает необходимость придания таким преступлениям самостоятельной формы в уголовном законе.

В связи со сказанным предлагаем дополнить ч. 1 ст. 159.6 пунктом 1.1. в следующей редакции: «Мошенничество, совершенное с использованием мобильных устройств, – хищение чужого имущества или приобретение права на чужое имущество, совершенное путем обмана или введения в заблуждение абонента сотовой связи, если эти действия повлекли передачу на принимающее мобильное устройство ложных данных с использованием метода цифровой обработки сигнала и модуляции либо иное вмешательство в функционирование мобильного устройства». При этом санкции новой нормы должны предусматривать увеличение размера наказания в связи с высокой социальной опасностью преступления, его распространенностью, развитием и доступностью рынка мобильных устройств, использованием виновными лицами правовой и технической уязвимости абонентов.

Аналогичный способ расширения содержания правовой нормы с классификацией на пункты 1.1 законодатель применяет в других статьях УК РФ, например, в ст. 205.1 УК РФ. Мы считаем, что достаточно дополнить ст. 159.6 УК РФ квалифицирующим признаком в п. 1.1, нежели впоследствии разграничивать ст. 159.3 и 159.6 УК РФ. При этом вменение преступнику рассматриваемого квалифицирующего признака будет иметь место только тогда, когда действия мошенника, использовавшего мобильное устройство, выступают в качестве главного фактора, причиняющего имущественный ущерб [3, с. 77].

Введение указанного квалифицирующего признака будет отражать не только увеличение степени общественной опасности такого рода мошенничества, но и избавит правоприменителя от необходимости отграничивать в анализируемых обстоятельствах от иных видов мошенничества признаки состава преступления – мошенничество, совершенное с использованием мобильных устройств.

Дифференциация способов совершения преступлений с использованием возможностей мобильных устройств, различных гаджетов позволит своевременно обнаруживать и пресекать такие общественно опасные действия и избавляться от побочного криминального воздействия на общество в его активном использовании современных технологий.

Список источников

1. Лабутин А.А. «Мобильные» мошенничества: основные способы совершения // Вестник Казанск. юрид. ин-та МВД России. 2021. Т. 12, № 3 (45). С. 50–55.

2. Кузбагаров М.Н., Кузбагарова Е.В. Единая биометрическая система и единая система идентификации и аутентификации как инструменты обеспечения безопасности банковских операций с использованием сети интернет: правовые и организационные вопросы // Правовое государство: теория и практика. 2020. Т. 16, № 4-2. С. 199–212.

3. Осокин Р.Б. Уголовно-правовая характеристика способов совершения мошенничества : дис. ... канд. юрид. наук. М., 2003. 187 с.

References

1. Labutin A.A. «Mobile» Fraud: the Main Ways of Committing. *Vestnik Kazanskogo yuridicheskogo instituta MVD Rossii = Bulletin of the Kazan Law Institute of MIA Russia,* 2021, vol. 12, no. 3 (45), pp. 50–55. (In Russian).

2. Kuzbagarov M.N., Kuzbagarova E.V. The Unified Biometric System and Unified System of Identification and Authentication as Tools to Ensure the Security of Banking Operations Using the Internet: Legal and Organizational Issues. *Pravovoe gosudarstvo: teoriya i praktika = The Rule-of-Law State: Theory and Practice,* 2020. vol. 16, no. 4-2, pp. 199–212. (In Russian).

3. Osokin R.B. *Ugolovno-pravovaya harakteristika sposobov sovershеniya moshennichestva. Kand. Diss.* [Criminal Law Characteristics of the Ways of Committing Fraud. Cand. Diss.]. Moscow, 2003. 187 p.

Информация об авторе

Ситдикова Гузель Зуфаровна *– кандидат юридических наук, доцент, доцент кафедры уголовного права и процесса Института права Башкирского государственного университета*

Information about the Author

Sitdikova Guzel Zufarovna *– Candidate of Sciences (Law), Associate Professor, Assistant Professor of the Chair of Criminal Law and Procedure, Institute of Law, Bashkir State University*

Статья поступила в редакцию 09.12.2021; одобрена после рецензирования 16.12.2021; принята к публикации 17.12.2021.
The article was submitted 09.12.2021; approved after reviewing 16.12.2021; accepted for publication 17.12.2021.