ВОПРОСЫ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПЛЕНИЯМ, СОВЕРШАЕМЫМ С ИСПОЛЬЗОВАНИЕМ ЭЛЕКТРОННЫХ СРЕДСТВ ПЛАТЕЖА

ISSUES OF COUNTERACTING CRIMES COMMITTED USING ELECTRONIC MEANS OF PAYMENT

УДК 34

Гаджиев Гаджи Русланович, магистрант, Санкт-Петербургский государственный экономический университет, РФ, г. Санкт-Петербург

Тюнин Владимир Ильич, доктор юридических наук, профессор кафедры уголовного права и уголовного процесса, Санкт-Петербургский государственный университет, РФ, г. Санкт-Петербург

Gadzhiev Gadzhi Ruslanovich, Master's student, Saint Petersburg State University of Economics, RF, St. Petersburg, gadzhi.gadzhiev.99@mail.ru

Tyunin Vladimir Ilyich, Doctor of Law, Professor of the Department of Criminal Law and Criminal Procedure,Saint Petersburg State University, RF, St. Petersburg

Аннотация

В статье рассматриваются некоторые проблемы противодействия преступлениям, связанным с оборотом электронных средств платежа, поднимается вопрос о необходимости более тщательного исследования криминологической характеристики преступлений, связанных с оборотом электронных средств платежа, анализируется международный опыт и вопросы взаимодействия между государствами в борьбе с преступлениями в сфере экономики с применением электронных технологий.

Annotation

The article examines some of the problems of combating crimes related to the circulation of electronic means of payment, raises the question of the need for a more thorough study of the criminological characteristics of crimes related to the circulation of electronic means of payment, analyzes the international experience and issues of interaction between states in the fight against crimes in the economic sphere using electronic technologies.

Ключевые слова: платеж, оборот, электронные средства платежа, киберпреступность, противодействие преступности

Keywords: payment, turnover, electronic means of payment, cybercrime, crime prevention

В современном мире процессы электронизации идут полным ходом. Активно развиваются компьютерные системы, делопроизводство и коммуникации переходят в электронную среду, развивается электронный оборот товаров, многие услуги переходят в режим on-line. Большое развитие системы электронного оборота получили в результате массового перехода людей на удаленную систему работы из-за пандемии Covid-19. Меры безопасности, принимаемые для предотвращения распространения заболевания, включали в себя и рекомендации по минимизации оборота наличных денег, повсеместно люди старались оплачивать покупки, проезд в транспорте и прочие услуги с помощью электронных средств платежа: платежных карт, электронных переводов, платежных поручений.

Происходящие в мире изменения неизбежно затрагивают не только сферу урегулированных законом отношений, но и мир криминала, который приспосабливается к изменениям в обществе гораздо быстрее, чем реагирует законодатель. Так было и в период появления первых платежных систем, когда мошенники развернули свою деятельность за счет низкой грамотности населения о методах работы с банкоматами и платежными картами, так

происходит и сегодня, когда меры противодействия новым видам преступности оказываются запоздалыми.

Предотвратить подобные ситуации помогают криминологические исследования и прогнозы развития преступности, которые проводятся по отдельным видам преступлений. Вместе с тем, и это не всегда бывает своевременным, что явно демонстрирует ситуация, сложившаяся с нормой о противодействии неправомерному обороту средств платежей, закрепленной ст. 187 УК РФ. Проведенный нами анализ научной литературы показывает, что полноценных криминологических исследований по данному составу преступления после внесения в него изменений в 2015 году не проводилось.

В научной литературе много внимания уделяется экономической преступности в целом, однако нет конкретизации на отдельных составах экономических преступлений, таких исследований либо нет вовсе, либо их крайне мало. Это негативно сказывается на вопросах противодействия преступлениям, связанным с неправомерным оборотом средств платежа.

Необходимость установления нормы об охране таких отношений вызвана изменениями, которые происходили в сфере экономической деятельности и распространением электронных платежных систем, появлением новых финансовых институтов и развитию государственной политики в данной отрасли.

Важным шагом к появлению нормы об уголовной ответственности за неправомерный оборот средств платежей стала Стратегия национальной безопасности, в которой важное место заняли положения об увеличении преступных проявлений в экономической сфере, которые связаны с использованием при совершении преступлений достижений компьютерных технологий и телекоммуникационных средств [1].

Одним из приоритетных направлений деятельности государства в сфере обеспечения экономической безопасности названы укрепление финансовой системы и обеспечение ее независимости и целостности, развитие и сохранение защищенности всех ее институтов.

Следующим важным основанием для появления такого объекта, как защита платежных операций, стало принятие Доктрины информационной безопасности, в которой, помимо прочего, отмечалось, что масштабы компьютерной преступности увеличиваются ежегодно, и в первую очередь такие преступления направлены именно на кредитно-финансовую отрасль экономики [2].

Таким образом, уголовно-правовая охрана и защита интересов в сфере осуществления платежей и оборота платежных средств стала важным шагом в развитии государственной политики в области обеспечения экономической безопасности.

В мировой практике, которая имеет более давнюю историю оборота платежных карт, выделяют несколько способов подделки карт: частичная и полная [2]. Для частичной характерно изменение лишь некоторых признаков карты, в то время как полная подделка заключается в воссоздании карты со всеми характерными признаками. Примечательно, что полная подделка может быть осуществлена на высоком уровне только при содействии со стороны работников банков, которые имеют доступ к особым технологиям производства и могут помочь изготовить карту таким образом, что ее будет невозможно отличить от оригинала. По мнению исследователей, в России такой способ подделки пока не получил широкого распространения, однако анализ мирового опыта противодействия экономической преступности в сфере оборота средств платежей позволяет сделать вывод о том, что появление таких поддельных карт в нашей стране – вопрос времени [2].

Из этого напрашивается необходимость более полноценного сотрудничества с международным сообществом по вопросам противодействия преступлениям, связанным с оборотом электронных средств платежей вообще и в сфере преступлений, совершаемых с применением компьютерных технологий – в частности.

Основой международного сотрудничества по борьбе с преступлениями в сфере высоких технологий являются международные нормативные акты, принятые большинством западных стран[9].

Наиболее значимым является Конвенция Совета Европы о киберпреступности, которая регулирует все основные вопросы противодействия киберпреступлениям, а также определяет их разновидности. В настоящее время сторонами Конвенции являются 56 государств, и этот список постоянно расширяется, поскольку во всем мире государства осознают необходимость консолидации мер по борьбе с преступлениями в компьютерных сетях [8, С. 168-179].

Проблема международного сотрудничества по противодействию компьютерных преступлений, связана с тем, что уровень развития технологий позволяет совершать эти деяния, находясь в любой точке мира, обходя границы государств. Киберпреступления являются преступлениями транснационального характера, что говорит о необходимости консолидации действий правоохранительных органов разных государств в борьбе с этими явлениями. Нормы международных правовых актов носят рекомендательный характер, позволяя государствам принимать решения об ответственности за компьютерные хищения на уровне национального законодательства.

Проблемными вопросами остаются порядок межведомственного взаимодействия между структурами правоохранительных органов и учреждениями, которые связаны с работой компьютерных систем, в первую очередь – это банки, операторы сотовой связи, организации электронных платежных систем [5, С. 182-187]. Отсутствие четкой процедуры их взаимодействия при расследовании рассматриваемого нами вида преступлений осложняет работу, в том числе и на межгосударственном уровне.

Работа по совершенствованию мер по противодействию преступлениям в сфере оборота электронных средств платежа носит как международный, так и национальный характер.

Наиболее яркими примерами активного подхода к решению проблем преступлений, связанных с компьютерной информацией, являются меры, принимаемые в Великобритании и США.

Так, в Великобритании с 2001 году в штатах полиции предусмотрен специальный отдел, который специализируется на расследовании и противодействии преступлениям в сфере высоких технологий. В штат этого подразделения входят следователи, специалисты по компьютерным системам, судебно-медицинские эксперты. В 2016 году это подразделение выделилось в самостоятельную службу – Национальный центр компьютерный преступлений, который обеспечивает безопасность онлайн деятельности на территории Великобритании, а также оказывает консультативную помощь гражданам по вопросам безопасности в сети Интернет и защите от мошеннических действий в сфере компьютерных технологий [6].

В США действует национальный центр защиты компьютерной инфраструктуры, который занимается защитой от кибератак, расследованием мошеннических действий в сети Интернет и прочих компьютерных преступлений. При этом Министерством обороны США создана специальная база, которая позволяет сотрудникам правоохранительных органов взаимодействовать между собой по вопросам расследования и предупреждения преступлений в сфере оборота электронных платежей, координировать деятельность по расследованию таких уголовных дел, направлять и получать запросы о взаимной помощи [7].

В рамках соглашений в соответствии с Конвенцией по борьбе с киберпреступностью США оказывают помощь государствам-членам соглашения по борьбе с экономическими преступлениями, совершаемыми с использованием электронных платежей. Кроме того, в рамках стран Большой семерки создан неформальный канал сбора и обмена сведениями о таких преступлениях, который помогает координировать работу по противодействию этим преступлениям [7].

Несмотря на активное развитие международных систем взаимодействия между правоохранительными органами государств, серьезным препятствием при расследовании мошенничества в сети Интернет и в сфере компьютерной информации остается то, что профессиональные мошенники используют иностранные ресурсы для расположения своих серверов. Последующее создание сайтов на этих серверах с целью совершения преступлений затрудняет проведение следственных действий, особенно, если у данного государства и Российской Федерации отсутствуют соглашения о сотрудничестве.

Опрос практических сотрудников по данному вопросу подтверждает этот вывод. Так, среди работников правоохранительных органов существует мнение, что трансграничный характер преступности усложняет расследование подобных преступлений. Выражается это в том, что адресат денежных транзакций может не находиться под контролем национального финансового регулятора (Центрального Банка), а, значит, невозможность его установления или, в лучшем случае, большая потеря времени при взаимодействии с правоохранительными органами других стран.

Все этого говорит о необходимости дальнейшего тщательного изучения вопросов, связанных с уголовной ответственностью за неправомерный оборот средств платежей. От того, насколько полно и всесторонне проводится исследовательская работа во многом зависят скорость и качество законодательной реакции на происходящие процессы.

Литература

1. "О Стратегии национальной безопасности Российской Федерации": Указ Президента РФ от 31.12.2015 N 683 // СЗ РФ. 2016. № 1 (ч. II). Ст. 212.
2. "Об утверждении Доктрины информационной безопасности Российской Федерации": Указ Президента РФ от 05.12.2016 N 646 // СЗ РФ. 2016. № 50. Ст. 7074.
3. Веснина С.Н., Неустроева А.В. Пластиковые карты как предмет преступного посягательства неправомерного оборота средств платежей //

Вестник Саратовской государственной юридической академии. – 2016. – № 6 (29). – С. 214-219.

4. Гущин Д.Н. К вопросу о необходимости развития системы научно-методического обеспечения расследования преступлений в сфере неправомерного оборота средств платежей // Юристъ-Правоведъ. – 2019. – № 2 (89). – С. 153-157.
5. Камко А.С. Проблемы и перспективы системы противодействия мошенничеству с использованием телекоммуникационного и компьютерного оборудования // Власть и управление на Востоке России. 2017. №4 (81). С. 182-187.
6. Официальный сайт The National Cyber Security Centre [Электронный ресурс]. Режим доступа: https://www.ncsc.gov.uk/ (дата обращения: 19.04.2020).
7. Хатауэй М. Киберготовность США: краткая информация. Опубликовано Потомакским институтом политических исследований [Электронный ресурс]. Режим доступа: https://analytica.digital.report/wp-content/uploads/2017/05/CRI-USA-RU.pdf (дата обращения: 19.04.2020).
8. Чернякова А.В. Международный и зарубежный опыт уголовно-правового противодействия хищениям, совершаемым с использованием компьютерной информации // Юридическая наука и правоохранительная практика. 2018. №4 (46). С. 168-179.
9. Конвенция Совета Европы о киберпреступности, принятая 23 ноября 2001 года; Дополнительный Протокол к Конвенции о преступлениях в сфере компьютерной информации относительно введения уголовной ответственности за правонарушения, связанные с проявлением расизма и ксенофобии, совершенные посредством компьютерных систем ETS N 189 (Страсбург, 28 января 2003 г.); Рамочное решение по борьбе с мошенничеством и подделкой безналичных платежных средств; Соглашение о сотрудничестве государств – участников СНГ в борьбе с преступлениями в сфере компьютерной информации, принятое 1 июня 2001

года в Минске; Соглашение Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности; Конвенция о кибербезопасности и защите персональных данных; типовой закон Лиги арабских государств о борьбе с преступлениями в сфере информационных систем (2004 год); типовые тексты законов Международного союза электросвязи (МСЭ), Карибского сообщества (КАРИКОМ), Карибского союза электросвязи (КСЭ) по киберпреступности, электронной торговле и электронным доказательствам, и другие

Literature

1. "On the National Security Strategy of the Russian Federation": Decree of the President of the Russian Federation of December 31, 2015 N 683 // SZ RF. 2016. No. 1 (part II). Art. 212.
2. "On the approval of the Doctrine of information security of the Russian Federation": Decree of the President of the Russian Federation of 05.12.2016 N 646 // SZ RF. 2016. No. 50. Art. 7074.
3. Vesnina S.N., Neustroeva A.V. Plastic cards as a subject of criminal encroachment of illegal circulation of means of payment // Bulletin of the Saratov State Law Academy. - 2016. - No. 6 (29). - S. 214-219.
4. Gushchin D.N. On the issue of the need to develop a system of scientific and methodological support for the investigation of crimes in the field of illegal circulation of means of payment // Yurist-Pravoved. - 2019. - No. 2 (89). - S. 153-157.
5. Kamko A.S. Problems and Prospects of Fraud Counteraction System Using Telecommunication and Computer Equipment // Power and Management in the East of Russia. 2017. No. 4 (81). S. 182-187.
6. Official site of The National Cyber Security Center [Electronic resource]. Access mode: https://www.ncsc.gov.uk/ (date of access: 19.04.2020).
7. Hathaway M. US Cyber Readiness: A Brief Information. Published by the Potomac Institute for Policy Studies [Electronic resource]. Access mode:

https://analytica.digital.report/wp-content/uploads/2017/05/CRI-USA-RU.pdf (date of access: 19.04.2020).

8. Chernyakova A.V. International and foreign experience of criminal-legal counteraction to thefts committed with the use of computer information // Legal Science and Law Enforcement Practice. 2018. No. 4 (46). S. 168-179.
9. Council of Europe Convention on Cybercrime, adopted on 23 November 2001; Additional Protocol to the Convention on Cybercrime, concerning the criminalization of offenses of racism and xenophobia committed through computer systems ETS N 189 (Strasbourg, 28 January 2003); Framework solution to combat fraud and counterfeiting of non-cash means of payment; The Agreement on Cooperation of the CIS Member States in Combating Crimes in the Sphere of Computer Information, adopted on June 1, 2001 in Minsk; The Shanghai Cooperation Organization Agreement on Cooperation in the Field of International Information Security; The Convention on Cybersecurity and Personal Data Protection; the League of Arab States Model Law on Combating Crimes in Information Systems (2004); model texts of laws of the International Telecommunication Union (ITU), the Caribbean Community (CARICOM), the Caribbean Telecommunication Union (CCU) on cybercrime, electronic commerce and electronic evidence, and others