УДК 343.72

Электронные денежные средства как предмет имущественных преступлений

Сметанин Христофор Христофорович, магистрант, Северо-Восточный Федеральный университет имени М. К. Аммосова, gulayika@mail.ru

В современном мире стремительного развития технологий важно соблюдать законодательные нормы как при их внедрении, так и при использовании гражданами, а также своевременно совершенствовать законодательство для защиты конституционных прав. Эти вопросы широко обсуждаются в научных трудах юристов, экономистов и социологов. Цель исследования — рассмотреть электронные денежные средства как предмет имущественных преступлений. По результатам исследования предложены рекомендации по совершенствованию правового регулирования электронных денежных средств.

Ключевые слова: имущественные отношения, имущественные преступления, финансовая документация, хищение, электронные денежные средства.

На законодательном уровне регламентировано рассмотрение электронных денежных средств (ЭДС) как предмета таких имущественных преступлений, как хищение (ст. 158 Уголовного кодекса Российской Федерации). Исходя из данного регламента, допускается рассмотрение электронных денежных средств в качестве предмета таких правонарушений, как кража (ст. 158), мелкое хищение (ст. 158.1), мошенничество (ст. 159, 159.1, 159.2, 159.3, 159.5, 159.6), присвоение или растрата (ст. 160), грабеж (ст. 161), разбой (ст. 162), вымогательство (ст. 163), причинение имущественного ущерба путем обмана или злоупотребления доверием (ст. 165). Это отнесение обусловлено приравниванием кражи средств с банковского счета к совершению преступления в отношении электронных денежных средств, о чем прямо говорится в законе (подп. «г» п. 3 ст. 158 Уголовного кодекса Российской Федерации).

Однако законодатель также устанавливает исключение для приравнивания вышеуказанных преступлений, определяя в действиях подозреваемого состав преступления, предусмотренного ст. 159.3 Уголовного кодекса Российской Федерации.

Следовательно, при определении субъекта правонарушения необходимо учитывать способ и средства совершения преступления, поскольку от этих факторов зависит квалификация противоправного деяния.

Оборот электронных денежных средств, как и любая иная сфера жизнедеятельности граждан, подвержен определенным рискам. В отношении данных средств риски можно условно разделить на внешние и внутренние. К внешним рискам можно отнести экономическую и политическую обстановку в стране, а также юридическую природу ЭДС и ряд социальных факторов. К числу внутренних рисков следует отнести восприятие лицом информации о способах осуществления оборота электронных денежных средств, а также связанные с информацией о наличии ЭДС у граждан риски, обусловленные третьими лицами.

Эти риски определяют возможность использования электронных денежных средств в качестве предмета противоправного деяния. Поскольку внешние риски и угрозы в процессе оборота электронных денежных средств не предполагают такой возможности, проанализируем категорию внутренних угроз и определим социально-правовую обоснованность уголовно-правовой охраны общественных отношений по обороту ЭДС.

К основным внутренним угрозам оборота ЭДС, согласно исследованиям экономистов-теоретиков и юристов-практиков, относится восприятие лицом информации о способах обращения ЭДС. Это определение подразумевает уровень грамотности населения в отношении осуществления операций с этим видом денежных средств. Современные молодые люди достаточно легко осознают способы осуществления оборота ЭДС, а также понимают основные принципы работы операторов электронных платежей, выполняя такие операции достаточно часто. Лица более старшего возраста часто избегают использования незнакомых средств платежа, однако при желании могут освоить навыки обращения с ЭДС.

Более пожилые лица не осуществляют таких операций и не стремятся к их освоению, считая эту систему сложной и небезопасной [1]. Эти данные содержатся в опросах граждан, проведенных одной из крупнейших финансовых организаций России. Результаты исследования подтверждают необходимость закрепления в образовательных программах обучения финансовой грамотности, расширив ее основными аспектами оборота ЭДС. Также необходимо законодательное закрепление норм по защите ЭДС.

Экономисты выделяют целый ряд рисков и угроз, которые обусловлены наличием сведений у третьих лиц об объемах ЭДС у граждан. Среди этих рисков и угроз выделяются следующие: фишинг, скимминг, генераторы, компьютерный шантаж и доступ сотрудников финансовых организаций к данным клиентов во время обработки информации внутри организации или оператора ЭДС [2].

Эти термины не представлены в законодательных и нормативно-правовых актах, поскольку принадлежат экономической терминологии. Однако при рассмотрении их сущности можно установить эквиваленты этим действиям в рамках уголовного законодательства Российской Федерации.

Определение фишинга в современных словарях или нормах не указано, что обуславливает необходимость дополнительного анализа теоретических сведений в отрасли экономики. Результаты анализа показали, что происхождение данного слова происходит от английского языка и в дословном переводе трактуется как «рыбалка». Это определение характеризует схему осуществления фишинга: злоумышленники, аналогично процессу рыбной ловли, «закидывают» ложную информацию с просьбой в адрес физического лица, замаскировав себя под авторитетную финансовую организацию, что вызывает ассоциации с маскировкой крючка на рыболовной удочке. Под данным термином принято понимать отправку (рассылку) информационных писем гражданам через Интернет и адреса электронной почты, в содержании которых приводится просьба об обновлении финансовой информации с целью ее актуализации и дальнейшей передачи третьим лицам [4].

Данное деяние содержит признаки мошенничества, предусмотренные статьей 159 УК РФ. В данном случае, с криминалистической точки зрения, электронные денежные средства будут рас-

сматриваться как материальная ценность. Однако отсутствие закрепления за конкретным физическим лицом ЭДС на счете в финансовой организации допускает признание потерпевшей стороной именно финансовую организацию, а не гражданина.

Мошенничество с использованием ЭДС обладает высокой латентностью и крайне низкой раскрываемостью, поскольку этот вид преступления осуществляется с применением дистанционных технологий.

Не менее опасный вид угрозы — скимминг. Это вид мошенничества, сущностью которого является использование специальных устройств для завладения информацией о данных физического лица, например, реквизитами электронных кошельков и данными платежных карт. В России скимминг достиг своего пика в первом десятилетии XXI в., когда степень защиты банкоматов была недостаточной, а доступ к программному обеспечению и считывающим устройствам для злоумышленников был почти свободным.

Хищение средств чаще всего происходило с использованием банкоматов, однако в современных системах банковского обслуживания терминалы обладают высокой степенью защиты. Снижение числа граждан, снимающих наличные в банкоматах, уменьшило актуальность этого вида мошенничества. Мошенники все еще используют скимминг для хищения средств с электронных кошельков граждан [6].

Перечисленные факторы обуславливают рассмотрение ЭДС в качестве предмета преступлений, предусмотренных п. 4 ст. 272 УК РФ «Неправомерный доступ к компьютерной информации», ст. 187 УК РФ «Неправомерный оборот средств платежей», ст. 159.3 УК РФ «Мошенничество с использованием электронных средств платежа». Содержание данных составов преступлений также допускает отнесение ЭДС к предметам преступлений.

Пункт «г» ч. 3 ст. 158 УК РФ предусматривает ответственность за кражу, совершенную с банковского счета, а также в отношении электронных денежных средств, что позволяет отнести ЭДС к предмету этого состава преступления. Хищение ЭДС осуществляется посредством тайного завладения информацией об электронных кошельках и прочими данными, с использованием которых в дальнейшем будет осуществлено хищение ЭДС.

На смену скиммингу в России пришли и продолжают развиваться генераторы — программное обеспечение, предназначенное для увеличения денежных средств на счетах электронных кошельков, а также для «защиты» электронных денежных средств пользователей. Состав данных правонарушений можно квалифицировать как изготовление, использование или сбыт поддельных платежных карт, электронных средств, электронных носителей информации, технических устройств, компьютерных программ, предназначенных для неправомерного осуществления приема, выдачи или перевода денежных средств, что эквивалентно содержанию ст. 187 УК РФ «Неправомерный оборот средств платежей». Это объясняется тем, что именно ЭДС являются предметом преступного посягательства.

Также экономистами определена такая угроза, как компьютерный шантаж. Этот вид корыстно-насильственного воздействия на личность заключается в удаленном внедрении вредоносного вируса, который блокирует интернет-браузер или всю операционную систему устройства. После блокировки пользователь видит на экране просьбу о перечислении денежных средств или о переходе по указанной ссылке для снятия блокировки. Доказать совершение такого преступления практически невозможно, однако при обращении в правоохранительные органы возбуждается уголовное дело по ст. 159.6 УК РФ «Мошенничество в сфере компьютерной информации». Предметом данного преступления могут быть ЭДС, если пользователь перешел по указанной ссылке, предоставив тем самым злоумышленникам доступ к сведениям о своих лицевых счетах и другим данным.

Кроме вышеперечисленных видов противоправных деяний, большое распространение получили риски, связанные с мошенничеством, в случае наличия у сотрудников финансовых организаций доступа к данным клиентов в момент обработки информации внутри организации или у оператора ЭДС. В данном случае могут быть различные виды преступлений. Во-первых, это передача (сбыт) такой информации третьим лицам сотрудниками финансовой организации, что может привести к хищению ЭДС пользователей. Это правонарушение будет квалифицироваться в зависимости от способа воздействия на сотрудника финансовой организации, числа задействованных лиц, средств совершения преступления и объемов причиненного ущерба.

Во-вторых, самостоятельное использование сотрудником (сотрудниками) финансовой организации информации в корыстных целях будет квалифицироваться по ст. 286 УК РФ «Превышение должностных полномочий» [5].

В соответствии с классификацией правонарушений по степени их тяжести, а именно по тяжести последствий их совершения, тайное хищение денежных средств с банковского счета гражданина или в отношении ЭДС является тяжким правонарушением, в то время как мошенничество, совершенное в отношении ЭДС, признается преступлением небольшой тяжести. Этот факт обусловлен не только последствиями, наступившими для потерпевшего по окончании противоправного деяния, но и способом его совершения: тайное хищение не влечет за собой обмана как такового, в отличие от мошенничества, при совершении которого потерпевшего намеренно вводят в заблуждение, вынуждая его собственноручно осуществить перевод денежных средств мошенникам.

Кроме того, размер ущерба в этом вопросе является ключевым. Редакция нормы от 12 июня 2024 г. в статьях закрепляет размер ущерба, причиненного собственнику имущества. Так, в соответствии с редакцией, значимость ущерба определяется, исходя из материальной обеспеченности потерпевшего, но в любом случае не может быть менее 5 тыс. руб.

Размер крупного ущерба (от 250 тыс. руб. до 1 млн руб.) и значительный ущерб (от 5 до 250 тыс. руб.) также прописаны. Данные правонарушения предусматривают ответственность за преступления небольшой тяжести. Здесь необходимо отметить, что данное решение не является справедливым, поскольку при низком уровне материальной обеспеченности гражданина (например, жилье по социальному найму, отсутствие работы или наличие инвалидности) сумма в размере 240 тыс. руб. будет являться крайне значительной. На законодательном уровне рассматривается как преступление небольшой степени тяжести.

Согласно разъяснениям, содержащимся в Постановлении Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. N 48 «О судебной практике по делам о мошенничестве, присвоении и растрате», если хищение имущества осуществлено с использованием поддельной или чужой кредитной, расчетной или иной платежной карты, а также путем предоставления уполномоченному сотруднику кредитной, торговой или иной организации заведомо ложной информации о принадлежности данной карты, такие действия подлежат квалификации как мошенничество.

В случаях, когда лицо похитило безналичные денежные средства, воспользовавшись конфиденциальной информацией держателя платежной карты, переданной злоумышленнику самим держателем карты под воздействием обмана или злоупотребления доверием, действия виновного квалифицируются как кража.

В данном случае, опираясь на ст. 128 Гражданского кодекса Российской Федерации, ЭДС будет относиться к категории иного имущества, поскольку не проявляется в виде наличных денежных средств или другого материального блага, а также выступает средством платежа, но не находится на персональном банковском счете гражданина.

Таким образом, в данном случае объектом противоправного деяния также будут выступать ЭДС, которые могут быть признаны имуществом (собственностью) гражданина. Процедура признания ЭДС собственностью гражданина включает предоставление в суде подтверждения пройденной идентификации личности при оформлении кабинета пользователя ЭДС. Электронные денежные средства выступают предметом имущественных преступлений, ответственность за которые предусмотрена уголовным законодательством страны. Объектом имущественных преступлений в данном случае будут являться отношения, возникшие между владельцем электронных денежных средств и их оператором, а предметом — непосредственно сами электронные денежные средства.

Примечания

1. Исследование Т-Кассы: россияне оплачивают 22 % покупок с помощью отечественных платежных сервисов, заменивших зарубежные аналоги. URL: https://www.tbank.ru (дата обращения: 02.01.2025).
2. Регулирование эмиссии и обращения электронных денег: виды и современные модели. URL: http://bmpravo.ru (дата обращения: 26.10.2024).
3. Пономаренко Е. В. Риски систем электронных денег // Финансы и кредит. 2007. N 43. С. 39–42.
4. Силаева В. Л. «Коммерциализация Интернета // Социологические исследования. 2012. N 10. С. 111–121.
5. Электронные деньги. URL: http://internetidengi.blogspot.ru (дата обращения: 25.10.2024).
6. Электронные деньги. URL: http://moneynews.ru (дата обращения: 26.10.2024).
7. Электронные платежные системы в России. URL: www.tadviser.ru (дата обращения: 24.10.2024).

English version

Electronic monetary funds as an object of property crimes

Smetanin Khristofor Khristoforovich, master’s student, M. K. Ammosov North-Eastern Federal University

In today’s rapidly evolving technological world, it is crucial to comply with legal norms both during their implementation and in their use by citizens, as well as to timely improve legislation to protect constitutional rights. These issues are widely discussed in the academic works of legal scholars, economists, and sociologists. This study aims to examine electronic monetary funds as an object of property crimes. Based on the research findings, recommendations are proposed for improving the legal regulation of electronic monetary funds.

Keywords: property relations, property crimes, financial documentation, theft, electronic monetary funds.