Керимов Шаиг Нусратович
магистрант
ФГБОУ ВО «Ярославский государственный
университет им. П.Г. Демидова»
г. Ярославль, Ярославская область

КРИПТОВАЛЮТА – ОБЪЕКТ УГОЛОВНО-ПРАВОВОЙ ОХРАНЫ

Аннотация*: в статье кратко освещаются этапы легализации цифровых финансовых активов в Российской Федерации. Исследуется вопрос возможности отнесения криптовалюты к объектам уголовно-правовой охраны. Детально раскрывается способ хищения криптовалюты.*

Ключевые слова*: цифровые финансовые активы, криптовалюта, объект уголовного права, фишинг.*

Сегодня цифровые технологии представляют собой неотъемлемую часть жизнедеятельности современного человека. С учетом настолько стремительного развития технологий, право на успевает оперативно реагировать на появление новых инструментов и технологических решений.

Такая ситуация сложилась с криптовалютой, которая объективно существует уже не один год, однако вопросы её правового регулирования оставляют желать лучшего.

Ошибочно отрицать факт того, что криптовалюта имеет огромный потенциал для получения реальной выгоды. Адепты криптовалют в Российской Федерации утверждают, что операции в криптовалюте будут осуществляться быстрее, удобнее и безопаснее. Центробанк, напротив, считает, что подобные платежи поспособствуют увеличению числа факторов, способствующих легализации (отмыванию) доходов, полученных преступным путем.

С 2014 года Центральным банком РФ и Министерством финансов принимались попытки запретить оборот криптовалюты в стране. Разработанный Минфином в 2016 году законопроект, которым предлагалось ввести в Уголовный кодекс РФ статью 187.1, устанавливающую ответственность за оборот денежных

суррогатов (к коим предлагалось отнести криптовалюту), тому подтверждение. Однако, данный законопроект не был внесен в Государственную Думу по причине отсутствия в законодательстве термина «денежный суррогат».

4 сентября 2017 года Центробанк выпустил письмо «Об использовании частных и виртуальных валют» (криптовалют)», указав, что большинство операций с криптовалютами совершаются вне правового регулирования как в РФ, так и в большинстве зарубежных государств.

25 января 2018 года Минфин опубликовал проект Федерального закона «О цифровых финансовых активах», определяющий основные понятия в сфере виртуальных финансов, устанавливающий в качестве основной задачи закрепление в российском праве финансовых активов, создаваемых и выпускаемых с использованием цифровых технологий.

Впрочем, воплощение проекта Федерального закона в жизнь не заставило себя долго ждать и 1 января 2021 года вступил в законную силу Федеральный закон от 31.07.2020 года №259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации».

Вместо распространенного термина «криптовалюта» закон о цифровых активах использует термин «цифровая валюта». Пункт 3 статьи 1 определяет цифровую валюту как совокупность электронных данных (цифрового кода или обозначения), содержащихся в информационной системе, которые предлагаются и (или) могут быть приняты в качестве средства платежа, не являющегося денежной единицей Российской Федерации, денежной единицей иностранного государства и (или) международной денежной или расчетной единицей, и (или) в качестве инвестиций и в отношении которых отсутствует лицо, обязанное перед каждым обладателем таких электронных данных, за исключением оператора и (или) узлов информационной системы, обязанных только обеспечивать соответствие порядка выпуска этих электронных данных и осуществления в их отношении действий по внесению (изменению) записей в такую информационную систему ее правилам.

Важно учесть, что на сегодняшний день Федеральный закон от 31.07.2020 года №259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» напрямую запрещает физическим и юридическим лицам оплачивать и принимать в качестве оплаты за товары, работы и услуги цифровую валюту (п. 10 ст. 4). Данную идею Минфин преследовал еще в 2018 году при разработке и опубликовании проекта Федерального закона.

Мы полагаем, что отношения, связанные с оборотом цифровых активов и цифровой валюты не должны находиться за рамками правового регулирования в целом, уголовно-правового, в частности. В доктрине верно отмечается – уголовно-правовая охрана общественных отношений по обороту цифровой валюты должна обеспечиваться вне зависимости от соблюдения или нарушения правил ее оборота потерпевшим [1, с. 146]. Даже если лицо нарушило порядок оборота ЦФА или криптовалюты, установленный Федеральным законом от 31.07.2020 года №259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» (далее – ФЗ №259) (например, получило цифровую валюту в качестве средства оплаты товаров (работ, услуг), не проинформировало в установленном порядке налоговые органы о факте обладания цифровой валютой, проигнорировало запрет на владение и (или) пользование иностранными цифровыми финансовыми инструментами, установленный в отношении государственных служащих), то корыстное посягательство на соответствующие цифровые объекты необходимо расценивать как преступление [7, с. 75]. Противоправное поведение потерпевшего в этом случае может повлечь применение к нему финансовых, дисциплинарных санкций, но оно не меняет сущности преступного посягательства и не исключает уголовной ответственности лиц, извлекающих выгоду за счет умышленного причинения ущерба обладателю ЦФА или криптовалюты.

В судебной практике давно сформировалась позиция, согласно которой преступное поведение лица не препятствует привлечению к уголовной ответственности за хищение принадлежащего ему имущества, даже если это имущество

выступало предметом или средством совершения другого преступления или правонарушения. Так, в силу пункта 16 Постановления Пленума Верховного Суда РФ от 15.06.2006 №14 (ред. от 16.05.2017) «О судебной практике по делам о преступлениях, связанных с наркотическими средствами, психотропными, сильнодействующими и ядовитыми веществами» действия лица, сбывающего с корыстной целью под видом наркотических средств какие-либо иные средства или вещества, следует рассматривать как мошенничество, несмотря на то, что обманутый приобретатель наркотика сам совершает преступление (покушение на незаконное приобретение наркотического средства). Точно так же и преступное поведение взяткодателя не мешает квалифицировать обманное завладение принадлежащими ему ценностями в качестве мошенничества.

В. В. Хилюта, не являясь сторонником признания криптовалюты предметом преступлений против собственности, все же настаивает на том, что уголовное право охраняет те отношения, которые уже есть и сложились на практике, при этом не имеет особого значения, успели ли цивилисты разработать для них соответствующие конструкции и придать им позитивный статус [8, с. 63]. Поэтому установленные ч. 6 ст. 14 ФЗ №259 ограничения на судебную защиту требований обладателей цифровой валюты, нарушивших порядок ее оборота, могут проявляться лишь в гражданско-правовой сфере. Отсутствие регулирования криптовалют не должно означать отсутствия их уголовно-правовой охраны.

Федеральный закон от 31.07.2020 года №259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» устанавливает, что для целей законодательства о банкротстве, исполнительном производстве и антикоррупционном законодательстве – цифровая валюта признается имуществом, т.е. входит в состав конкурсного имущества и т. д. Этим устанавливается признание вещных прав на криптовалюту и возможность их судебной защиты. Возникает двоякая, не свойственная другим видам объектов гражданских прав ситуация: вещные права на криптовалюту подлежат правовой защите, а обязательственные, т.е. вытекающие из гражданско-правовых договоров, по которым криптовалюта получена в

качестве встречного представления, – не подлежат. Признавая криптовалюту имуществом, становится очевидной их имущественная ценность, и как следствие – необходимость её уголовно-правовой защиты.

Наиболее распространённым хищением криптовалют является фишинг. Используя данный способ хищения, преступник ставит перед собой цель не взломать техническую защиту информационной системы, на которой находятся счёт со средствами потенциальной жертвы, а лишь завладеть счётом и воспользоваться средствами от имени владельца данного счёта. Распространенность данного способа обусловлена простотой его реализации, а также возможностью анонимно похитить денежные средства или права на имущество.

Используя фишинг, злоумышленник не взламывает технические средства защиты различных платформ (в нашем случае инвестиционной платформы), следовательно, в соответствии со статьей 12 Федерального закона от 02.08.2019 №259-ФЗ «О привлечении инвестиций с использованием инвестиционных платформ и о внесении изменений в отдельные законодательные акты Российской Федерации» (далее – ФЗ от 02.08.2019 №259) оператор инвестиционной платформы не несёт материальную ответственность за хищение цифровых прав внутри его инвестиционной платформы при таком способе хищения. Данное обстоятельство свидетельствует о том, что инвестору необходимо самостоятельно защищать свои права и не надеяться на помощь оператора инвестиционной платформы [6, с. 48], что указывает на дополнительный криминогенный фактор (помимо латентности) данного преступления.

Елена Бондарь раскрывает понятие фишинга, как мошенничества, в результате которого злоумышленники заманивают доверчивых пользователей на свои сайты, замаскированные под сайты заслуживающих доверия организаций, и выведывают у них персональные данные, номера счетов и кредитных карт [3, с. 27]. Данное определение не является бесспорным, так как замаскированный сайт является лишь конкретным способом совершения фишинга, а не главным признаком состава преступления. Валерий Гречишников косвенно раскрывает понятие фишинга как использование социальной инженерии, заставляя жертву

добровольно раскрыть информацию о паролях или банковских реквизитах либо напрямую перевести денежные средства на указанный счет. Хачатурова С.С. раскрывает суть понятия фишинг как завладение личными данными обычных людей посредством компьютерных технологий с целью завладения их средствами, в том числе и финансовыми. Дмитрий Бахтеев определяет фишинг как комплекс методов по получению конфиденциальной пользовательской информации [2, с. 25].

Анализируя данные определения, стоит обратить особое внимание на синтез метода социальной инженерии и компьютерных технологий при использовании фишинга в сети Интернет.

Безусловно, на практике могут возникать примеры фишинга при помощи использования телефонных звонков или посредством рассылки SMS-сообщений, однако, на сегодняшний день актуальность указанных способов сходит на нет.

Итак, фишинг в сфере цифровых прав следует понимать как мошенничество с использованием компьютерных технологий, направленное на завладение информацией о конфиденциальных данных пользователей без взлома технических средств защиты информационных систем с целью хищения цифровых прав.

Фишинг посягает на несколько объектов уголовно-правовой охраны: на общественные отношения, обеспечивающие безопасность в сфере компьютерной информации, а также непосредственно на отношения прав собственности. Для начала стоит разобраться с объективной стороной преступления, предметом которого выступает компьютерная информация.

Из буквального толкования диспозиции статьи 272 Уголовного кодекса РФ следует, что не всякая компьютерная информация охраняется уголовным законом. Следовательно, для того, чтобы понять, подпадает ли данное общественно-опасное деяние под категорию преступлений, в сфере компьютерной информации, необходимо установить, на какие именно данные пользователя сети «Интернет» направлено преступное посягательство и являются ли они объектом уголовно-правовой охраны?

Статья 9 Федерального Закона от 02.08.2019 №259-ФЗ «О привлечении инвестиций с использованием инвестиционных платформ» предусматривает способ подтверждения утилитарного цифрового права цифровым свидетельством, под которой понимается – неэмиссионная бездокументарная ценная бумага, не имеющая номинальной стоимости, удостоверяющая принадлежность ее владельцу утилитарного цифрового права.

Законодатель урегулировал создание и функционирование аккаунта пользователя (депонента) для учёта цифровых свидетельств с помощью так называемого счёта депо, информацию о котором ведёт непосредственно депозитарий, что делает невозможным хранение цифрового права, цифровой валюты или цифрового финансового актива непосредственно у инвестора, однако, в соответствии с пунктом 3 статьи 9 вышеназванного Федерального закона, депозитарий осуществляет в инвестиционной платформе утилитарное цифровое право, в отношении которого выдано цифровое свидетельство, по указанию депонента, на счете депо которого осуществляется учет прав на цифровое свидетельство. Следовательно, главной задачей преступника будет получение доступа к счёту депо, где будет существовать реальная возможность распоряжения цифровым имуществом, однако, для этого преступнику потребуется пройти аутентификацию.

Законодатель в данном Федеральном законе не предусмотрел никаких императивных способов аутентификации пользователя при входе в счёт депо в инвестиционной платформе, но, можно предположить, что таким способами будет пароль от конкретного счёта. В таком случае, пароль от счета депо – это конфиденциальные данные пользователя.

Определившись с предметом посягательства, необходимо разобраться с вопросом о том, относится ли пароль от инвестиционной платформы, к компьютерной информации, охраняемой законом. Понятие «охраняемая законом компьютерная информация» носит расплывчатый характер и охватывает практически всю информацию на машинном носителе [4, с. 12]. По своей сути пароль – это средство идентификации для входа в счёт депо, следовательно, он является

неотъемлемой часть информации о таком счёте. Думается, что охраняемой является всякая информация, которая защищена от неправомерного входа.

Для защиты пароля как средства идентификации в инвестиционной платформе стоит руководствоваться пунктом 1 статьи 8.6 Федерального закона «О рынке ценных бумаг» от 22.04.1996 №39-ФЗ, согласно которому держатели реестра и депозитарии обязаны обеспечить конфиденциальность информации о лице, которому открыт лицевой счет (счет депо), а также информации о таком счете, включая операции по нему. Безусловно, отношения, связанные с оборотом цифровых прав и цифровых валют не подпадают под действие указанного Федерального закона, между тем, использовать положения данной статьи при защите законных интересов граждан возможно по аналогии.

Важно обратить внимание на то, что данная статья обязывает депозитария обеспечить конфиденциальность пароля, а в случае нарушения конфиденциальности, в силу п.6 данной статьи, депонент имеет право требовать от депозитария возмещения убытков.

Полагаем, что в случае фишинга, когда лицо самостоятельно передаёт данные преступникам под влиянием обмана или существенного заблуждения, именно по вине инвестора нарушается конфиденциальность данной информации, следовательно, в случае фишинга депозитарий не несёт ответственность за нарушение конфиденциальности информации и не обязан возмещать убытки депоненту, так как убытки возникли по вине депонента.

Следующим признаком объективной стороны преступления в сфере компьютерной информации является неправомерность доступа к паролю. Под неправомерным доступом следует понимать несанкционированное собственником или владельцем информации ознакомление с данными, содержащимися на машинных носителях или в ЭВМ, имеющими уровень защиты в соответствии с законодательством. Как правило, при фишинге, сам собственник передаёт преступнику пароль от счёта, однако данная передача конфиденциальных данных происходит под влиянием обмана или существенного заблуждения, следовательно, передача данных имеет порок воли, который влечёт за собой отсутствие добровольности

на передачу данных. На основании вышеизложенного, при фишинге передачу данных следует считать несанкционированной с собственником.

Данный состав является материальным, так как предусматривает наличие последствий в виде уничтожения, блокирования, модификации либо копирования компьютерной информации. В случае фишинга, пароль в любом случае будет копирован в строку введения преступником, следовательно, лицо полностью выполнит объективную сторону преступления.

Подводя итог объективной стороны преступления (фишинга) в сфере компьютерной информации, можно говорить о том, что на основании приведенных ранее в ходе исследования положений нормативных актов, пароль от счёта депо в инвестиционной платформе не имеет самостоятельной нормы для его охраны, между тем, его защита возможна по аналогии, путем обращения к Федеральному закону «О рынке ценных бумаг» от 22.04.1996 №39-ФЗ. Само хищение и копирование пароля от счёта депо в инвестиционной платформе подлежит уголовно-правовой оценке и является основанием для привлечения к уголовной ответственности по статье 272 Уголовного кодекса РФ.

Оценивая объективную сторону преступления, предметом которого является имущество (цифровые права, цифровая валюта), стоит обратить внимание на статью 159.6 Уголовного кодекса РФ – Мошенничество в сфере компьютерной информации, то есть хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей.

Проводя анализ признаков объективной стороны преступления, направленного на хищение имущества путем фишинга, стоит обратить особое внимание на тот факт, что по статьи 272 Уголовного кодекса РФ лицо несёт ответственность только при неправомерном доступе к охраняемой законом информации, следовательно, состав статьи 159.6 Уголовного кодекса РФ не охватывает состав статьи 272 Уголовного кодекса РФ. Данный вывод подтверждается и абз. 2 п. 20

Постановления Пленума Верховного Суда РФ от 30.11.2017 №48 (ред. от 15.12.2022) «О судебной практике по делам о мошенничестве, присвоении и растрате», согласно которому, мошенничество в сфере компьютерной информации, совершенное посредством неправомерного доступа к компьютерной информации или посредством создания, использования и распространения вредоносных компьютерных программ, требует дополнительной квалификации по статье 272, 273 или 274.1 УК РФ.

Стоит обратить внимание на тот факт, что фишинг не направлен непосредственно на хищение чужого имущества, а направлен лишь на облегчение доступа к данному имуществу путем получения пароля. Согласно абзацу 3 пункта 2 Постановления Пленума Верховного Суда РФ от 30 ноября 2017 г. №48 «О судебной практике по делам о мошенничестве, присвоении и растрате» если обман не направлен непосредственно на завладение чужим имуществом, а используется только для облегчения доступа к нему, действия виновного в зависимости от способа хищения образуют состав кражи или грабежа, то и сам фишинг образует состав кражи либо грабежа в зависимости от способа хищения.

Пункт 21 данного Постановления разъясняет случаи, когда хищение происходит от имени владельца счёта депо. В тех случаях, когда хищение совершается путем использования учетных данных собственника или иного владельца имущества независимо от способа получения доступа к таким данным (тайно либо путем обмана воспользовался телефоном потерпевшего, подключенным к услуге «мобильный банк», авторизовался в системе интернет-платежей под известными ему данными другого лица и т. п.), такие действия подлежат квалификации как кража, если виновным не было оказано незаконного воздействия на программное обеспечение серверов, компьютеров или на сами информационно-телекоммуникационные сети. Указанная позиция, являющаяся спорной, находит свое отражение в правоприменительной практике. Спорная она потому, как на практике могут возникать случаи, в которых потерпевший, используя открытость информации о договорах инвестирования, сможет наблюдать за выводом собственных средств с лицевого счёта и путем сообщений в электронной почте давать

преступнику понять о том, что хищение происходит в его присутствии. В таком случае п.20 Постановления Пленума Верховного Суда РФ от 30 ноября 2017 г. №48 «О судебной практике по делам о мошенничестве, присвоении и растрате» будет противоречить п. 3 и/или п.5 Постановления Пленума Верховного суда от 27 декабря 2002 года №29 «О судебной практике по делам о краже, грабеже и разбое», так как на лицо будут все признаки грабежа. Думается, что физическая отдаленность преступника и надлежащего собственника цифровых прав с учётом специфики функционирования сети «Интернет» не будет является основанием для квалификации деяния как кражи в силу того, что преступник будет осознавать понимание собственника о противоправности его действий в момент их совершения.

Таким образом, фишинг квалифицируется по статье 158 Уголовного кодекса РФ либо по статье 161 Уголовного кодекса РФ (в зависимости от способа хищения), и в случае копирования идентификационных данных (пароля) потребуется дополнительная квалификация по ст.272 Уголовного кодекса РФ.

Исходя из того факта, что на сегодняшний день еще не сформировалась правоприменительная практика по защите данного специфического права, полагаем, что следует руководствоваться разъяснениями Постановления Пленума Верховного Суда РФ от 27 декабря 2002 г. №29 «О судебной практике по делам о краже, грабеже и разбое», а именно пунктом 6, согласно которому кража и грабеж считаются оконченными, если имущество изъято и виновный имеет реальную возможность им пользоваться или распоряжаться по своему усмотрению, а так же пунктом 6 Постановления Пленума ВС РФ от 30 ноября 2017 г. №48 «О судебной практике по делам о мошенничестве, присвоении и растрате» согласно которому, если мошенничество совершено в форме приобретения права на чужое имущество, преступление считается оконченным с момента возникновения у виновного юридически закрепленной возможности вступить во владение или распорядиться чужим имуществом как своим собственным. Следовательно, моментом окончания фишинга стоит считать с момента возникновения у преступника возможности распорядиться чужим цифровым правом, а именно с момента входа в

счёт депо. В свою очередь оконченным хищением цифровой валюты следует считать момент получения на публичный адрес преступника цифровой валюты.

Субъективная сторона фишинга, как способа хищения, может быть выражена только в форме прямого умысла, тогда как субъективная сторона фишинга, как способа неправомерного доступа к компьютерной информации, может быть выражена как форме прямого, так и косвенного умысла.

Субъектами преступления фишинга, как способа хищения, могут быть лица, достигшие 14-летнего возраста, а субъектами преступления фишинга, как способа неправомерного доступа, к компьютерной информации – лица, достигшие 16-летнего возраста.

Список литературы

1. Абрамова Е.Н. К вопросу о понятии криптовалюты: проблемы терминологии и формирования дефиниции / Е.Н. Абрамова // Банковское право. – 2021. – №2. – С. 19–27. DOI 10.18572/1812-3945-2021-2-19-27. EDN CKLHBP

2. Бахтеев Д.В. О некоторых современных способах совершения мошенничества в отношении имущества физических лиц / Д.В. Бахтеев // Российское право. – 2016. – №3. – С. 22–25.

3. Гречишников В.А. Детерминанты мошенничества с использованием электронных средств платежа и способы его предупреждения / В.А. Гречишников // Российский судья. – 2019. – №5. – С. 25–30.

4. Гульбин Ю. Преступления в сфере компьютерной информации / Ю. Гульбин // Российская юстиция. – №10. – С. 12–16.

5. Немова М.И. Криптовалюта как предмет имущественных преступлений / М.И. Немова // Закон. – 2020. – №8. – С. 145–150. EDN ICNVZZ

6. Номоконов В.А., Тропина Т.Л. Киберпреступность как новая криминальная угроза / В.А. Номоконов, Т.Л. Тропина // Криминология: вчера, сегодня, завтра. – 2012. – №1 (24). – С. 44–49.

7. Ображиев К.В. Преступные посягательства на цифровые финансовые активы и цифровую валюту: проблемы квалификации и законодательной

регламентации / К.В. Ображиев // Журнал российского права. – 2022. – №2. – С. 71–87. DOI 10.12737/jrl.2022.018. EDN TFLWKT

8. Хилюта В.В. Криптовалюта как предмет хищения (или к вопросу о переформатировании предмета преступлений против собственности) / В.В. Хилюта // Библиотека уголовного права и криминологии. – 2018. – №2. – С. 58–68. EDN YRVHGI