

ПРОБЛЕМЫ КВАЛИФИКАЦИИ МОШЕННИЧЕСТВА С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

А. А. Галягина, студентка II курса направления «Юриспруденция» Саранского кооперативного института (филиала) автономной некоммерческой образовательной организации высшего образования Центросоюза Российской Федерации «Российский университет кооперации»

Научный руководитель: **И. П. Асанова**, кандидат филологических наук, доцент кафедры публичного права Саранского кооперативного института (филиала) автономной некоммерческой образовательной организации высшего образования Центросоюза Российской Федерации «Российский университет кооперации»

Рассматриваются проблемы квалификации мошенничества с использованием информационных технологий.

Ключевые слова: мошенничество, квалификация мошенничества, мошенничество с использованием информационных технологий.

XXI век значительно отличается от предыдущих тем, что пользование и усовершенствование информационных технологий все больше набирает темпы. Информационные технологии настолько облегчили рутинную жизнь человека, что все манипуляции, действия мигом совершаются одним нажатием кнопки, что значительно облегчают работу человека, не затрачивая на это большое количество времени. Поэтому практически все сферы жизни общества переходят на более высокую ступень развития, используя в своей деятельности техническое обеспечение в виде компьютеров и сети Интернет. Безусловно, информационные технологии не стоят на месте, уже невозможно представить какую-либо сферу, где не используют компьютеры. Так, например, использование кредитных карт для хранения денежных сбережений, передача важной информации через Интернет или использование электронной цифровой подписи в какой – либо деятельности и т.д. Так можно привести множество примеров из жизни, где широко используется компьютерная информация. Теперь нереально видеть наш мир без компьютерных технологий, ибо они

поглотили все сферы общественных отношений, но, к сожалению, параллельно с этим пришли проблемы, наносящие вред человеку в роли пользователя компьютерных технологий. В связи с этим появляется новый уровень преступности – преступность в сфере компьютерной информации.

Ни для кого не секрет что такое «фишинг». Это вид интернет-мошенничества, где главной целью является получение доступа к конфиденциальным данным пользователей — логинам и паролям. Кроме того, сильно распространилось мошенничество с использованием информационных технологий. Поэтому возникла потребность ввести меры воздействия против преступников в данной области. Отсюда вытекает проблема, как квалифицировать такой вид преступлений? Она остается актуальной по сей день.

Пример «фишинга» можно рассмотреть в следующем. Мошенник дает возможность пользователю ввести личные данные, например, свою информацию о кредитных картах. Заметим, что все манипуляции лицо выполняет целиком и полностью сам, не догадываясь, что оно попадает в ловушку мошенников.

Под мошенничеством понимается получение чужого имущества или приобретение права на чужое имущество путём обмана или злоупотребления доверием. Это определение находит свое место в ст. 159 УК РФ. При этом лицо, которое попало в такую «ловушку», свободно передаёт свое имущество либо право на него. Неоднократно, при таком типе мошенничеств, лицо, в отношении которого совершилось преступление, узнаёт о отрицательных последствиях произошедшего через некоторое время, например, когда посмотрел счет своей сберегательной карты и увидел отрицательный счет. Получается, отсутствует один из главных признаков состава преступления – «добровольность».

Вниманию представлены термины, которые встречаются в определении значения мошенничества: «злоупотребление доверием» и «обман». Отсюда создается вопрос: кто же здесь является объектом обмана? В нашем понимании

заключается то лицо, которое совершило преступление, т.е. преступник обхитряет компьютер и получает имущество жертвы. Но, ссылаясь на Постановление Пленума Верховного суда РФ от 27.12.2007 № 51 "О судебной практике по делам о мошенничестве, присвоении и растрате», говорится об обмане или злоупотреблении доверием, как об объективной стороне состава мошенничества; наряду с этим на месте объекта обмана изначально стоит человек, соответственно, потерпевшим лицом не будет являться не компьютер, не компьютерная информация. При данном виде преступления нужна тесная связь между потерпевшим и преступником, так как изначально воздействие идет на психику личности, а действия компьютерной информации имеют абсолютно технический характер.

Таким образом, законодатель закрепляет в Уголовном законе статью 159.6 «Мошенничество в сфере компьютерной информации» [1, С.114].

Если прибегнуть к мировой практике, то известно, что в Австралии такие деяния квалифицируются, как «имущественный вред, причинённый с целью извлечения незаконной выгоды для преступника или третьего лица, путём влияния на процессы автоматизированной обработки данных с помощью специальных программ, ввода, изменения или уничтожения данных или иным способом, влияющим на процесс обработки данных». Мысль этой статьи понятна, что объектом является не сам компьютер, не процессы автоматизированной обработки данных, а различные программы, подобно способу, посредством которого лицо создает преступление.

При анализе состава преступления с использованием информационных технологий, выявляются значимые разногласия, применяемые к преступлениям такого рода. [2] Они выражаются как в объекте, так и в квалифицирующих признаках. Эта тема приходится одной из главных для уголовного законодательства РФ на сегодняшний день. Отсюда и нет единого мнения сравнительно природы подобных преступлений. Следовательно, законодателю следует разработать правильный путь к решению этого вопроса, так как люди

поддаются многим жизненным обстоятельствам и нередко совершают такого рода преступления. [3]

Выходит, что понятие «компьютерное мошенничество» не оправдывает характеристику мошенничества и различного рода хищения с использованием компьютерных технологий, в связи с этим следует включить в качестве квалифицирующего признака кражи (ст.158 УК РФ), где смысл заключается не в обмане тех или иных потерпевших с использованием информационных технологий, а только так, как это сказано нормой ст. 159.6 УК РФ «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» или же вводить дополнительные статьи, регулирующих ответственность за любые виды хищения с применением компьютерных технологий.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. «Уголовный кодекс Российской Федерации» от 13.06.1996 № 63-ФЗ (с изм. и доп.) // Консультант Плюс. Информационно-правовой портал. – Режим доступа: [URL:http://www.consultant.ru/](http://www.consultant.ru/).
2. Антонов, И. О., Шалимов А. Н. Актуальные проблемы расследования мошенничества с использованием компьютерной информации. [Электронный ресурс]. Научная электронная библиотека – Режим доступа: URL: <http://cyberleninka.ru/article/n/aktualnye-problemy-rassledovaniya-moshennichestva-s-ispolzovaniem-kompyuternoy-informatsii>
3. Алферова, Ю. О. Проблемы квалификации компьютерного мошенничества. – Научная электронная библиотека. Режим доступа: URL: <http://cyberleninka.ru/article/n/problemy-kvalifikatsii-kompyuternogo-moshennichestva>.