Гужанова Е. Г.

МОШЕННИЧЕСТВО: ПРОБЛЕМЫ КВАЛИФИКАЦИИ

Гужанова Екатерина Гайозовна, студентка 2 курса Белорусского государственного университета, г. Минск, Беларусь, guganova2003@gmail.com

Научный руководитель: ст. преподаватель Кривой А. Н.

IT-технологии стали новой реальностью всех сфер общественной жизни, в том числе криминальной. Преступники активно используют компьютерные технологии при совершении преступлений экономической направленности, что существенно упрощает им доступ к имуществу и имущественным правам.

Одним из способов улучшения правоприменительной практики является изучение и использование законодательного опыта зарубежных государств. Так, в целях упрощения судебной практики законодатель Российской Федерации для квалификации такого рода преступлений добавил ст. 159.6 Уголовного кодекса Российской Федерации «Мошенничество в сфере компьютерной информации», т. е. 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.

Рассмотрим вопрос о целесообразности применения законодательного опыта Российской Федерации по включению в Уголовный кодекс статьи, предусматривающей ответственность за компьютерное мошенничество.

Прежде всего можно сказать, что после введения в Уголовный кодекс Российской Федерации (УК РФ) данной статьи, предусматривающей ответственность за мошенничество в сфере компьютерной информации, в отсутствие каких-либо разъяснений практикующим юристам в этой стране пришлось столкнуться с множеством проблем применения этой нормы.

Мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ) – это не обманное, «классическое» мошенничество, которым мы привыкли его представлять. Достаточно подробно освещены вопросы разграничения между собой кибермошенничества, кражи и «классического» мошенничества. На практике могут возникнуть трудности в квалификации достаточно популярного способа киберхищения – фишинга. Технология фишинга заключается в рассылке писем на электронную почту владельцам денежных средств о том, что они якобы стали победителями какой-либо акции. Если владелец переходит по ссылке, отраженной в этом письме, данные его банковской карты (электронного кошелька) отсылаются злоумышленникам. Далее денежные средства потерпевшего без его ведома перемещаются на счета, подконтрольные хакерам, причем нередко производится коррекция страниц с историей доступного баланса с целью скрыть хищение.

В основном деяния, указанные в данном составе преступления, посягают на электронные деньги потерпевших, вследствие этого можно сказать, что безналичные и электронные денежные средства выступают предметом хищения, а не приобретения права на него. В практическом аспекте это означает, что такое деяние в зависимости от обстоятельств может быть квалифицировано не только как мошенничество, но и как кража и присвоение.

Например, злоумышленник, используя незаконно добытое имя пользователя и код доступа для осуществления онлайновых безналичных банковских операций, перечислил определенную денежную сумму с расчетного счета потерпевшего на подконтрольный ему счет. Однако распорядиться ими не смог по причине ареста банковского счета. В судебной практике подобные деяния квалифицировались как покушение на мошенничество в сфере компьютерной информации. Объяснялся такой подход тем, что виновный, по сути, не достиг корыстной цели (наличие которой отличает хищение от угона, самоуправства и многих других смежных составов), никак не обогатившись от изъятия чужих денежных средств.

Как квалифицировать это действие – как кражу или кибермошенничество? Если не было воздействия, так скажем, на цифровое пространство и независимо от того, каким способом добыты учетные данные потерпевшего, то такое киберхищение подлежит квалификации как кража. Таким образом, не является кибермошенничеством изменение данных о состоянии банковского счета и (или) о движении денежных средств, произошедшее в результате использования виновным учетных данных потерпевшего. Значит, можно сказать, что фишинг представляет собой кражу. Но все-таки при получении этих данных посредством фишинга нарушается процесс обработки, хранения, передачи компьютерной информации (виновный использует вредоносное ПО, чтобы заполучить сведения), что, соответственно, позволяет хакеру незаконно завладеть чужим имуществом. А это как раз по смыслу должно признаваться мошенничеством в сфере компьютерной информации.

Таким образом, преступления, указанные в ст. 159.6 УК РФ, совершаются не путем обмана или злоупотребления доверием конкретного субъекта, а путем доступа к компьютерной системе, что находит свое отражение и в составе данного преступления. Объективная сторона компьютерного мошенничества существенно отличается от «классического мошенничества», совершенного путем обмана или злоупотребления доверием, а значит, в новом составе речь идет вовсе не о мошенничестве, а уже о самостоятельной форме хищения с конкретным способом совершения, отличным от других форм хищения чужого имущества, поэтому использование в данной статье термина «мошенничество» является некорректным. Следовательно, внедрение данного состава преступления в Уголовный кодекс Республики Беларусь нецелесообразно, так как это не позволит упростить правоприменительную практику и приведет к дополнительным теоретическим и практическим проблемам.