МОШЕННИЧЕСТВО В ЦИФРОВОЙ СРЕДЕ: ПРОБЛЕМЫ КВАЛИФИКАЦИИ

Бекмуродов Дилшодбек

Балтабаева Озода

Атаханова Фотимахон

Садриддинова Нигина

Студенты Ташкентского Государственного Юридического Университета.

https://doi.org/10.5281/zenodo.15190863

Аннотация. *Мошенничество изначально предполагало под собой преступление с хищением имущества путем обмана или злоупотребления доверием без учета цифровой среды. Эта статья предусматривает обзор проблемы при квалификации такого деяния, рассмотрение зарубежного опыта и возможные решения для этой проблемы.*

Ключевые слова: *Мошенничество, квалификация преступления, фишинг, вишинг, фарминг, объективные признаки, объект преступления, объективная сторона, nullun crimen sine lege, специальные нормы, общие нормы.*

FRAUD IN THE DIGITAL ENVIRONMENT: QUALIFICATION ISSUES

Abstract. *Fraud was originally assumed to be a crime involving theft of property by deception or abuse of trust without taking into account the digital environment. This article provides an overview of the problem of qualifying such an act, consideration of foreign experience and possible solutions to this problem.*

Keywords: *Fraud, qualification of a crime, phishing, vishing, pharming, objective features, object of a crime, objective side, nullun crimen sine lege, special rules, general rules.*

Введение:

С ежедневным развитием сферы инноваций и созданием все новых технологий заставляет людей менять свой образ жизни так что в конечном итоге делает невозможным жить без технологий. Такое развитие событий уже началось и может казаться что это очень даже хорошо: безпроблемное общение с человек находящийся в сотни километров друг от друга, уникальные идеи от искусственного интеллекта, возможность платить имея только телефон при себе и ничего лишнего. Однако как и наличие двух сторон у одной медали, так и внедрение технологический услуг может иметь негативные последствия для людей. Как определяет Уголовный кодекс Республики Узбекистан, мошенничество это завладение чужим имуществом или правом на чужое имущество путем обмана или злоупотребеления доверием[1].

[1] Уголовный Кодекс Республики Узбекистан от 22 сентября 1994 г. (в редакции от 8 октября 2024 г.)

Еще к 60 годам прошлого века **квалификация мошенничества** не представляла особого труда, однако после начала развития хакерства в 65-ых, а со временем и мошенничества к 90-ым годам[2] прошлого века, определение состава преступлений, в особенности объективной стороны, такого рода мошенничества стало намного сложнее из-за **неопредленности в понятии мошенничества.** К примеру в мошенничестве в виде вывода денежных средств с карты, потерпевший по своей воле передает их, что делает невозможным должным образом квалифицировать преступление. Со временем ничего не изменилось. Все также люди придумывают новые способы мошенничество, в то время как органы государственной безопасности и органы по кибербезопасности делают все, дабы не дать мошенникам осуществить задуманное.

Виды кибермошенничества:

Одними из самых популярных видов мошенничества в информационной среде являются фишинг, вишинг и фарминг.

Фишинг - вид интернет-мошенничества, цель которого получение доступа к конфиденциальным данным пользователя (логинам и паролям). Пользователь думает, что переходит на заявленный сайт, однако фактически его перенаправляют на подставной сайт. Как правило, жертвами фишеров становятся клиенты банков и платежных систем.[3]

Вишинг (от англ. voice — голос и phishing — фишинг), или голосовой фишинг, — вид мошенничества, при котором злоумышленники используют голосовую связь для манипуляции пользователем, например с целью получения его персональных данных, таких как учетные данные от аккаунтов в интернет-сервисах или финансовые сведения.[4]

Фарминг (Pharming) — это гибрид слов phishing «фишинг» и farming «занятие сельским хозяйством». Это похожий на фишинг тип онлайн-мошенничества, когда злоумышленники создают поддельные веб-сайты и перенаправляют туда трафик легального веб-сайта, чтобы заполучить конфиденциальную информацию пользователей.[5]

Это еще верхушка Айсберга, под которой прячется еще огромное количество методов и способов для осуществления злых умыслов мошенниками.

По официальной статистике Центра кибербезопасности, в 2024 году было выявлено 12 млн попыток совершить кибератаку, в то время как в 2023 году этот показатель составлял всего лишь 11 млн.

---

[2] Кадакин Б.И. Мошенничество в интернете. С. 13

[3]Фишинг (phishing) // TAdviser: информационный портал. – URL: https://www.tadviser.ru/index.php/Статья:Фишинг_(phishing) (дата обращения: 07.04.2025)

[4] Вишинг // Энциклопедия Касперского. – URL: https://encyclopedia.kaspersky.ru/glossary/vishing/ (дата обращения: 07.04.2025).

[5] Фарминг // Kaspersky Resource Center. – URL: https://www.kaspersky.ru/resource-center/definitions/pharming (дата обращения: 07.04.2025).

В добавок, заявления о мошенничестве, поступившвших в 2024 году возросло на 34% по сравнению с 2023 годом[6]. Осознание факта, что совершение мошенничества в информационной сети требует минимальных усилий и определение состава мошенничества для привлечения к ответственности мошенника требует больших затрат и много времени подталкивает многих на этот путь, что подтверждается вышеприведенной статистикой.

Суть проблемы квалификации:

Причиной почему возникает проблема при квалификации мошенничества лежит на неопределенности объективных признаков, то есть объекта (предмета) и объективной стороны (способ осуществления общественно опасного деяния). Конкретнее, при определении объекта, преступник на деле обманывает компьютер и приобретает какое-либо право на имущество. Это правильно только с одной стороны, ибо обманывает мошенник не компбютер, а собственника имущества или права на имущество. А с объективной стороны, такое преступление считается уникальным. Так как в роли вспомогательного инструмента выступает хищение имущества путем обмана и злоупотребления доверием. Сам факт обмана не может быть основанием для квалификации преступления как мошенничества, что делает это преступления уникальным в своем роде.[7]

Дополнением к этой проблеме можно добавить отсутствие конкретной нормы в системе законодательства Республики Узбекистан в случае совершения данного деяния в сфере компьютерной информации. А аналогия права и закона при возникновении уголовных отношений не допускается по принципу "nullun crimen sine lege", что означает "Нет наказания без закона".

Международный опыт:

Как пример, государства которые внедрили в свое законодательство нормы регулирующие мошенничество осуществленные через информационную сеть, можно взять Германию, Австрию и Российскую Федерацию. Каждый из уголовных кодексов этих государств по разному определили техническое мошенничество. **В Германии** такое деяния определено статьей 263а Уголовного кодекса как "намерение получить для себя или третьего лица имущественную выгоду, путём причинения вреда имуществу другого лица, воздействуя на результат обработки данных вследствие неправильного создания программ, использования неправильных или неполных данных, путём неправомочного

[6] Ирода Туляшева. В Узбекистане за год совершено свыше 12 млн кибератак. Официальный сайт Kun.uz. - URL.: https://kun.uz/ru/news/2025/02/03/v-uzbekistane-za-god-soversheno-svyshe-12-mln-kiberatak

[7] Комментарий к Уголовному кодексу Республики Узбекистан. Особенная часть /М. Х. Рустамбаев [Под общей ред. А .А . Палван-Заде]— Т.: ИПТД «0 ‘qituvchi», 2004. — 1024 с.

использования данных или иного неправомочного воздействия на результат обработки данных". А статья 148а Уголовного кодекса **Австрии** такое же деяние 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".[8] Что насчет **России**, там имеется разделение общей нормы (Статьи 159) на специальные нормы (159.1-159.6). Такое разделение помогает при уникальных ситуциях в суде используя специальные нормы, квалифицировать преступление по существу.

Пути решения и предложения:

Проблем достаточно, однако и решения имеются. Для решения проблемы с пониманием и улучшением квалификации мошенничества необходимо внедрить специальные нормы права, регулируюшие отношения непредусмортенные в общей норме права (168 статья УК РУз). А то, как это будет внедрено может основываться на зарубежном опыте.

Для предотвращения попадания на мошеннические действия, можно повысить уровень цифровой безопасности всех, начиная с раннего возраста.

Заключение:

В заключении можно сказать что ежедневное развитие технологий улучшает жизнь на лучшую сторону. Однако люди, желающие совершить преступления, жертвую спокойствием других, для получения выгоды, могут найти способы и методы ее совершения не смотря ни на что.

REFERENCES

1. Уголовный Кодекс Республики Узбекистан от 22 сентября 1994 г. (в редакции от 8 октября 2024 г.)
2. Кадакин Б.И. Мошенничество в интернете. С. 13
3. Фишинг (phishing) // TAdviser: информационный портал. – URL: https://www.tadviser.ru/index.php/Статья: Фишинг_(phishing) (дата обращения: 07.04.2025)
4. Вишинг // Энциклопедия Касперского. – URL: https://encyclopedia.kaspersky.ru/glossary/vishing/ (дата обращения: 07.04.2025).

[8] Алферова Ю.О, Дементьев О.М. Проблема квалификации компьютерного мошенничества, под ред. SCIENCE TIME, С 6.

5. Фарминг // Kaspersky Resource Center. – URL: https://www.kaspersky.ru/resource-center/definitions/pharming (дата обращения: 07.04.2025).
6. Ирода Туляшева. В Узбекистане за год совершено свыше 12 млн кибератак. Официальный сайт Kun.uz. - URL.: https://kun.uz/ru/news/2025/02/03/v-uzbekistane-za-god-soversheno-svyshe-12-mln-kiberatak
7. Комментарий к Уголовному кодексу Республики Узбекистан. Особенная часть /М. Х. Рустамбаев [Под общей ред. А .А . Палван-Заде]— Т.: ИПТД «0 ‘qituvchi», 2004. — 1024 с.
8. Алферова Ю.О, Дементьев О.М. Проблема квалификации компьютерного мошенничества, под ред. SCIENCE TIME, С 6.