Impact Factor: 9.9 ISSN-L: 2544-980X

Правовые Аспекты Противодействия Кибермошенничеству В Республике Узбекистан

Маримбоев М. Р. [1]***, Югай Л. Ю*** [2]

Одной важнейших задач, предусмотренных в рамках реализации Стратегии «Узбекистан-2030», утвержденной Указом Президента Республики Узбекистан № УП-158 от 11.09.2023 г. является обеспечение кибербезопасности на национальном Интернет-пространстве.

При этом, согласно отчету за 2023 г. Государственного унитарного предприятия (ГУП) «Центр кибербезопасности», если в 2022 г. в национальном киберпространстве Республики Узбекистан было зафиксировано 4433789 кибератак, то уже в 2023 г. зарегистрировано 11020235 кибератак. Таким образом, за указанный период наблюдается рост кибератак в национальном виртуальном сегменте Республики Узбекистан на 148%.[3]

Рассматривая вопрос актуальности кибермошенничества, можно сказать, что в законодательстве Республики Узбекистан для кибермошенничества не предусматривается отдельная статья. Оно является квалифицирующим признаком мошенничества и закреплено в пункте «г» части 3, статьи 168 Уголовного кодекса Республики Узбекистан.

Зачастую в правоприменительной практике квалификация кибермошенничества возникало затруднение у следователей. В связи с чем, в Республике Узбекистан *была принята новая редакция Постановления Пленума Верховного Суда Республики Узбекистан № 17 «О судебной практике по делам о мошенничестве» от 23 июня 2023 г., которая предусматривает особенности квалификации мошенничества, в том числе совершенного с использованием информационной системы и информационных технологий. Предыдущее Постановление Пленума Верховного суда Республики Узбекистан № 35 «О судебной практике по делам о мошенничестве» от 11 октября 2017 г. данные аспекты не охватывало.*

Принятое Постановление Пленума Верховного суда определило, что под мошенничеством, совершенным с использованием информационной системы, в том числе информационных технологий (пункт «г» части третьей статьи 168 УК), понимается хищение имущества, находящегося в финансовых, банковских учреждениях, фондах и т.п., совершаемое путем обмана посредством манипулирования с помощью компьютерного оборудования, мобильного телефона, планшета или других подобных технических устройств.

При этом, при анализе национального законодательства Республики Узбекистан некоторые специалисты отмечают об отсутствии отдельных норм в Уголовном Кодексе Республики Узбекистан. По их мнению, необходимо включить новый раздел «Преступления в сфере информационных технологий и безопасности, средств телекоммуникаций и связи», который будет включать в себя отдельные более узкие главы»[4].

[1] Курсант 2-курса факультета Следственной деятельности Академии МВД Республики Узбекистан

[2] Научный руководитель, доктор юридических наук, и.о. профессора кафедры Административной деятельности ОВД Академии МВД Республики

[3] O'zbekiston Respublikasi kiberxavfsizligi - 2023 yil hisoboti. Режим доступа: https://csec.uz/uz/news/maqolalar/o-zbekiston-respublikasi-kiberxavfsizligi-2023-yil-hisoboti/. Дата доступа: 02.02.2024.

[4] Расулев А.К., Югай Л.Ю. Совершенствование уголовно-правовой политики в сфере противодействия киберпреступности в Республике Узбекистан // Защитник Отечества. – 2023. – №16. С. 308-309.

Кроме того, имеются и иные мнения, согласно которым необходимо внести в Пленум Верховного Суда Республики Узбекистан «О судебной практики по делам о мошенничеств» такие определения как киберворовство, кибермошенничества в целях единого толкования, квалификации и дальнейшего расследования данной категории уголовных дел» [4].;.

Присоединяясь к вышеуказанным мнениям, считаем целесообразным внести уголовную ответственность за совершение кибермошенничества как отдельную статью 168[1] УК Республики Узбекистан.

К примеру, кибермошенничество включает в себя отдельные подвиды, способы и впоследствии размер нанесенного ущерба может быть разным. Способами совершения кибермошенничества, является вишинг (с помощью телефонного звонка), фишинг (через отправления ссылки), получения обманным путем личных данных и т.д. Наглядным примером к этому может быть тот факт, что во многих государствах кибермошенничество выделено в отдельную статью УК. Например: «хищение посредством использования компьютерной техники (статья 212 УК Республики Беларусь)»[5];.

Или статья 159.6 УК РФ предусматривающая уголовную ответственность за 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 Кроме того, Постановление Пленума Верховного Суда РФ от 15.12.2022 N 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет»[6] оказывает существенную помощь в квалификации данных видов преступлений. При этом основным объектом является отношения собственности независимо от ее формы, а дополнительным объектом выступают – правоотношения обеспечивающие информационную безопасность.

Исходя из всех выше предложенных мнений реализация предлагаемых средств правовой защиты позволяет повысить эффективность правоохранительной деятельности и раскрываемости кибермошенничества за счет сдерживания его распространения, разоблачения преступников и внедрения новых норм в уголовное законодательство. Можно сказать, что кибермошенничество является тем видом преступления, которому противодействовать можно путем применения организационных, правовых, социальных, технических и методических мер.

1. O'zbekiston Respublikasi kiberxavfsizligi - 2023 yil hisoboti. Режим доступа: https://csec.uz/uz/news/maqolalar/o-zbekiston-respublikasi-kiberxavfsizligi-2023-yil-hisoboti/. Дата доступа: 02.02.2024.
2. Расулев А.К. Перспективы развития политики в области противодействия киберпреступности в Узбекистане // Общество и инновации. – 2023. – №3. – Том 4. – С. 126-127.
3. Williams E.J., and Joinson A.N. Developing a measure of information seeking about phishing // Journal of Cybersecurity. 2020. Vol. 6. No. 1. P. 13.
4. Xin (Robert) Luo, Wei Zhang, Stephen Burd, Alessandro Seazzu. Investigating phishing victimization with the HeuristicSystematic Model: A theoretical framework and an exploration.

[5] Уголовный кодекс Республики Беларусь [Электронный ресурс]: от 9 июля 1999 г. № 275-З. Источник: https://pravo.by/document/?guid=3871&p0=hk9900275 – Национальный правовой Интернет-портал Республики Беларусь.

[6] О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет» [Электронный ресурс]: Постановление Пленума Верховного Суда РФ от 15 декабря 2022 г. № 37. Доступ из справ. -правовой системы «Консультант плюс».

Anderson School of Management, University of New Mexico, 1924 Las Lomas NE, MSC05 3090, Albuquerque, NM 87131, USA. URL: http://dx.doi.org/10.1016/j.cose.2012.12.003

5. Югай Л.Ю. Совершенствование уголовно-правовой политики в сфере противодействия киберпреступности в Республике Узбекистан // Защитник Отечества. – 2023. – №16. С. 308-309.
6. Сабырбаева А.Б. Электронные доказательства как новый вид доказательства при расследовании современных форм мошенничества. // Review of law sciences. – 2020. – Спец выпуск. – С. 218-219.
7. Постановление Пленума Верховного Суда РФ от 15.12.2022 N 37 "О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть Интернет https://www.vsrf.ru/documents/own/?category=resolutions_plenum_supreme_court_russian. (Дата обращения 20.04.2024г.).
8. Постановление Пленума Верховного суда Республики Узбекистан, от 23.06.2023 г. № 17 «О судебной практике по делам о мошенничестве» https://lex.uz/uz/docs/6523584. (Дата обращения 30.04.2024)