“ADOLAT”
MILLIY HUQUQIY AXBOROT MARKAZI
Guvohnoma № 636478
Litsenziya C-5669732

“HUQUQ va BURCH+” —
«ПРАВО и ДОЛГ+» —
"RIGHT and DUTY+"
Journal home page:
https://adolatmarkazi.uz/magazine/electron?id=310

2025-yil
2-son
iyul
ISSN 3093-8546



Цифровое мошенничество: трансформация классического преступления в эпоху информационных технологий

Рустам Зуфаров,
Профессор кафедры «Уголовное право, криминология и борьбы с коррупцией» Ташкентского государственного юридического университета
доктор юридических наук
e-mail: rustamaxmedovich1@gmail.com

Аннотация. Maqolada raqamli texnologiyalar va elektron aloqalarning rivojlanishi natijasida yuzaga kelgan firibgarlikning zamonaviy shakllari ko‘rib chiqiladi. Raqamli jinoyatchilar psixologiyasi, ularning harakat mexanizmlari, shuningdek, O‘zbekiston Respublikasida raqamli firibgarlik uchun javobgarlikni tartibga soluvchi huquqiy normalar tahliliga alohida e’tibor qaratilmoqda.Bunday huquqbuzarliklarning oldini olishda aholining raqamli savodxonligini oshirish va huquqiy bilimini oshirish muhimligi ta’kidlandi.

Калит сўзлар. Raqamli firibgarlik, axborot texnologiyalari, jinoiy javobgarlik, fishing, huquqiy himoya.

Аннотация. В статье рассматриваются современные формы мошенничества, обусловленные развитием цифровых технологий и электронных коммуникаций. Особое внимание уделяется психологии цифровых преступников, механизмам их действий, а также анализу юридических норм, регулирующих ответственность за цифровое мошенничество в Республике Узбекистан. Подчёркивается важность цифровой грамотности и правового просвещения населения в целях профилактики подобных преступлений.

Ключевые слова. Цифровое мошенничество, информационные технологии, уголовная ответственность, фишинг, правовая защита.

Annotation. The article examines modern forms of fraud caused by the development of digital technologies and electronic communications. Particular attention is paid to the psychology of digital criminals, the mechanisms of their actions, as well as the analysis of legal norms governing liability for digital fraud in the Republic of Uzbekistan.The importance of digital literacy and legal education of the population in order to prevent such crimes is emphasized.

Keywords. Digital fraud, information technology, criminal liability, phishing, legal protection.

Развитие цифровых технологий открыло перед обществом новые возможности, но одновременно породило и новые угрозы. Президент Республики Узбекистан Ш.М.Мирзиёев в своих выступлениях не раз поднимал вопрос об усилении цифровой безопасности и борьбы с киберпреступностью. Так, в Послании Президента Республики Узбекистан Олий Мажлису от 20 декабря 2022 года указывалось: «Мы должны усилить наши меры по обеспечению кибербезопасности, создать надежную цифровую инфраструктуру и правовую базу для борьбы с киберугрозами». Также, в рамках Стратегии «Цифровой Узбекистан – 2030» Президент неоднократно подчеркивал необходимость модернизации законодательства в области информационной безопасности, подготовки специалистов в сфере кибербезопасности, активного противодействия цифровым преступлениям.

Одной из наиболее опасных форм киберпреступности является цифровое мошенничество — преступление, совершаемое с использованием информационно-коммуникационных технологий с целью обмана и незаконного завладения чужим имуществом или данными.

Согласно статье 168 Уголовного кодекса Республики Узбекистан, мошенничество определяется как хищение чужого имущества или приобретение права на имущество путём обмана или злоупотребления доверием. В контексте цифровых технологий данное деяние получает новые формы реализации, сохраняя при этом ключевую характеристику — введение жертвы в заблуждение.

Современный мошенник – это не обязательно подозрительный субъект, вызывающий недоверие. Наоборот, он может производить впечатление уверенного, образованного и вежливого профессионала. Его поведение направлено на создание иллюзии надёжности, а знания в области психологии, IT и даже юриспруденции позволяют ему манипулировать поведением жертв. Он может имитировать официальную переписку, подделывать документы, использовать сложные схемы обмана, опираясь на знание слабых мест в системах безопасности и поведения людей.

Он действует как опытный манипулятор – знает, как вызвать у человека страх, жалость, доверие или спешку. Это делает его особенно опасным: люди сами передают ему доступ к своим деньгам или персональным данным.

С распространением информационных технологий, электронных сервисов, цифровых банков и онлайн-торговли мошенники получили в своё распоряжение новые инструменты. Сегодня мошенничество может происходить через интернет и социальные сети – фальшивые магазины, объявления о «работе мечты», просьбы о помощи от поддельных аккаунтов знакомых, через мессенджеры и SMS – ложные уведомления от «банков» или «госорганов» с просьбой ввести данные карты, через фишинг-сайты – подделки официальных сайтов, куда пользователь вводит свои личные данные, не зная, что они сразу передаются

Guvohnoma № 636478 Litsenziya C-5669732 ISSN 3093-8546

злоумышленникам.

Распространение цифровых платформ (онлайн-банкинг, маркетплейсы, электронные госуслуги) значительно расширило инструментарий злоумышленников. Среди наиболее распространённых видов цифрового мошенничества можно выделить:

Фишинг – отправка поддельных писем и сообщений от имени банков, магазинов и госорганов с целью получения персональных данных;

Вишинг – телефонные звонки от якобы представителей банка или службы безопасности с просьбой сообщить конфиденциальные данные;

Мошенничество в социальных сетях – взлом аккаунтов, рассылка фейковых сообщений от имени знакомых с просьбами перевести деньги;

Ложные интернет-магазины — создание фальшивых сайтов с целью получения оплаты за несуществующие товары;

Инвестиционные и кредитные схемы – предложения «быстрого дохода» или «выгодного кредита» с предварительным взносом.

Современные мошенники используют достижения в области искусственного интеллекта и нейросетей. С помощью технологий deepfake создаются аудио- и видеосообщения, имитирующие речь знакомых или официальных лиц. Такие методы затрудняют распознавание обмана и повышают его эффективность.

Кроме того, использование электронных цифровых подписей, особенно в системах государственных услуг (например, через портал my.gov.uz), также становится объектом атак, направленных на подделку или перехват информации.

Уголовное законодательство Республики Узбекистан предусматривает ответственность за мошенничество в зависимости от вида, масштаба ущерба и способа совершения преступления. Цифровая форма может рассматриваться как квалифицирующее обстоятельство, усиливающее ответственность.

Как было выше указано, мошенничество (статья 168 Уголовного кодекса Республики Узбекистан) — это умышленное завладение чужим имуществом или правами на имущество путем обмана или злоупотребления доверием. Это преступление относится к категории преступлений против собственности.

Закон различает несколько видов мошенничества в зависимости от тяжести, способа и последствий преступления:

Простое мошенничество – наказывается штрафом, обязательными или исправительными работами, либо ограничением или лишением свободы.

Мошенничество, совершенное группой лиц по предварительному сговору — более строгое наказание.

Мошенничество с причинением значительного ущерба гражданину или государству – является отягчающим обстоятельством.

Мошенничество в крупном и особо крупном размере — влечет более длительные сроки лишения свободы.

Мошенничество, совершенное с использованием служебного положения или в сфере предпринимательской деятельности – квалифицируется отдельно.

Современные технологии породили новые виды мошенничества, такие как: использование интернет-платформ, мессенджеров, социальных

сетей; фишинг, поддельные сайты, взлом аккаунтов; мошенничество с банковскими картами и электронными кошельками; преступления с использованием вредоносного ПО, «вирусов», ботов и т.д.

Законодательство признаёт, что использование информационных технологий при совершении преступления может рассматриваться как квалифицирующий признак, то есть такой, который усиливает ответственность.

В делах о цифровом мошенничестве ключевое значение имеют доказательства в электронном виде, это – электронные переписки, IP-адреса; данные сотовых операторов и банков; результаты технической экспертизы устройств; логи и записи серверов, облачных хранилищ и др.

Помимо этого, следственные органы всё активнее применяют цифровую криминалистику и сотрудничают с IT-компаниями.

Небезынтересна статистика по поводу цифрового мошенничества в Узбекистане. По данным Генеральной прокуратуры и Министерства внутренних дел Республики Узбекистан: в 2023 году было зарегистрировано более 18 000 случаев мошенничества, из них около 6 000 — с использованием информационно-коммуникационных технологий (ИКТ). За первые 6 месяцев 2024 года количество цифровых преступлений увеличилось на 30% по сравнению с аналогичным периодом предыдущего года. Основными жертвами цифрового мошенничества становятся пенсионеры, молодёжь и пользователи онлайн-банкинга.

Так, в Ташкенте группа лиц создала поддельный интернет-магазин с привлекательными ценами на электронику. Сотни граждан переводили деньги за несуществующие товары. Ущерб составил более 2 миллиардов сумов. Преступники были осуждены по статье 168 УК Республики Узбекистан (мошенничество, совершенное организованной группой с использованием ИКТ) и приговорены к 8 и 10 годам лишения свободы.

Один из фигурантов получил доступ к SIM-карте гражданина путем подмены и повторной активации номера. Затем он восстановил доступ к банковскому приложению и перевел средства на свои счета. Ущерб — 120 миллионов сумов. Обвиняемый осуждён на 5 лет лишения свободы.

Мошенники через фейковые страницы известных брендов в Instagram предлагали выиграть призы и запрашивали данные банковских карт. Более 300 граждан стали жертвами фишинга. Сотрудники киберполиции выявили схему, и двое подозреваемых были арестованы.

В настоящее время ведётся работа по созданию Кодекса о кибербезопасности, который будет регулировать порядок ответственности за преступления, совершённые с использованием цифровых технологий. Регулярно проводятся информационные кампании через СМИ и социальные сети. Банки Узбекистана усиливают двухфакторную аутентификацию и уведомляют клиентов о возможных рисках. Школы и вузы вводят основы цифровой грамотности, включая темы по киберугрозам. Снижение уровня цифрового мошенничества невозможно без формирования устойчивых навыков цифровой и правовой грамотности у населения. Важно помнить, что: ни один банк или госорган не запрашивает коды подтверждения, PIN-коды или пароли по телефону или через мессенджеры; необходимо проверять подлинность интернет-ресурсов (домен .uz, защищённый протокол https); следует

Guvohnoma № 636478 Litsenziya C-5669732 ISSN 3093-8546

воздерживаться от ввода персональных данных на неизвестных сайтах.

Цифровое мошенничество является актуальной угрозой в условиях стремительной цифровизации общества. Оно требует комплексного подхода, включающего законодательное регулирование, технические меры защиты и правовое просвещение. Только при взаимодействии государства, специалистов в области права и IT, а также при активном участии самих граждан можно эффективно противостоять этому опасному явлению.