КИБЕРМОШЕННИЧЕСТВО: ВЗАИМОЗАВИСИМОСТЬ МЕТОДА СОВЕРШЕНИЯ ПРЕСТУПЛЕНИЯ И ХАРАКТЕРИСТИК ЛИЧНОСТИ ПРЕСТУПНИКА

Алламбергенов Исламбек Садатдинович
ведущий научный специалист Исследовательсокого института криминологии Республики Узбекистан

Аннотация: *Актуальность работы и выбор темы обусловлены ростом количества ежегодно регистрируемых преступлений, совершённых путём обмана и злоупотребления доверием с использованием информационно-телекоммуникационных технологий и сети Интернет, крайне низким процентом их раскрываемости, сложностью установления лиц, совершивших данный вид мошенничества, что вызвано объективными и субъективными причинами, одной из которых является наличие у субъектов преступной деятельности знаний в сфере IT-технологий, возможностей их использования для разработки и реализации преступных мошеннических схем, для анонимной работы в интернет-пространстве, упрощающей сокрытие следов мошенничества.*

Ключевые слова: *информационно-телекоммуникационные технологии, сеть Интернет, виртуальное пространство, кибермошенничество, кибермошенник, личность преступника, способ преступления.*

KIBER FIRIBGARLIK: JINOYAT SODIR ETISH USULI VA JINOYATCHI SHAXS XUSUSIYATLARINING O'ZARO BOG'LIQLIGI

Annotatsiya. *Mavzuning dolzarbligi va tanlanishi aldov va ishonchni suiiste'mol qilish yo'li bilan axborot-telekommunikatsiya texnologiyalari va Internet tarmog'idan foydalangan holda sodir etiladigan jinoyatlar sonining ortishi, ularni oshkor etish darajasining juda pastligi, ushbu turdagi firibgarlikni amalga oshirgan shaxslarni aniqlashning murakkabligi bilan bog'liq. Bu muammolar obyektiv va subyektiv sabablar bilan izohlanadi, ulardan biri – jinoiy faoliyat subyektlarining IT-texnologiyalar sohasidagi bilimlari, firibgarlik sxemalarini ishlab chiqish va amalga oshirishda ulardan foydalanish imkoniyatlari, Internet makonida anonim ravishda harakat qilish imkoniyati bo'lib, bu holat firibgarlik izlarini yashirishni osonlashtiradi.*

Kalit so'zlar: *axborot va telekommunikatsiya texnologiyalari, Internet, virtual makon, kiber firibgarlik, kiber firibgar, jinoyatchi shaxsi, jinoyat usuli.*

CYBER FRAUD: THE INTERDEPENDENCE BETWEEN THE METHOD OF CRIME COMMISSION AND THE OFFENDER'S PERSONALITY TRAITS

Abstract*. The relevance of this study is determined by the rapid increase in the number of crimes committed through deception and abuse of trust using information and telecommunication technologies and the Internet. Of particular concern is the extremely low detection rate of such crimes, which is due to both objective and subjective factors. A key factor is the perpetrators' specialized knowledge in IT, which enables them to develop and implement complex fraudulent schemes, operate anonymously in the virtual space, and effectively conceal traces of their illegal activity. The methodological basis of the study includes generalization, description, analysis and synthesis, induction and deduction, as well as statistical and formal legal methods.*

Keywords: *information and telecommunication technologies, Internet, virtual space, cyber fraud, cybercriminal, offender personality, method of crime commission.*

В трактовках многочисленных словарей узбекского языка “фирибгар” – это нечестный человек, занимающийся шулерством, махинациями, специализирующийся на мошеннических операциях и аферах с целью личной наживы, ровно как и аферист – человек, занимающийся аферами, иначе – преступными схемами, построенными на желании легкой наживы.

В мире всегда существовали аферисты или мошенники, которые умудрялись, завладеть чужим имуществом или деньгами обманным путём в самых разнообразных масштабах. Пострадать от действий мошенника, а следовательно, стать жертвой мошенника может практически кто угодно.

Существует множество способов хищения чужого имущества или приобретения права на него путём обмана или злоупотребления доверием, применяемые в самых различных сферах – в предпринимательстве, образовании, здравоохранении, страховании, кредитно-банковской, информационно-коммуникационной и др. Действия мошенников, преследующих цель похитить чужую собственность или приобрести на нее права, могут также состоять из вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей. Именно мошенничество с использованием современных информационных технологий получает все большее распространение в наши дни. Как отмечают ведущие специалисты мира «специфика этой разновидности мошенничества заключается в том, что обман перенесен в виртуальный мир, в сферу информационных технологий» [1].

Опеределение иформационным технологиям дано в статье 3 Закона ”Об информатизации” и под ним понимается совокупность методов, технических средств, приёмов и процессов, применяемых для сбора, хранения, поиска, обработки и распространения информации.

Уголовно-правовой запрет на совершение мошенничества в сфере информационных систем, в том числе с использованием информационных технологий, установлен в пункте «г» части 3 статьи 168 Уголовного кодекса Республики Узбекистан.

Анализ и обобщение правоприменительной практики, научной юридической литературы и иных источников позволил прийти к выводу о том, что в контексте рассматриваемого мошенничества употребляются также понятия «компьютерное мошенничество», «мошенничество в сети Интернет», «мошенничество в сфере интернета и информационных технологий», «мошенничество с применением современных информационных технологий», «мошенничество в сфере высоких технологий», «кибермошенничество» (как разновидность киберпреступлений). Причем термин «кибермошенничества» стал достаточно распространенным и часто употребляемым. Соответственно, появившиеся, в контексте активно набирающей обороты информатизации общества, аферисты нового типа получили название «кибермошенники» [7].

Следует отметить, что кибермошенничество в нашей стране, равно как во всем мире, процветает достаточно давно. Активизацию деятельности кибермошенников следует связать с распространением в мире пандемии короновирусной инфекции COVID-19, установлением для большинства стран, исключением из которых не стал и Узбекистан, режима самоизоляции, когда граждане фактически были вынуждены оставаться в пределах мест своего проживания, обучаясь и работая удалённо.

Такой ситуацией не могли не воспользоваться кибермошенники – субъекты преступной деятльности, обладающие знаниями в сфере IT-технологий, осведомленные о проблемах организации информационной безопаснности и защиты информации и связанных с этим возможностями реализации

того или иного способа обмана или злоупотребления доверием в интернет-пространстве. С этого времени количество регистрируемых преступлений обнаруживает регуярный рост.

Так, согласно официальным данным, представленным начальником центра Кибербезопасности МВД Республики Узбекистан подполковником Б.Мамаджановым, за последние 5 лет число киберпреступлений в Узбекистане увеличилось в 68 раз. Случаи краж и мошенничества, связанных с банковскими картами с каждым днём набирают обороты. Как отмечается, количество данных преступлений в 2024 году увеличилось в 9,1 раза по сравнению с 2023 годом. За этот период число обращений от физических и юридических лиц по фактам правонарушений в киберпространстве возросло в 34 раза. В результате киберпреступлений в период с 2021 по 2024 годы граждане понесли ущерб на сумму более 1 трлн. 909 млрд. сумов. Только в 2024 году ущерб составил 603 млрд. сумов.

«Если в 2019 году с использованием информационных технологий было совершено 863 преступления по 18 видам, то в 2024 году зафиксировано 58 800 преступлений по 62 видам. Наблюдается значительный рост доли киберпреступлений в общей преступности, что делает их профилактику особенно актуальной», – заявил руководитель центра Бекзод Мамажонов.

По его словам, если в 2023 году доля киберпреступлений в общей структуре преступности составляла 6,2%, то в 2024 году она достигла 44,4% – то есть практически каждое второе преступление совершается с использованием информационных технологий. Основную часть киберпреступлений (98%) составляют преступления, связанные с банковскими картами (киберкражи и кибермошенничество).

Киберпреступления в основном совершаются следующими способами:

60% – путём отправки вредоносных ссылок и программ с целью получения доступа к банковской карте или управлению мобильным устройством;

16% – с использованием различных уловок для получения СМС-кодов подтверждения доступа к банковским картам и аккаунтам в мобильных приложениях;

4% – путём оформления онлайн-кредитов на имя пострадавшего;

11% – посредством мошенничества на онлайн-торговых платформах;

9% – через различные схемы обмана с привлечением денежных средств граждан.

Отмечено, что с целью предотвращения таких правонарушений предпринимаются различные правовые, организационные и технические меры.

На основании приведённого анализа и статистических данных видно, что в условиях широкого распространения информационно-коммуникационных технологий и неограниченного обмена информацией в режиме реального времени, киберпреступность превращается в сложную транснациональную проблему. В этой связи как никогда важно повысить осведомлённость граждан о современных киберугрозах и уровень их цифровой грамотности [9].

Изложенное свидетельствует о том, что рассматриваемое мошенничество характеризуется высокой степенью латентности и низкой раскрываемостью. Такое положение дел, а также сложность выявления и установления кибермошенников предопределяет особенность рассматриваемых деяний.

Другой их особенностью является быстрый мониторинг социальных условий, интересов и потребностей общества и на этой основе быстрое совершенствование или создание новых способов мошенничества, в том числе со сложными схемами, обеспечивающими сокрытие следов преступной деятельности, – без непосредственного контакта с жертвой, дейтсвуя анонимно и удалённо из любой точки земного шара, оставаясь недосягаемыми для правоохранителей. Однако это

не означает, что мошенники не используют более простые и уже отработанные схемы мошенничества.

Приступая к анализу типичной личности кибермошенников отметим, что сведения о ней находятся в кореляционной зависимости от способа совершения киберпреступлений и это следует учитывать в процессе их выявления, расследования и раскрытия. Представляется целесообразным обозначить, наиболее часто реализуемые на сегодняшний день, способы такого мошенничества.

Эксперты единогласно сходятся во мнении, что таковым, прежде всего, является фишинг, позвоялющий получить конфиденциальную и финансовую информацию интернет-пользователей. Фишинг как способ мошенничества реализуется посредством: а) рассылки электронных писем, замаскированных под послания от легитимных отправителей, б) предложения пользвателям посетить поддельные ресурсы. Следует отметить, что создание и продвижение таких клонированных интернет сайтов, скопированных с оригиналов, активно используется кибермошенниками. Такой обман осуществляется с целью добиться от пользователя перехода по предложенным в сообщениях ссылкам, оставления на фейковых ресурсах персональной и платежной информации, позволяющей осуществлять вход в разные сервисы, получать доступ к финасам обманутых пользователей. В отдельных случаях данные действия могут служить подготовкой к реализации комплексной атаки на компанию с этой же целью.

Принято считать, что риски и потери денежных средств со счетов клиентов кредитных и иных финансовых организаций в большей степени происходят из-за целенаправленных атак хакеров. Однако кибермошенничество также занимает одно из лидирующих мест в списке потерь организаций.

Сегодня также активно реализуется смишинг – способ кибермошенничества, заключающийся в выманивании у жертвы важной личной информации путем отправления СМС-сообщения с выдуманной проблемой и дальнейшего предложения перейти по ссылке, указанной в СМС, на замаскированный под легитимный ресурс, сайт или в приложение, в том числе заражённые вредоносным программным обеспечением, где пользователю предлагается вбить персональные данные, а также иную интересующую мошенников информацию. К разновидности смишинговой схемы можно добавить взлом аккаунтов мессенджеров и социальных сетей – WhatsApp, Telegram, “Однаклассники”, ВК, Тикток и др., с целью дальнейшей рассылки сообщений с различными просьбами от имени пользователей: например, перевести деньги, перейти по ссылкам, пройти фейковые опросы, участвовать в фейковом голосовании или в розыгрыше призов и т.п.

Поскольку сейчас практически каждый человек пользуется смартофоном, еще одним распространённым способом кибермошенничества, позволяющим завладеть личной информацией пользователя, является установка на смартфон зараженных вирусом приложений под видом обычных программ. Этому предшествует звонок мошенника на телефон пользователя от имени службы безопасности банка, сотрудников правоохранительных органов, сотрудников сотовой компании и т.п. С помощью телефонного звонка мошенник обманным путем для завладения ценной информацией заставляет жертву совершить определенные действия (*пройти по ссылке, отпарвленной в СМС, продиктовать СМС-коды, присылаемые для подтверждения транзакций, сообщить рекви-зиты банковских карт и пр.*)

Следуеть отметить вновь применяемый и усовершенствованный, активно использовавшийся ранее такой способ кибермошенничества, как заражение компьютеров, смартфонов и иных технически сложных устройств вирусом-вымогателем, который блокирует их работу, зашифровывает файлы, ставя тем

самым под угрозу хранящуюся в них информацию. При этом жертва вводится в заблуждение относительно возможности возобновления доступа к файлам и получает сообщение с требованием перевода денег на счета электронных кошельков, чаще – криптовалютных, чтобы невозможно было их отследить.

К этому следует добавить мошенничество, связанное: а) с фриланс-услугами (*размещение на сайтах предложения простого, быстрого заработка с возможностью работать удалённо за хорошее вознаграждение, но в большинстве случаев жертве предлагается предварительно оплатить выдачу обучающих материалов за «введение в профессию», включая доступ к заказам*); б) с фейковыми интернет-аукционами, предлагающими приобрести лоты (товары) по более низкой цене; в) с брокерской деятельностью (*выманивание денег посредством предложения жертве открыть брокерский счет, как правило онлайн, и получить в кратчайшие сроки сверхдоход от биржевой деятельности*); г) с онлай-играми (*предложение совершить внутриигровые покупки продуктов, например, перечисление предоплаты мошенникам за продажу игрового инвентаря*); д) с онлайн-знакомствами на соответствующих сайтах; е) с созданием финансовых пирамид; ж) с блогерской деятельностью (*выманивание денежных средств у подписчиков под предлогом инвестирования и последующей выплаты повышенных процентов в виде дохода от такой деятельности; под предлогом букмекерских ставок через «подставные» матчи*); з) с фиктивным блогерством (*выманивание денег у автора блога и подписчиков канала, заключающееся в предварительном похищении аккаунтов известных блогеров, опубликовании от их имени постов с просьбой перевода денег на различные цели, в том числе обращении к реальному блогеру с предложением возврата доступа к каналу за вознаграждение*).

Достаточно популярно на сегодняшний день кибермошенничество с криптовалютами, реализация преступной схемы которого состоит в сборе средств на развитие криптовалютных проектов с использованием фиктивного ICO (*Initial Coin Offering*) и последующей реализацией фейковой криптовалюты за валюту, имеющую реальную стоимость (*например, биткоин, эфириум*).

В любом случае реализация подобных схем позволяет кибермошенникам получить доступ к финансам своих жертв – обманутых пользователей. При этом общим для всех способов кибермошенничества будет использование информационно-коммуникационных технологий, сети Интернет, компьютерного и сетевого оборудования, программного обеспечения, средств и устройств связи и т.п. В свою очередь, как верно отмечает А.М. Кустов, «сведения о способе совершения преступления содержат большой объём криминалистически значимой информации о преступном событии и его участниках» [4]. Следовательно, абсолютно уместно говорить о том, что способ совершения кибермошенничества и личность кибермошенника находятся между собой в корреляционной связи и зависимости.

Криминалистическое изучение личности преступника включает установление криминалистически значимой информации о нем, присущих ему анатомических, биологических, психологических и социальных свойствах, знания о которых необходимы, и методических задач по раскрытию и расследованию преступления. Исходя из этого, кибермошенник является носителем указанных свойств и качеств, сформировавшихся под воздействием различных обстоятельств, окружающей среды, оказавших, в свою очередь, влияние на формирование его преступного поведения.

В частности, речь идет о социально-демографических, нравственно-психологических и иных свойствах личности, изучение и установление которых, является одним из

ключевых аспектов при расследовании преступлений.

Как свидетельствуют статистические данные, кибермошенники – лица мужского пола (83 %), в возрасте 18-30 лет (66 %), проживающие в городских населенных пунктах. Однако следует учитывать, что они легко могут менять место жительства, перемещаясь в пределах регионов, выезжая за пределы Республики Узбекистан, в том числе переезжая из страны в страну, приспосабливаясь под режимы пребывания, установленными зарубежными государствами. В случае выезда за границу, преступники, как правило, действий по смене гражданства не предпринимают, но нередко реализуют возможность оформления вида на жительство в стране пребывания. Более половины таких лиц не обременены семьей и детьми, что обеспечивает им высокую мобильность. Как следствие, это создаёт сложность установления и оперативного задержания кибермошенников. Возрастная категория предопределяет уровень дохода кибермошенников: чем меньше возраст, слабее знания, умения, навыки в IT-сфере, тем меньше дохода и финансов.

Русские учёные В.А. Аксенов и Т.В. Молчанова подразделяют интернет-мошенников на классических и профессиональных, действующих в том числе в составе организованных групп. Они отмечают, что в преступной деятельности для получения сверхдоходов первые (классические) используют телефонные устройства, компьютеры и иные информационно-телекоммуникационные технологии, вторые (профессионалы) – ведущие средства анонимизации в сети Интернет (VPN, браузер TOR и т.п.) при осуществлении звонков с использованием IP-телефонии [2].

Выражая свое согласие с предложенной классификацией, поддерживаем утверждение указанных авторов, что первой группе кибермошенников присущи, по сути, известные, но периодические модифицируемые способы мошенничества (фриланс-услуги, фейковые интернет-аукционы и брокерская деятельность, онлайн-знакомства, онлайн-игры, смишинг, вишинг, некоторые виды фишинга), реализуемые посредством интернета, компьютерных технологий, средств мобильной связи. Представители второй группы – профессионалы действуют с корыстным мотивом. Реализуемые ими схемы мошенничества достаточно сложны. В частности, это махинации с криптовалютами, хакерские атаки с целью завладения имуществом юридических лиц, средствами на банковских счетах финансовых организаций. Данной группе свойственно совершение преступлений в крупном и особо крупном размерах. Здесь обозначенные преступления могут совершаться как в одиночку (соучастники замещаются специальными программами, помогающими достичь преступного результата) так и группой, в том числе организованной, которая может состоять из таких же профессионалов-хакеров, а также включая лиц, не имеющих профессионального образования в области IT-технологий.

В большинстве случаев лица с таким профессиональным образованием ранее не судимы. Причем мотивация вовлечения их в занятие криминальной деятельностью на первых порах не всегда характеризуется корыстным мотивом, который постепенно замещает изначальный – самоутверждение, исследовательский интерес, демонстрация возможностей.

Вместе с тем уровень образования преступников распределился следующим образом: лица, имеющие высшее профессиональное образование, составили – 12,8%, среднее профессиональное образование – 29,2%, среднее общее образование – 57,9%. Причем у 75% лиц высшее и неоконченное высшее образование связано со сферой IT-технологий. Это объясняет наличие у них компетенций в области информатизации, криптовалютных, интернет и иных смежных технологий, веб-дизайна, функционирования

трансграничных цифровых сервисов, протоколов передачи данных и обработки информации и т.п.

Следует отметить, что для кибермошенников с хакерскими способностями в большей мере характерны замкнутость, виртуальное общение на закрытых форумах, контакты с узким кругом лиц. Отчасти их можно назвать эскапистами, интровертами. В беседе между собой кибермошенники используют сленг программистов, хакеров, жаргонизмы, употребляемые в среде интернет-мошенников.

Для устойчивой группы кибермошенников в связи с реализацией сложных способов обмана в преступную деятельность могут вовлекаться лица, не имеющие отношение к IT-сфере, но выполняющие промежуточные действия, носящие обеспечительный характер в механизме реализации криминальных схем. Такие лица в 48% случаев имеют криминальное прошлое и судимость за различные преступления. Вместе с тем кибермошенники – это, как правило, находчивые, изобретательные, целеустремленные, амбициозные лица. По справедливому замечанию О.Роде, они «предприимчивые, авантюристичные и даже харизматичные люди, которые могут получить крупные преступные доходы, с большой вероятностью избежав при этом уголовной ответственности» [8]. Среди них нередко встречаются лица инициативные, с хорошими организаторскими способностями.

Для выполнения промежуточных действий привлекаются подставные лица (дропы) из числа социально незащищенных, в том числе из неблагополучных слоев населения, за небольшое вознаграждение участвующие в обналичивании незаконно полученных денежных средств, на которых могут оформляться компании, аренда помещений, приобретенное оборудование и т.п. Реализация мошенничества, требующего работы с жертвами через кол-центры, предполагает привлечение для телефонного общения с ними лиц коммуникабельных, способных быстро ориентироваться в ситуации, обладающих знаниями в области психологии, социальной инженерии. Движимые мотивом легкой наживы, они активно включаются в криминальный процесс.

На основании этого выявление лиц, причастных к совершению рассматриваемых деяний, требует от правоохранительных органов тщательного изучения реальных и виртуальных контактов соучастников. Особенно большую проблему представляет установление организатора, который является мозговым центром, имеет возможность контролировать весь криминальный процесс и руководить им из любой точки планеты. Анонимизация преступной деятельности достигается посредством использование высокотехнологичных устройств, программ Tor, SSH, VPN, proxy, I2P и др., которые затрудняют возможность отслеживания местонахождения преступника. Возможность работы на удаленном рабочем сервере (особенно находящемся в другой стране) также создает препятствие в доступе правоохранительных органов к криминалистически значимой информации.

Подводя итог, еще раз подчеркнем, что достижению преступного результата кибермошенниками способствует наличие у них знаний в области IT-технологий, социальной инженерии, психологии, приобретенных посредством образования и самообразования. В процессе выявления, раскрытия и расследования рассматриваемого вида мошенничества требуется учитывать взаимосвязь и взаимозависимость между способом его совершения и личностью мошенника, анализ которых позволит судить об уровне профессионализма и компетенции мошенников, выдвинуть версии о субъектах преступной деятельности, их количестве, отведенной им роли, возможном местонахождении. Данная информация позволит правоохранительным органам своевременно принять меры по установлению и задержанию лиц, причастных к совершению преступления, пресечь возможность уничтожения следов, попытки скрыться от следствия и суда.

Использованные источники

1. Закон №560-II “Об информатизации” Республики Узбекистан от 11 декабря 2003 года
2. Аксенов В.А., Молчанова Т.В. Особенности личности современного интернет-мошенника в механизме индивидуального преступного поведения // Криминологический журнал. – 2020. № 4 – С. 79-86
3. Волохова О.В. Личность подозреваемого при установлении механизма преступления // Правовой альманах. 2023. №8 (30). С.6-11
4. Кустов А.М. Криминалистика и механизм преступления: цикл лекций. М. Московский психолого-социальный институт. Воронеж: МОДЭК. 2002. 304 с.
5. Лопашенко Н.А. Компьютерное мошенничество- новое слово в понимании хищения или ошибка законодателя?// Пермский юридический альманах. 2019. №2. С.598-609.
6. Попов А.М., Шурухов В.А. К вопросу о криминалистической характеристике киберпреступлений // Вестник криминалистики. 2023. №2 (86). С.57-69.
7. Попов А.М. Шурухунов В.А. Особенности использования и приминения компьютерно-технических средств и технологий при расследовании преступлений в условиях пандемии // Проблемы противодействия киберпреступности: материалы международной научно-практической конференции, Москва. 08.04.2023 г. М: Московская академия Следственного комитета РФ.
8. Роде О. Киберпреступник глазами российских психологов: черты, мотивы, ценности, отклонения. [Электронный ресурс]. URL: https://habr.com/ru/companies/bastion/articles/765490
9. Https://www.gazeta.uz/uz/2025/05/29/kiberjinoyat/