Pro Index | Journal of Innovation in Educational and Social Research
Volume: 2 Issue: 1 Year: 2024
ISSN: 2992-894X | http://journals.proindex.uz

О Факторах, Детерминирующих Совершение Интернет-Мошенничеств В Республике Казахстан

Намысов Ерлан Думанович
Самостоятельный соискатель Университета общественной безопасности Республики Узбекистан

Аннотация: Данная научная статья анализирует факторы, детерминирующие совершение интернет-мошенничества. Интернет-мошенничество представляет серьезную опасность как для частных лиц, так и для предприятий в связи с развитием информационных технологий и их интеграцией в повседневную деятельность общества. В этом контексте рассматриваются мотивы преступников, психологические проблемы и социальные факторы, влияющие на решение человека совершить мошенничество в Интернете. Рассматриваются такие аспекты, как наличие специализированных подразделений, международная координация, техническая оснащенность правоохранительных органов. Отмечается слабость законодательства в области кибербезопасности и проблемы с анализом и сбором цифровых доказательств.

Ключевые слова: Республика Казахстан, превенция, правоохранительные органы, интернет-мошенничества, детерминанты, Интернет, цифровизация, международное взаимодействие.

Использование цифровых технологий становится повседневной реальностью современного общества, затрагивая как большинство сфер профессиональной деятельности, так и повседневную жизнь жителей большинства государств земного шара, в том числе и Республики Казахстан. Долгое время в сфере правоприменительной деятельности в этом направлении наблюдалось значительное отставание. Данное отставание можно объяснить рядом объективных факторов, в том числе спецификой области, необходимостью четкой формализации деятельности, требованием особых правил ведения учета, фиксации и проверки документов, доказательств и иных фактических материалов.

Исследование факторов, влияющих на совершение преступлений, играет важную роль в современной криминологии. Особенно актуально это для изучения интернет-мошенничества, поскольку знание причин его возникновения является необходимым условием для создания эффективных средств защиты и профилактики этого вида преступлений. В криминологии с причинами преступности связывают ряд социально-психологических факторов. Данные факторы могут выступать, как в качестве непосредственных триггеров преступного поведения, так и в качестве глубинных, долговременных воздействий.

При этом очень важно помнить, что к таким факторам можно отнести несправедливость общества, финансовые трудности, психологическое давление и многие другие элементы, которые могут повлиять на поведение человека [1, с. 268].

Как следствие в повседневной деятельности граждане должны придерживаться так называемой «цифровой компетентности» являющейся составляющим элементом понятия «информационная компетентность», поскольку последнее предполагает, в целом, достаточную совокупность навыков и умений по поводу оперирования информацией (получением, обработкой, использованием, хранением и т.д.). В данном случае не имеет принципиального значения носитель данной информации, однако, следует признать, что в

последние годы информационная компетентность все больше связывается именно с навыками работы с электронными носителями информации.

Большая часть казахстанцев сталкивалась с финансовым мошенничеством – таковы результаты социологического исследования, проведенного Агентством по регулированию и развитию финансового рынка. Согласно социологическому исследованию, 55,8 % респондентов сталкивались с финансовым мошенничеством, из них 34,2% – с телефонным мошенничеством (вишинг), 32,7% – с интернет-мошенничеством (фишинг). 21,6% опрошенных были участниками мошенничества со стороны финансовых пирамид, 11,5% – с платежными картами.

Основной группой риска финансового мошенничества являются люди пенсионного возраста. 50,7% опрошенных старше 63 лет не смогли сразу распознать мошенничество, из них 6,3% частично передавали информацию преступникам и никогда не уточняли данные организации, от которой звонил преступник [2].

Все это говорит о том, что преступления, совершаемые в Интернете, представляют существенную угрозу для современного общества, а их рост за последние несколько десятилетий создает трудности для правоохранительных органов и кибербезопасности. Таким образом, для защиты от таких опасностей, как киберпреступность, крайне важно обладать «цифровой компетентностью».

Важным фактором, который необходимо учитывать, является степень осведомленности населения о различных формах киберпреступности. Граждане должны уметь распознавать подозрительные обстоятельства и понимать, что безответственное поведение в Интернете может привести к раскрытию их личной информации или денежным потерям.

Важнейшее значение имеет также безопасность личных данных, которые люди передают и хранят в Интернете. Для этого необходимо знать, как использовать надежные пароли, двухфакторную аутентификацию и шифрование для предотвращения нежелательного доступа к конфиденциальным данным. Чтобы не попасть в руки хакеров, гражданам также следует знать о процедурах безопасности при использовании электронной почты, социальных сетей и онлайн-платежей [3, с. 53].

О последствиях интернет-преступлений должны знать как отдельные граждане, так и общество в целом. Знания и сотрудничество граждан необходимы для эффективной борьбы с киберпреступностью, поскольку они могут распознавать и пресекать киберугрозы.

Правоохранительная сфера имеет определенную специфику, в отличие от иных сфер информатизации, которая обуславливается неизбежным фактором определенной степени «закрытости» процесса расследования преступлений, необходимой для обеспечения его целей и задач, а также конфиденциальности информации лиц, участвующих в уголовном процессе и самой информации по конкретному уголовному делу. Безусловно, экономический сектор, сектор оказания государственных услуг в гораздо большей степени благоприятны для формирования цифровых платформ в силу их большей открытости, выраженного «сервисного» характера деятельности.

Недооценка комплексного характера любого технологического решения может иметь самые неблагоприятные последствия, поскольку она способна не только усугубить ранее имевшие место проблемы, но и создать дополнительные затруднения. Соответственно, в данном направлении фактически нет мелочей, вплоть до решения самых элементарных организационных вопросов, чтобы обеспечить информационную безопасность.

Важнейшее значение при изучении преступности имеют обстоятельства, создающие условия, при которых вероятность совершения преступления возрастает. К таким обстоятельствам можно отнести неэффективные стратегии предотвращения преступлений, нечеткое законодательство, слабую работу правоохранительных органов и т.д. Важно подчеркнуть, что разработка тактики пресечения данного вида преступлений требует

осознания как факторов, способствующих, так и решающих проблему интернет-мошенничества. И повышение уровня кибербезопасности, и просвещение населения об опасностях Интернета, и совершенствование методов расследования киберпреступлений правоохранительными органами [4, с. 115].

Мошенничество в Интернете зависит от ряда переменных, которые могут либо стать причиной, либо способствовать совершению таких преступлений. Ниже приведем детерминирующие факторы влияющие на рассматриваемую нами проблематику.

1. Потенциальная *анонимность* стала возможной благодаря Интернету, что имеет важные последствия для кибербезопасности и правоохранительной деятельности. Онлайновые пользователи могут скрывать свою личность и физическое местоположение, что затрудняет их идентификацию. В этом и заключается суть такой анонимности.

Способность сети предложить несколько инструментов для сокрытия персональных данных, таких как виртуальные частные сети (VPN), анонимные браузеры и сервисы для шифрования сообщений, является одной из причин распространения феномена онлайн-анонимности. Благодаря техническим средствам пользователи сетей могут избежать идентификации. Кроме того, среда Интернета в целом способствует формированию культуры анонимности.

Пользователи часто имеют возможность общаться в виртуальной среде, используя при этом вымышленные имена или псевдонимы, чтобы скрыть свою подлинную личность. Высокая степень анонимности в Интернете, однако, таит в себе серьезные опасности. Мошенники, сохраняя анонимность, совершают целый ряд преступных действий направленных на материальное обогащение через обман все тех же активных пользователей Интернета. Правоохранительные органы часто сталкиваются с серьезными трудностями при установлении личности мошенников и их местонахождения.

2. Интернет-мошенничество – сложный и своеобразный вид киберпреступлений, требующий от исполнителей *технических познании*. Преступники, занимающиеся этим видом мошенничества, умело используют технологические возможности сети для совершения обманных действий на потенциальных жертв.

Способность разрабатывать, изменять и использовать опасное программное обеспечение (malware) – одна из основных показателей, характеризующих технические способности киберпреступников. Речь идет о создании троянских программ, червей, программ-шпионов и других вредоносных программ, которые могут быть скрытно установлены на устройства жертвы и использованы для доступа к персональным данным, кражи конфиденциальной информации или даже захвата устройства.

3. Глобальная сеть Интернет представляет собой многогранную инфраструктуру, охватывающую всю планету и состоящую из нескольких компьютерных сетей, серверов, ресурсов и оборудования, разбросанных по географическому принципу. Отсутствие централизованного управления или единого субъекта, полностью контролирующего всю сеть, является ключевой характеристикой Интернета. Применение традиционных правовых рамок и концепций регулирования в контексте Интернета сопряжено с большими трудностями. Интернет не может управляться законом в традиционном смысле этого слова, поскольку в нем нет очевидного владельца или управляющей организации.

В результате *законодательный контроль над Интернетом практически отсутствует*, что можно объяснить отличительными особенностями этого всемирного информационного ресурса. Данный факт играет на пользу лица, занимающимся незаконной преступной деятельностью.

4. *Рост информационных технологий* в современном обществе – это удивительное явление, имеющее широкие социокультурные, экономические и политические последствия. Процесс информатизации и глобализации общества невозможен без прогресса. Стремительный технический прогресс и меняющиеся требования общества сделали неизбежным постепенное

внедрение и интеграцию современных IT-решений во многие сферы повседневной жизни человека. В результате этого процесса произошли значительные изменения в сфере коммуникации, образования, занятости, развлечений и многих других аспектов жизни человека.

Информационные технологии принесли обществу огромную пользу, ускорив доступ к информации, повысив эффективность бизнес-процессов, улучшив доступ к здравоохранению и образованию, а также расширив связь со всем миром. Распространение интернет-мошенничества – одна из тех опасностей и проблем, которые принесло с собой развитие информационных технологий.

Интернет-мошенничество – это уголовное преступление, в ходе которого преступники используют возможности Интернета для мошенничества и заработка денег. В связи с тем, что Интернет стал широко доступен и люди проводят в нем все больше времени, этот вид киберпреступлений получил широкое распространение. Злоумышленники используют различные методы, включая фишинг, мошенничество с банковскими картами, социальную инженерию и другие, чтобы обмануть пользователей Интернета и получить доступ к их деньгам. Интернет-мошенничество наносит вред обществу, ослабляя доверие к онлайновому миру и нанося финансовый ущерб частным лицам и организациям [5, с. 102].

5. *Экстерриториальность* – это фактор, определяющий мошенничество, которое является следствием глобализации и развития информационных технологий. Экстерриториальность означает, что преступление совершается, когда оно происходит на территории государства, независимо от того, находится ли преступник там физически или нет.

При совершении преступления в сети Интернет деяние может попадать под уголовный закон сразу нескольких государств. При этом не во всех виртуальное мошенничество может быть криминализировано. В случае если злоумышленник находится на территории одного государства, потерпевший, на территории другого, а сервера на территории третьего, то уголовная ответственность может наступать по законодательству любого государства, участвующего в данных правоотношениях, но при условии международного соглашения.

6. Одним из ключевых компонентов предотвращения интернет-мошенничества является изучение и оценка *недостатков в работе правоохранительных органов*. Недостатки существенно влияют на эффективность выявления и предотвращения преступлений в сфере кибербезопасности. Рассмотрим ключевые элементы и связь между недостатками правоохранительных органов и выявлением интернет-мошенничества в данном контексте.

- недостаток технических знаний и подготовки в области кибербезопасности является одним из основных недостатков правоохранительных органов. Современные киберпреступники используют сложные и передовые методы интернет-мошенничества, что обусловлено стремительным развитием технологий. Раскрытие таких преступлений может быть достаточно сложным из-за неполных знаний и умений правоохранительных органов;
- во многих странах не хватает или недостаточно специализированных подразделений по борьбе с киберпреступностью. Несмотря на то, что подразделения способны проводить расследования в области информационной безопасности, их нехватка может привести к задержкам и ухудшению результатов расследований;
- поскольку мошенники могут действовать на международном уровне, борьба с интернет-мошенничеством требует международного сотрудничества. Отсутствие сотрудничества и обмена информацией между странами может привести к тому, что преступники будут избегать правосудия, а раскрытие мошенничества будет менее эффективным;
- сбор доказательств – очень сложный процесс в эпоху Интернета. Не всегда удается представить цепочку доказательств, связывающих личность злоумышленника с его местонахождением и намерениями. Процесс сбора и изучения цифровых доказательств

имеет ряд недостатков, из-за которых поиск мошеннических преступлений может занять больше времени [6, с. 228].

В связи с тем, что недостатки правоохранительных органов оказывают огромное влияние на выявление интернет-мошенничества, необходимо приложить больше усилий для повышения квалификации сотрудников, создания специализированных подразделений, укрепления международного сотрудничества, совершенствования законодательства в области кибербезопасности. Эффективные меры в этих областях могут значительно активизировать борьбу с интернет-мошенничеством и гарантировать более высокий процент раскрываемости этого вида преступлений.

Таким образом, научное рассмотрение переменных, влияющих на совершение интернет-мошенничества, подчеркивает важность исследования элементов и обстоятельств, приводящих к росту этого вида киберпреступности в современном информационном обществе. Для эффективной борьбы с интернет-мошенничеством и создания превентивных мер необходим анализ этих характеристик. По данным криминологических исследований, на совершение интернет-мошенничества человека может толкнуть множество социальных и психологических факторов. К ним относятся социальная несправедливость, финансовые трудности, а также многочисленные ситуации, которые могут привести к преступной деятельности.

Список использованных источников:

1. Старостенко О.А. Виктимологическая характеристика мошенничества, совершаемого с использованием информационно-телекоммуникационных технологий // Гуманитарные, социально-экономические и общественные науки. – 2020. – № 5. – С. 267–270.
2. Казахстанцы чаще всего сталкиваются с телефонным и интернет-мошенничеством [Электронный ресурс] // https://kapital.kz/finance/113713/kazak hstantsy-chashche-vsego-stalkivayut-sya-s-telefonnym-i-internet-moshennichestvo m.html.
3. Овчинский В. С. Криминология цифрового мира: учебник для магистратуры. – М.: Норма: ИНФРА М, 2018. – 177 с.
4. Рудых А.А. Информационно-технологическое обеспечение криминалистической деятельности по расследованию преступлений в сфере информационных технологий: дис. ... канд. юрид. наук. – Ростов-на-Дону, 2020. – 224 с.
5. Ивлева И.М. Основные детерминирующие факторы мошенничества в сети интернет // Актуальные проблемы публичного права. – 2022. – № 3. – С. 101–104.
6. Остапенко В.Н. Факторы, влияющие на совершение мошенничества с использованием средств сотовой связи, и его расследование // Закон и право. – 2020. – № 12. – С. 227–229.