Pro Index | Journal of Sustainability in Integrated Policy and Practice

Volume: 2 Issue: 1 Year: 2024

http://journals.proindex.uz

Оценка Эффективности Мер Борьбы И Профилактики Интернет-Мошенничеств

Намысов Ерлан Думанович

Самостоятельный соискатель Университета общественной безопасности Республики Узбекистан

Аннотация: В центре внимания научной статьи – изучение и оценка эффективности различных методов и тактик предотвращения и борьбы с интернет-мошенничеством. Необходимость принятия эффективных мер защиты становится все более актуальной в связи с возросшей активностью мошенников в интернет-пространстве и растущей угрозой финансовой безопасности и персональным данным пользователей. Для оценки эффективности этих процедур используются статистические данные, исследования случаев мошенничества, а также мнения ученых-юристов по кибербезопасности. Полученные результаты могут быть использованы в качестве основы для дальнейшего совершенствования системы кибербезопасности и создания более эффективных тактик защиты от интернет-мошенничества с целью обеспечения безопасности и доверия пользователей в онлайновой среде.

Ключевые слова: Республика Казахстан, интернет-мошенничества, оценка, противодействие, меры борьбы, превенция, правоохранительные органы.

С развитием современных информационных технологий и широким распространением доступа в Интернет мошенничество стало одной из самых серьезных опасностей, как для людей, так и для компаний. Преступники совершают различные мошеннические действия на цифровых платформах, среди которых фишинг, кибератаки, кража персональных данных, денежные махинации и другие виды мошенничества. Рост числа пользователей Интернета и расширение их сетевого поведения делают данное исследование актуальным. Объем интернет-мошенничества растет с каждым годом, что является большой проблемой для правоохранительных органов, правоведов и специалистов по кибербезопасности.

Этому способствовал неподготовленный и неэффективный переход к рыночной экономике, а также становление и развитие ее институтов способствовали созданию условий для криминализации части населения и формированию прибыльного «черного» рынка. Что обусловило необходимость формирования отдельных видов мошенничества. Мошенничества отличаются быстротой адаптации к новой деловой практике и изменениям законодательства, маскировкой под гражданско-правовые сделки, использованием фиктивных компаний и нотариусов, применением технических средств, знанием требований законодательства, регулирующего сделки, и другими факторами.

Все это усугубилось в результате отсутствия работы в период карантина, перехода на сетевую торговлю и стремления людей избежать физического контакта. В этом период сформировался настоящий рынок товаров и услуг, который быстро перерос в сетевые торговые отношения. В реальности люди были вынуждены приспосабливаться к нормам

современного общества, а поскольку у них не было соответствующего опыта использования Интернета и знаний о проблемах безопасности и надежности сети, они были склонны становиться жертвами мошенничества. Данный феномен несет социокультурные изменения, ибо образ жизни современного человека во многом зависит от онлайн-ресурсов: от онлайн-покупок до банковских операций.

При этом развитие информационных и коммуникационных технологий продолжает ускоряться, и мошенники активно адаптируются к новым условиям. С развитием технологий возникают новые способы мошенничества, которые требуют актуальных стратегий предотвращения.

В Республике Казахстан на государственном уровне поднимаются вопросы борьбы с интернет-мошенничеством. Президент Республики Казахстан в ходе своих выступлений регулярно поднимает данный вопрос. Так, из послания следует, что «отдельное внимание следует уделить валу интернет- и телефонного мошенничества. Правоохранительным органам нужно усилить информационно-аналитическую работу по выявлению и нейтрализации подобных угроз. Следует также системно повышать правовую и финансовую грамотность граждан» [1].

Изложенное свидетельствует о намерении первых лиц государства и всего аппарата искоренить данную проблему, однако на данный момент, согласно данных статистики, прилагаемых усилий не достаточно. Необходима совместная плодотворная и продуктивная борьба с фактами проявления интернет-мошенничества, а для этого необходимы усилия всего мирового сообщества, так как за частую, преступника и жертву разделяют государственные границы.

За последние несколько лет в Республике Казахстан значительно увеличилось количество случаев интернет-мошенничества, что свидетельствует о нарастании проблемы. В 2020 г. было зарегистрировано 14 220 случаев интернет-мошенничества, что стало первым существенным признаком активизации этого вида преступного поведения. Затем эта тревожная тенденция усугубилась: число случаев интернет-мошенничества выросло до 21 405 в 2021 г. и, несмотря на некоторое снижение, достигло 20 569 в 2022 г. Поскольку уже зафиксировано 9 545 случаев интернет-мошенничества, ситуация не стабилизируется даже в первой половине 2023 г. [2].

Приведенные статистические данные указывают на серьезную проблему, которую необходимо решать как обществу в целом, так и правоохранительным организациям с помощью мер государственного принуждения. Интернет-мошенничество ставит под угрозу не только способность граждан поддерживать свою финансовую безопасность, но и их веру в цифровой мир, который становится все более и более важным для повседневной жизни. Интернет-мошенничество не только наносит жертвам психологический вред, но и подрывает их доверие к безопасности в Интернете. Для того чтобы цифровое общество оставалось стабильным и развивалось, необходимо бороться с этим видом преступлений.

В современную цифровую эпоху существуют различные способы мошенничества, а также методы его пресечения. Мошенничеству в Интернете могут подвергаться не только физические лица, но и предприятия, учреждения, органы местного самоуправления, органы государственной власти, организации различных форм собственности. Распространение мошеннических сообщений по электронной почте или на сайтах, используемых физическими и юридическими лицами, другими субъектами управления и подобными организациями, является одним из часто используемых способов мошеннических действий. При своевременном принятии специальных мер безопасности можно защитить имущество и имущественные права от несанкционированного проникновения «сетевых» злоумышленников.

Следует отметить, что эффективность мер противодействия минимальна, если рассматривать статистику случаев интернет-мошенничества. В ходе исследования мы выяснили, что

диапазон этих измерений достаточно широк. В данном случае имеет место противоречие: несмотря на широкое применение профилактических мер, в некоторых аспектах частота преступлений с использованием интернет-технологий действительно растет. Это можно объяснить особенностями оборудования, используемого для их совершения, так как в этом случае сложно выяснить, как совершается преступление, выявить, задокументировать и собрать доказательства. Учитывая вышесказанное, важно рассмотреть вопрос о том, каким образом службы и ведомства могут взаимодействовать для привлечения правонарушителей к ответственности, поскольку, к сожалению, примеры нераскрытого мошенничества не являются аномалией в современной практике [3, с. 193].

Все большее значение приобретают усилия государственных органов, включая ужесточение наказания для мошенников, совершенствование законодательной базы в области кибербезопасности и расширение международного сотрудничества в борьбе с киберпреступностью. Ключевым моментом в этом вопросе может стать превенция, поэтому очень важно проводить образовательные инициативы, направленные на повышение уровня понимания населением того, как защитить себя от мошенничества в Интернете и как соблюдать основные правила безопасности. Данные меры помогут создать более безопасную среду в Интернете для всех пользователей и успешную кампанию по борьбе с мошенничеством в Интернете.

Проблема интернет-мошенничества выходит далеко за рамки определения этого термина. Мы можем лишь отметить, что интернет-мошенничество и другие мошеннические действия в сети не имеют определения в законодательстве Республики Казахстан, что, на наш взгляд, является проблемой. Как можно бороться с чем-то, если не знаешь, что это такое? Решение этого вопроса позволит ответственным органам эффективно бороться с компьютерным мошенничеством. Однако важно привести п. 4 ч. 2 ст. 190 Уголовного кодекса Республики Казахстан, который предусматривает уголовную ответственность за мошенничество совершенное путем обмана или злоупотребления доверием пользователя информационной системы [4], что в какой-то степени аккумулирует в себе понимание интернет-мошенничества.

Ученые также предприняли попытку восстановить законодательную справедливость. Так, О.В. Левашова и Е.Ю. Сурнова считают, что мошенничество в Интернете следует определять, как особый вид мошеннических действий или махинаций, при которых используется один или несколько компонентов Интернета, таких как чаты, доски объявлений, электронная почта, сайты с различными товарами и другие элементы, позволяющие потенциальному преступнику заманить потенциальную жертву, вызвав у нее интерес к определенной информации [5, с. 115].

Данное определение позволяет понять, что сегодня мошенники становятся все более искусными в использовании технологических и социальных приемов для завоевания доверия клиентов, несмотря на видимость надежности и продуманности. Они умеют копировать сертификаты безопасности, дублировать товарные знаки и даже внешний вид сайтов. Кроме того, мошенники получают доступ к данным клиентов, таким как пароли и реквизиты банковских карт, путем фишинга и использования мошеннических схем. Данным уловкам подвержены даже опытные пользователи. В связи с этим важно понимать, что для определения степени безопасности сайта недостаточно только его внешнего вида. Пользователям следует проявлять осторожность, следить за адресной строкой браузера, проверять сайты и стараться ограничить публикацию своих персональных данных.

Интернет-мошенничество, которое Н.Ю. Дусева определяют как хищение чужого имущества или приобретение права на имущество путем обмана и злоупотребления доверием совершаемое через сеть Интернет, по мнению автора, является подвидом обычного мошенничества [6, с. 191].

Наиболее полное, на наш взгляд, определение дано интернет-мошенничеству А.Е. Струковым, по мнению ученого данное мошенничество является разновидностью

киберпреступности, которое заключается в завладении чужим имуществом или получении права на имущество путем обмана или злоупотребления доверием. Данные киберпреступления совершаются в Интернете с помощью информационно-коммуникационных устройств, систем или сетей, а также других способов доступа в интернет-пространство в пределах их соединений, направленных против компьютерных систем, компьютерных сетей и вычислительных систем, компьютерных данных [7, с. 11].

Проведенный анализ данных определений позволяет прийти к следующим выводам. Определение интернет-мошенничества, данное Н.Ю. Дусевой, подчеркивает суть этого явления как хищения имущества путем обмана и злоупотребления доверием, является простым и понятным. При этом оно может показаться слишком широким, в нем не указаны конкретные способы совершения интернет-мошенничества и не прослеживается связь между ним и преступностью.

С другой стороны, определение интернет-мошенничества, данное А.Е. Струковым, является более полным и актуальным. В нем интернет-мошенничество выделяется как особый вид киберпреступлений и подчеркивается его цифровой аспект. В определении также перечислены средства и методы, используемые для его совершения, в том числе информационно-коммуникационные системы и средства. При этом следует отметить, что данное определение может быть излишне специализированным и не учитывать все виды интернет-мошенничества. Определение может быть дополнено подробными сведениями о различных проявлениях этого явления и о совершенствовании тактики мошенничества с течением времени.

Под интернет-мошенничеством, использующим информационно-коммуникационные устройства, системы, сети и иные способы доступа в интернет-пространство, по нашему мнению, следует понимать вид киберпреступлений, заключающийся в завладении чужим имуществом или приобретении права на имущество путем обмана и злоупотребления доверием. Сюда относятся различные виды мошенничества, совершаемые с использованием интернет-платформ и виртуальных сред с целью незаконного получения выгоды путем использования, направленные на материальное обогащение.

В последнее время резко возросла популярность таких криптовалют, как Bitcoin (BTC), Litecoin (LTC), Namecoin, Zerocoin, Quark, Megacoin, Namecoin, Peercoin, Worldcoin и др. Они представляют собой децентрализованные цифровые активы, которые не управляются правительствами или центральными банками. Однако с ростом интереса к криптовалютам растет и их использование в незаконной деятельности. Так как децентрализованные цифровые валюты, такие как биткойн, позволяющие осуществлять платежи без посредников и обеспечивающие анонимность, естественно, привлекают организованные преступные группировки. Эти группировки используют криптовалюты для проведения транзакций в DarkNet – части скрытой сети Интернет. Основой DarkNet является технология Onion Router (TOR), обеспечивающая высокий уровень анонимности.

Одним из важных аспектов является тот факт, что криптовалюты не регулируются в большинстве стран, в том числе и в Казахстане. Согласно действующему законодательству, криптовалюты не считаются ни электронными деньгами, ни наличными, ни ценными бумагами. В связи с этим требования по регистрации и ведению учета не распространяются на их операции.

Все это подчеркивает сомнительность правового положения криптовалют, а также неформальность и непрозрачность операций с ними. Отсутствие регулирования делает использование криптовалют юридически неоднозначным и может облегчить их незаконное использование. В связи с развитием технологий и компьютеризацией общества мошенничество и другие уголовные преступления все чаще совершаются преступниками, активно использующими новейшие научно-технические разработки. Криптовалюты сегодня являются частью этих технических разработок и используются для сокрытия денежных потоков.

Интернет-мошенничество проявляется в контексте использования криптовалют и децентрализованных финансовых технологий следующими способами:

- злоумышленники могут создавать фальшивые веб-сайты и электронные письма, которые выглядят как подлинные биткоин-биржи и кошельки. Они могут запрашивать персональные данные и пароли пользователей, чтобы получить доступ к их криптовалютным счетам и похитить деньги;
- коммерческие структуры могут использовать первичные предложения монет (ICO) для заработка, гарантируя инвесторам значительную прибыль от вложенных средств. Однако такие проекты часто становятся объектом мошенничества и исчезают после получения финансирования;
- в Интернете широко распространены мошеннические схемы, обещающие инвесторам большие доходы от вложений в биткоины;
- злоумышленники с помощью вредоносного ПО получают доступ к компьютерам и кошелькам пользователей, похищают приватные ключи и крадут криптовалюты;
- нерегулируемые криптовалютные биржи могут удерживать средства пользователей или устанавливать неоднозначные комиссии и курсы обмена;
- такие схемы часто работают как финансовые пирамиды, где первые инвесторы получают деньги от новых участников до тех пор, пока они не разрушатся;
- приложения и кошельки, доступные в онлайн-магазинах, могут быть поддельными и предназначенными для хищения средств пользователей;
- криптовалюты могут использоваться для теневых сделок на «темных рынках», где продаются наркотики, оружие и другие незаконные товары и услуги;
- злоумышленники могут предлагать поддельные товары и услуги, требовать оплату в криптовалюте, а после получения платежа исчезать [8, с. 70].

В результате в настоящее время Интернет является крупнейшей в мире информационно-телекоммуникационной сетью, поскольку он способствует обмену информацией по различным дисциплинам и уровням знаний, а также выполнению договорных обязательств, трудовых и иных задач. Несмотря на то что эта сеть содержит средства защиты от преступных действий злоумышленников, она все еще уязвима и нуждается в действиях соответствующих сторон для предотвращения преступлений.

Для того чтобы не стать жертвой мошенников в Интернете необходимо соблюдать ряд мер безопасности и предосторожности, среди которых следует выделить:

1. Аутентификация и пароли:

- ✓ использование сильных и уникальных паролей;
- ✓ включение двухфакторной аутентификации (2FA).

2. Сетевая и программная безопасность:

- ✓ регулярное обновление операционных систем и программного обеспечения;
- ✓ использование надежных антивирусных программ;
- ✓ защита домашней сети паролем и настройка маршрутизатора;
- ✓ избегание открытых Wi-Fi сетей для чувствительных операций;
- ✓ проверка безопасности сайта перед проведением онлайн-платежей.

3. Осознанное поведение и финансовая бдительность:

- ✓ осторожность при открытии электронных писем от незнакомых отправителей;

- ✓ проверка адресов электронной почты и доменов отправителей;
- ✓ осторожное размещение информации в социальных сетях;
- ✓ ограничение доступа к личным данным;
- ✓ покупка у надежных онлайн-магазинов;
- ✓ регулярная проверка финансовых отчетов и банковских выписок;
- ✓ бдительность и подозрительность по отношению к предложениям и выигрышам;
- ✓ обучение современным методам мошенничества и немедленное сообщение о мошенничестве органам правопорядка.

Эффективность стратегий по пресечению и предотвращению интернет-мошенничествам была оценена в контексте данной научной статьи. Исследование показало, что ряд переменных, таких как целесообразность их внедрения, осведомленность пользователей и динамика изменений в среде информационных угроз, влияют на то, насколько эффективны меры безопасности в Интернете. Запрещая злоумышленникам доступ к личной информации и финансовым ресурсам пользователей, меры аутентификации, сетевой и программной безопасности оказывают существенное влияние на снижение риска интернет-мошенничества.

Также была подчеркнута важность грамотного поведения и финансовой осведомленности. Для снижения успешности интернет-мошенничества и защиты интересов пользователей очень важны обратная связь с пользователями, просвещение и более глубокое понимание современных стратегий мошенничества. Несмотря на значительные успехи в борьбе с Интернет-мошенничеством, преступники постоянно совершенствуют свои стратегии. Для эффективной борьбы с интернет-мошенничеством государственные органы бизнес и общество в целом должны работать сообща, постоянно отслеживать, адаптировать и совершенствовать меры безопасности.

Список использованных источников:

1. Справедливое государство. Единая нация. Благополучное общество [Электронный ресурс]: Послание Главы государства Касым-Жомарта Токаева народу Казахстана от 1 сентября 2022 г. // https://adilet.zan.kz/rus/docs/ K22002022_2
2. Основные показатели органов уголовного преследования: аналитический обзор [Электронный ресурс] // Официальный сайт Комитета по правовой статистике и специальным учетам Генеральной прокуратуры Республики Казахстан. Информационный сервис. URL: https://www.qamqor. gov.kz/
3. Березняк В.А. Предотвращение мошенничества в интернете // Научный вестник Днепропетровского государственного университета внутренних дел. – 2023. – № 1. – С. 190–196.
4. Уголовный кодекс Республики Казахстан от 3 июля 2014 г. № 226-V // Казахстанская правда. – 2014. – 9 июля.
5. Левашова О.В., Сурнова Е.Ю. Понятие мошенничества с использованием мобильных средств связи и сети Интернет // Государственная служба и кадры. – 2021. – № 2. – С. 114–117.
6. Дусева Н.Ю. Интернет-мошенничества: понятие и история развития // Научные исследования высшей школы по приоритетным направлениям науки и техники: сборник статей Международной научно-практической конференции. – В 2 ч. Ч.2/ – Уфа: АЭТЕРНА, 2018. – С. 191–192.
7. Струков А.Е. Понятие и способы мошенничества // Вестник магистратуры. – 2022. – № 1-2 (124). – С. 10–12.
8. Екимцев С.В. Понятие и сущность мошенничества // Современное общество и право. – 2023. – № 1 (62). – С. 68–73.