ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

«Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ» КЕАҚ

Студенттер мен жас ғалымдардың
«ǴYLYM JÁNE BILIM - 2023»
XVIII Халықаралық ғылыми конференциясының
БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ
XVIII Международной научной конференции
студентов и молодых ученых
«ǴYLYM JÁNE BILIM - 2023»

PROCEEDINGS
of the XVIII International Scientific Conference
for students and young scholars
«ǴYLYM JÁNE BILIM - 2023»

2023
Астана

УДК 001+37
ББК 72+74
G99

«ǴYLYM JÁNE BILIM – 2023» студенттер мен жас ғалымдардың XVIII Халықаралық ғылыми конференциясы = XVIII Международная научная конференция студентов и молодых ученых «ǴYLYM JÁNE BILIM – 2023» = The XVIII International Scientific Conference for students and young scholars «ǴYLYM JÁNE BILIM – 2023». – Астана: – 6865 б. - қазақша, орысша, ағылшынша.

ISBN 978-601-337-871-8

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.

В сборник вошли доклады студентов, магистрантов, докторантов и молодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 001+37
ББК 72+74

ISBN 978-601-337-871-8

ПРОБЛЕМЫ ПРИМЕНЕНИЯ СПЕЦИАЛЬНЫХ ЗНАНИЙ ПРИ РАССЛЕДОВАНИИ МОШЕННИЧЕСКИХ ДЕЙСТВИЙ В СЕТИ ИНТЕРНЕТ

Шуханов Рустем Сарсенович
rustem.shuhanov@mail.ru
магистрант 1 курса, кафедры уголовно-правовых дисциплин
ЕНУ им. Л.Н.Гумилева, Астана, Казахстан
Научный руководитель – Е.К. Даурембеков

Изучение мошеннических действий в сети Интернет является актуальным в связи с увеличением частоты таких действий. По мере того, как все больше финансовых транзакций и личной информации передаются в Интернете, риск интернет-мошенничества продолжает расти [1]. Расследование и предотвращение мошеннических действий в Интернете имеет важное значение для защиты отдельных лиц и организаций от финансовых потерь и другого ущерба. Однако изучение мошеннических действий в сети Интернет связано с рядом проблем, так как технологии развиваются быстрыми темпами, а изучение и применение специальных знаний в этой области развиваются медленно. Методы, используемые мошенниками, постоянно развиваются, и следователи и эксперты должны быть в курсе новейших технологий и методов, чтобы эффективно расследовать и предотвращать мошенничество. Кроме того интернет-мошенничество часто осуществляется за границей, что затрудняет расследование и судебное преследование. Следователи должны ориентироваться в международных законах, правилах и процедурах, чтобы эффективно расследовать интернет-мошенничество и преследовать его в судебном порядке. Последние дни финансовые транзакции в Интернете могут быть сложными и включать несколько юрисдикций, что затрудняет отслеживание и выявление мошеннических действий. Следователи должны хорошо разбираться в финансовых системах и правилах, чтобы эффективно расследовать финансовое мошенничество. В целом, изучение мошеннических действий в Интернете необходимо для понимания методов, используемых мошенниками, и разработки эффективных стратегий предотвращения и расследования интернет-мошенничества.

Поскольку тема широка и охватывает ряд информационных, финансовых и процессуальных вопросов судебной и следственной деятельности, авторы в первую очередь определяют следующие цели и задачи:

- классифицировать основные проблемы в процессе использования специальных знаний для изучения интернет-мошенничества;
- выявить наиболее распространенные виды интернет-мошенничества и дать научные рекомендации по расследованию интернет-мошенничества.

В настоящий время цифровая неграмотность может способствовать распространению дезинформации, онлайн-мошенничества и киберзапугивания, поскольку люди могут быть не способны критически оценивать информацию, с которой они сталкиваются в Интернете, или защищать себя от онлайн-угроз. Цифровая неграмотность относится к отсутствию знаний и навыков, необходимых для эффективного использования технологий и цифровых инструментов, таких как компьютеры, смартфоны и Интернет. Это также может включать в себя непонимание того, как ориентироваться на онлайн-платформах, общаться с помощью цифровых средств и защищать свою личную информацию в Интернете. Проблема цифровой неграмотности может иметь значительные негативные последствия для отдельных людей и общества в целом. Те, кто неграмотен в цифровой сфере, могут иметь ограниченный доступ к информации, возможностям трудоустройства и образовательным ресурсам. Они также могут оказаться в невыгодном положении, когда речь заходит о гражданском и политическом участии, поскольку многие аспекты современной жизни требуют определенного уровня цифровой компетентности. Согласно цифровому We Are Social за 2021 год, по состоянию на январь 2021 года 77% населения Казахстана являются

пользователями Интернета [2]. 2022 В среднем по РК показатель превысил 85% [3]. Однако цифровая грамотность по-прежнему остается проблемой для некоторых слоев населения. Свыше 20 тысяч интернет-мошенничеств произошло в 2022 году в Казахстане [4]. По мошенничеству зафиксирована динамика роста показателя за февраль 2022 года и февраль 2023 года на 14,4% (ст. 190 УК) (с 6380 до 7300) [5].

Правительство Казахстана реализовало несколько программ по борьбе с цифровой неграмотностью и содействию цифровизации в стране. Программа «Цифровой Казахстан» - эта программа была запущена в 2017 году с целью содействия цифровизации и инновациям в различных секторах экономики, таких как образование, здравоохранение и государственные услуги. Программа направлена на повышение цифровой грамотности населения и на то, чтобы сделать цифровые технологии более доступными [6]. Программа «Цифровой шелковый путь» - эта программа была запущена в 2019 году с целью содействия цифровому подключению и экономическому сотрудничеству между Казахстаном и другими странами региона [7]. Программа направлена на содействие развитию цифровой инфраструктуры, услуг и навыков в Казахстане и повышение цифровой конкурентоспособности страны.Программа «Электронное правительство 3.0» - данная программа была запущена в 2019 году с целью дальнейшего развития электронных государственных услуг в Казахстане [8]. Эти программы демонстрируют приверженность правительства Казахстана продвижению цифровизации и повышению цифровой грамотности населения. Они направлены на решение проблем, связанных с цифровой неграмотностью, и обеспечение того, чтобы Казахстан оставался конкурентоспособным в мировой экономике.

В Казахстане интернет-мошенничество регулируется несколькими законодательными актами, как Уголовный кодекс Республики Казахстан, Закон «О персональных данных и их защите» и Закон «Об информатизации». Уголовный кодекс Республики Казахстан предусматривает уголовную ответственность за различные формы интернет-мошенничества, включая компьютерный взлом, кражу личных данных, фишинг и финансовое мошенничество в Интернете. Именно Статья 188. Взлом, Статья 189. Несанкционированный доступ к компьютерной информации, Статья 190. Производство, использование и распространение вредоносных компьютерных программ, Статья 190-1. Распространение информации, использование которой наносит вред другим лицам, Статья 197. Кража личных данных и Статья 308. Преступления, связанные с интернет-мошенничеством, караются штрафами, тюремным заключением или и тем и другим, в зависимости от тяжести правонарушения.

Закон «О персональных данных и их защите» закон регулирует сбор, хранение и использование персональных данных в Казахстане. Подделка или фальсификация электронных документов. Закон устанавливает правила защиты данных и налагает наказания за несанкционированный доступ к персональным данным, включая штрафы и тюремное заключение. Закон «О регулировании торговой деятельности» регулирует электронные транзакции и коммерцию в Казахстане. Он устанавливает требования к электронным подписям, онлайн-контрактам и другим электронным документам, а также налагает штрафы за мошеннические онлайн-транзакции. Именно Статья 15. Несанкционированный доступ к персональным данным и Статья 18. Ответственность за нарушение законодательства о защите персональных данных [9]. В этих статьях и параграфах излагаются конкретные правонарушения, связанные с интернет-мошенничеством, и наказания за их совершение. Важно отметить, что этот список не является исчерпывающим и что другие законы и нормативные акты также могут иметь отношение к борьбе с интернет-мошенничеством в Казахстане.

Закон «Об информатизации» регулирует использование информационных технологий в Казахстане и устанавливает правила информационной безопасности и защиты данных. Закон регулирует общественные отношения в сфере информатизации, возникающие на территории Республики Казахстан между государственными органами, физическими и юридическими лицами при создании, развитии и эксплуатации объектов информатизации, а

также при государственной поддержке развития отрасли информационно-коммуникационных технологий [10]. Эти законы обеспечивают правовую основу для борьбы с интернет-мошенничеством в Казахстане и для защиты прав физических и юридических лиц, использующих цифровые технологии. Они демонстрируют приверженность правительства созданию безопасной и заслуживающей доверия цифровой среды в стране.

Интернет-мошенничество - это глобальная проблема, которая затрагивает частных лиц, предприятия и правительства по всему миру. Для борьбы с этим преступлением страны по всему миру внедрили различные меры и инициативы по предотвращению, выявлению и судебному преследованию интернет-мошенничества [11]. Одной из таких международных инициатив является Глобальная программа по борьбе с киберпреступностью (GPC), запущенная Управлением Организации Объединенных Наций по наркотикам и преступности (УНП ООН) в 2013 году. GPC нацелен на укрепление потенциала государств-членов по расследованию киберпреступлений и судебному преследованию за них путем предоставления технической помощи, обучения и поддержки. GPC также содействует международному сотрудничеству и обмену информацией между государствами-членами в целях борьбы с киберпреступностью.

Другой инициативой является Конвенция Совета Европы о киберпреступности, также известная как Будапештская конвенция, которая была принята в 2001 году. Конвенция является первым международным договором о киберпреступности и направлена на гармонизацию национальных законов, улучшение международного сотрудничества и создание основы для международной помощи в расследовании и судебном преследовании киберпреступлений. По состоянию на 2021 год Конвенцию ратифицировали 66 стран [12]. В Европейском союзе (ЕС) в 2013 году был создан Европейский центр по борьбе с киберпреступностью (EC3) в качестве центрального центра сотрудничества правоохранительных органов в борьбе с киберпреступностью. EC3 сотрудничает с государствами-членами в целях поддержки расследований, обеспечения подготовки кадров и экспертных знаний, а также содействия обмену информацией между правоохранительными органами [13].

В Азии Ассоциация государств Юго-Восточной Азии (АСЕАН) учредила Министерское совещание АСЕАН по кибербезопасности (AMMCS) для координации усилий государств-членов по борьбе с киберпреступностью, включая интернет-мошенничество. AMMCS способствует обмену информацией, наращиванию потенциала и сотрудничеству между государствами-членами в целях укрепления кибербезопасности в регионе [14]. В целом, международное сотрудничество и координация между правоохранительными органами имеют решающее значение для борьбы с интернет-мошенничеством и другими формами киберпреступности. Обмениваясь информацией и опытом и работая сообща, страны могут лучше защищать своих граждан и предприятия от угрозы киберпреступности.

В Казахстане есть несколько государственных органов и агентств, ответственных за борьбу с интернет-мошенничеством и другими формами киберпреступности. Одним из ключевых учреждений в этом отношении является Министерство цифрового развития, инноваций и аэрокосмической промышленности. Министерство осуществляет надзор за разработкой и внедрением политик и правил, касающихся кибербезопасности, включая предотвращение и выявление интернет-мошенничества. Министерство также работает с другими государственными учреждениями и заинтересованными сторонами из частного сектора над разработкой национальных стратегий кибербезопасности и борьбы с киберпреступностью. Еще одним важным учреждением является Комитет национальной безопасности (КНБ) Казахстана, который отвечает за поддержание национальной безопасности и борьбу с угрозами информационным и коммуникационным системам страны. КНБ работает над выявлением и предотвращением кибератак и киберпреступлений, включая интернет-мошенничество. Он также сотрудничает с международными партнерами для повышения кибербезопасности и обмена информацией. Кроме того, Комитет информации отвечает за регулирование и надзор за телекоммуникационной отраслью страны. Комитет

информации работает над обеспечением безопасности и надежности телекоммуникационной инфраструктуры страны, включая защиту от кибератак и других форм киберпреступности.

При правительстве Казахстана в 2017 году была выпущена концепция «Киберщит Казахстана». Это концепция всеобъемлющей инициативы в области кибербезопасности, направленная на укрепление системы кибербезопасности страны, защиту критической инфраструктуры и содействие безопасному использованию Интернета отдельными лицами, предприятиями и правительствами. В стратегии изложены цели и приоритеты страны в области кибербезопасности, а также рекомендации по разработке и внедрению политик и правил, связанных с кибербезопасностью. Инициатива включает создание Центра управления кибербезопасностью, отвечающего за мониторинг и анализ киберугроз, координацию реагирования на инциденты и информирование заинтересованных сторон о ситуации. Он также служит центральным узлом для обмена информацией об угрозах с внутренними и международными партнерами. Инициатива также включает в себя различные программы обучения и повышения осведомленности для частных лиц, предприятий и государственных учреждений, направленные на продвижение передового опыта в области кибербезопасности и снижение киберрисков [15].

В процессе использования специальных знаний для изучения интернет-мошенничества возникает несколько основных проблем. Мы можем классифицировать следующим образом:

- ограниченный доступ к данным;
- отсутствие сотрудничества;
- быстро меняющаяся тактика;
- правовые и этические вопросы;
- процессуальные порядки;

Интернет-мошенничество является глобальной проблемой, и для эффективного изучения этого явления необходимо сотрудничество между правоохранительными органами, исследователями и другими заинтересованными сторонами. Однако многие страны неохотно делятся информацией или сотрудничают в расследованиях, что затрудняет полное понимание проблемы. Еще одной проблемой при изучении интернет-мошенничества является ограниченный доступ к данным. Многие интернет-мошенники действуют анонимно и используют шифрование и другие методы, чтобы скрыть свою личность и действия, что затрудняет доступ исследователей к необходимым данным для изучения их тактики и моделей [16, p. 202]. Интернет-мошенники постоянно разрабатывают новые тактики, чтобы избежать обнаружения и опережать правоохранительные органы. Это означает, что специализированные знания должны постоянно обновляться, чтобы идти в ногу с последними тенденциями и тактикой [17].

Изучение интернет-мошенничества поднимает ряд правовых и этических вопросов, включая вопросы конфиденциальности, защиты данных и использования личной информации. Исследователи должны тщательно разбираться в этих вопросах, чтобы их исследования были законными и этичными. Правовые проблемы могут затруднить получение доказательств и судебное преследование виновных в интернет-мошенничестве, особенно если они находятся в другой юрисдикции. Однако понимание правовой базы, связанной с интернет-мошенничеством, может помочь определить области, в которых можно укрепить законы и правила, чтобы обеспечить лучшую защиту жертв.

Проведение расследования интернет-мошенничества – сложный и многогранный процесс, требующий специальных знаний, навыков и инструментов. Поскольку все расследование должно быть организовано на правовой основе, следователи и эксперты должны соблюдать ряд процессуальных требований. Наиболее распространенным применением специальных знаний при расследовании интернет-мошенничества является организация судебных экспертиз. Одним из наиболее важных вопросов при организации судебной экспертизы по интернет-мошенничеству является сохранение доказательств. Доказательства могут быть легко уничтожены или изменены в цифровом мире, и

следователи должны принять меры для обеспечения того, чтобы данные были сохранены с точки зрения криминалистики. Это включает в себя создание копии исходных данных и сохранение цепочки поставок. Законом Республики Казахстан установлено, что «Судебный эксперт не вправе: самостоятельно собирать материалы для исследования; проводить исследования, которые могут повлечь полное или частичное уничтожение объектов либо изменение их внешнего вида или основных свойств, если на это не было специального разрешения органа (лица), назначившего судебную экспертизу» (сатья 23, пунк 2,3) [18]. В процессе доказывания эксперты имеют мало возможностей с точки зрения закона.

Поэтому следователи должны иметь возможность собирать данные таким образом, чтобы не изменять и не уничтожать исходные доказательства. Это включает в себя использование специализированных инструментов и методов для создания точной копии данных на компьютере подозреваемого или другом цифровом устройстве.

Все вышеперечисленные проблемы, которые связаны с расследованием киберпреступлений, являются наиболее распространенными в мире. Однако остаются вопросы, которые необходимо более глубоко осмыслить и сопоставить с основной проблемой. Эти вопросы касаются типов интернет-мошенничества и их наиболее распространенных тактик. Интернет-мошенничество может происходить в различных областях, и сложно выделить какую-то одну область как наиболее распространенную для интернет-мошенничества. В последнее время широко распространены мошенничество с фишингом, мошенничество с инвестициями, мошенничество с покупками в интернете и мошенничество с технической поддержкой. Кроме того, кража личных данных также является более распространенной формой онлайн-мошенничества [19].

Мошенничество с фишингом — это мошеннические попытки получить конфиденциальную информацию, такую как учетные данные для входа в систему и данные кредитной карты, выдавая себя за заслуживающую доверия организацию по электронной почте, текстовым сообщениям или в социальных сетях. Мошенничество с покупками в Интернете включает поддельные веб-сайты или онлайн-рынки, которые продают поддельные или несуществующие товары или берут оплату за товары, которые никогда не были доставлены. Мошенничество с инвестициями часто нацелено на людей, стремящихся получить высокую прибыль с минимальным риском или вообще без риска, предлагая возможности мошеннических инвестиций в поддельные предприятия или схемы Понци. Мошенники, выдающие себя за сотрудников службы технической поддержки авторитетных компаний, убеждают жертв предоставить доступ к своим компьютерам или данным кредитной карты для устранения фиктивных проблем. Кража личных данных включает несанкционированное использование чьей-либо личной информации для доступа к финансовым счетам, открытия новых кредитных счетов или получения кредитов или услуг.

В заключении, в ходе исследования были выявлены и классифицированы основные проблемы интернет-мошенничества. К ним были отнесены следующие проблемы. - ограниченный доступ к данным;

- отсутствие сотрудничества;
- быстро меняющаяся тактика;
- правовые и этические вопросы;
- процессуальные порядки.

Также в ходе исследования были выделены наиболее распространенные виды интернет-мошенничества. Мы включаем следующие виды:

- мошенничество с фишингом;
- мошенничество с инвестициями;
- мошенничество с покупками в интернете;
- мошенничество с технической поддержкой;
- кража личных данных.

В связи с этим предлагаем следующие предложения.

- Прежде всего, глубокий анализ международных исследований, связанных с быстро меняющейся тактикой. Ведь эти анализы позволяют нам наблюдать за меняющимися и новыми способами международного сотрудничества и общения в сфере интернет-мошенничества;

- проведение исследований для внедрения эффективного способа анализа правовых и этических проблем в странах мира. В свою очередь, это откроет путь для развития правовой базы выявления интернет-мошенничества в нашей стране.

- систематизировать исследования процессуального порядка и проанализировать основные вопросы производства судебных экспертиз;

- подготовка методологии междисциплинарного исследования в связи с участившимся в последнее время явлением интернет-мошенничества в различных сферах (финансы, личная безопасность, получение психологического доверия).

Список использованных источников:

1. LLP P.O. Интернет-мошенничества вызвали широкий общественный резонанс [Electronic resource] // Profit.kz — ИТ в Казахстане. URL: https://profit.kz/news/64128/Internet-moshennichestva-vizvali-shirokij-obschestvennij-rezonans/ (accessed: 04.04.2023).
2. 93digital. Digital 2021 - Global Overview [Electronic resource] // We Are Social UK. 2021. URL: https://wearesocial.com/uk/blog/2021/01/digital-2021-uk/ (accessed: 11.04.2023).
3. Уровень цифровой грамотности населения повысился в Казахстане - Новости Казахстана и мира на сегодня [Electronic resource]. 2022. URL: https://24.kz/ru/news/social/item/548763-uroven-tsifrovoj-gramotnosti-naseleniya-povysilsya-v-kazakhstane (accessed: 11.04.2023).
4. INFORM.KZ. Свыше 20 тысяч интернет-мошенничеств произошло в прошлом году в Казахстане [Electronic resource] // Казинформ. 2023. URL: https://www.inform.kz/ru/article/4026710 (accessed: 11.04.2023).
5. Правовая статистика [Electronic resource]. URL: https://qamqor.gov.kz/crimestat/indicators/criminal (accessed: 11.04.2023).
6. Об утверждении Государственной программы “Цифровой Казахстан” - ИПС “Әділет” [Electronic resource]. URL: https://adilet.zan.kz/rus/docs/P1700000827 (accessed: 11.04.2023).
7. Что такое цифровой шелковый путь ⊳ zakon.kz [Electronic resource]. URL: https://www.zakon.kz/4969015-chto-takoe-tsifrovoy-shelkovyy-put.html (accessed: 11.04.2023).
8. Корея намерена разработать «Электронное правительство 3.0» [Electronic resource] // Информационная система ПАРАГРАФ. URL: https://online.zakon.kz/Document/?doc_id=31610793 (accessed: 11.04.2023).
9. О персональных данных и их защите - ИПС “Әділет” [Electronic resource]. URL: https://adilet.zan.kz/rus/docs/Z1300000094 (accessed: 11.04.2023).
10. Об информатизации - ИПС “Әділет” [Electronic resource]. URL: https://adilet.zan.kz/rus/docs/Z1500000418 (accessed: 11.04.2023).
11. Global Programme on Cybercrime [Electronic resource] // United Nations : Office on Drugs and Crime. URL: //www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html (accessed: 11.04.2023).
12. Budapest Convention - Cybercrime [Electronic resource]. URL: https://www.coe.int/en/web/cybercrime/the-budapest-convention (accessed: 11.04.2023).
13. European Cybercrime Centre - EC3 [Electronic resource] // Europol. URL: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3 (accessed: 11.04.2023).
14. ASEAN-EU Statement on Cybersecurity Cooperation [Electronic resource] // ASEAN Main Portal. 2019. URL: https://asean.org/asean-eu-statement-on-cybersecurity-cooperation/ (accessed: 11.04.2023).

15. Об утверждении Концепции кибербезопасности (“Киберщит Казахстана”) - ИПС “Әділет” [Electronic resource]. URL: https://adilet.zan.kz/rus/docs/P1700000407 (accessed: 11.04.2023).

16. Атаманов Р.С. Некоторые вопросы расследования мошенничества в сети Интернет // Актуальные Проблемы Российского Права. Федеральное государственное бюджетное образовательное учреждение высшего …, 2010. № 4. P. 201–205.

17. tengrinews.kz. Новые схемы интернет-мошенников: как защитить себя, рассказали полицейские [Electronic resource] // Главные новости Казахстана - Tengrinews.kz. 2023. URL: https://tengrinews.kz/kazakhstan_news/novyie-shemyi-internet-moshennikov-zaschitit-sebya-493259/ (accessed: 04.04.2023).

18. О судебно-экспертной деятельности - ИПС “Әділет” [Electronic resource]. URL: https://adilet.zan.kz/rus/docs/Z1700000044 (accessed: 05.04.2023).

19. Белицкий В.Ю. Распространенные виды мошенничеств в сети интернет // Актуальные Проблемы Современности. Частное учреждение" Академия" Болашак", 2020. № 2. P. 31–36.

Подсекция 10.4 Уголовная политика и уголовное законодательство: современные вызовы и поиск эффективных решений

УДК 343.2/.7