DOI 10.54596/2958-0048-2024-2-132-139
УДК 341.234
МРНТИ 10.81.35

ИНТЕРНЕТ-МОШЕННИЧЕСТВО И ЕГО ВЛИЯНИЕ НА ЭКОНОМИЧЕСКУЮ БЕЗОПАСНОСТЬ В СОВРЕМЕННОМ МИРЕ

Умурзаков И.Г.[1], Протасова О.В.[1], Салтурина А.М.[2]
[1]НАО «Северо-Казахстанский университет имени Манаша Козыбаева»*
Петропавловск, Казахстан
[2]ТОО «Казахстанский центр коммерциализации технологии»
Астана, Казахстан
[*]Автор для корреспонденции: ibrayumurzakov2003@mail.ru

Аннотация

В современном мире экономическая безопасность становится ключевым аспектом обеспечения стабильности и развития. В данной статье рассматривается проблема мошенничества как одной из основных угроз экономической безопасности. Авторы выделяют различные виды мошенничества, обсуждают их характеристики и механизмы действия. Особое внимание уделяется современным формам мошенничества, таким как интернет-мошенничество, и их распространению. Статья также предлагает ряд мер по борьбе с мошенничеством, включая образовательные программы для населения нашей страны. Обсуждается необходимость государственного вмешательства и разработки эффективных стратегий для защиты экономических интересов граждан и обеспечения экономической безопасности в целом.

Ключевые слова: экономическая безопасность, мошенничество, угрозы, виды мошенничества, электронное мошенничество, защита экономических интересов.

ИНТЕРНЕТТЕГІ АЛАЯҚТЫҚ ЖӘНЕ ОНЫҢ ҚАЗІРГІ ӘЛЕМДЕГІ ЭКОНОМИКАЛЫҚ ҚАУІПСІЗДІККЕ ӘСЕРІ

Умурзаков И.Г.[1], Протасова О.В.[1], Салтурина А.М.[2]
[1]«Манаш Қозыбаев атындағы Солтүстік Қазақстан университеті» КеАҚ*
Петропавл, Қазақстан
[2]«Қазақстандық технологияларды коммерцияландыру орталығы» ЖШС
Астана, Қазақстан
[*]Хат-хабар үшін автор: ibrayumurzakov2003@mail.ru

Аңдатпа

Қазіргі әлемде экономикалық қауіпсіздік тұрақтылық пен дамуды қамтамасыз етудің негізгі аспектісіне айналуда. Бұл мақалада алаяқтық мәселесі экономикалық қауіпсіздіктің негізгі қауіптерінің бірі ретінде қарастырылады. Авторлар алаяқтықтың әртүрлі түрлерін бөліп көрсетеді, олардың сипаттамалары мен әрекет ету механизмдерін талқылайды. Интернеттегі алаяқтық сияқты алаяқтықтың заманауи түрлеріне және олардың таралуына ерекше назар аударылады. Сондай-ақ, мақалада алаяқтыққа қарсы бірқатар шаралар, соның ішінде біздің ел халқына арналған білім беру бағдарламалары ұсынылған. Мемлекеттің араласуы және азаматтардың экономикалық мүдделерін қорғау және жалпы экономикалық қауіпсіздікті қамтамасыз ету үшін тиімді стратегияларды әзірлеу қажеттілігі талқыланады.

Түйін сөздер: экономикалық қауіпсіздік, алаяқтық, қауіп-қатер, алаяқтық түрлері, электрондық алаяқтық, экономикалық мүдделерді қорғау.

INTERNET FRAUD AND ITS IMPACT ON ECONOMIC SECURITY IN THE MODERN WORLD

Umurzakov I.G.[1], Protasova O.V.[1*], Salturina A.M.[2]
[1]«Manash Kozybayev North Kazakhstan University» NPLC*
Petropavlovsk, Kazakhstan
[2]Kazakhstan Technology Commercialization Center LLP, Astana, Kazakhstan
[*]Corresponding author: ibrayumurzakov2003@mail.ru

Abstract

In the modern world, economic security is becoming a key aspect of ensuring stability and development. This article examines the problem of fraud as one of the main threats to economic security. The authors identify various types of fraud, discuss their characteristics and mechanisms of action. Special attention is paid to modern forms of fraud, such as online fraud, and their spread. The article also suggests a number of measures to combat fraud, including educational programs for the population of our country. The need for government intervention and the development of effective strategies to protect the economic interests of citizens and ensure economic security in general is discussed.

Key words: economic security, fraud, threats, types of fraud, electronic fraud, protection of economic interests.

Введение

Экономическая безопасность становится проблемой первостепенной важности в современном мире. Она определяется как состояние, обеспечивающее динамичное развитие экономической системы и решение социальных проблем и задач [2]. Экономическая безопасность подвергается различным угрозам, которые мешают эффективному управлению и развитию экономики. Угрозы безопасности включают:

1) внешние и внутренние (в зависимости от местонахождения источника опасности);

2) потенциальные (возникновение опасности) и актуальные (возникновение опасности при недостаточности одного или нескольких факторов для причинения вреда);

3) природные, техногенные природные, социальные и иные (в зависимости от характера угрозы).

Мы согласны с Н.Н. Корзаевой в том, что мошенничество является одной из существующих угроз, подрывающие экономическую стабильность, нансоящие вред финансовой системе и вызывают социальные распрения в современном обществе [2].

Также мы можем сказать, что под экономическим мошенничеством понимается действие, направленное на попытку дестабилизации финансовой безопасности организации, независимо от ее правовой формы. Статья 190 Уголовного кодекса Республики Казахстан гласит, что основными признаками мошенничества являются действия, совершенные путем обмана (обычно преступное лицо втирается в доверие человека для присвоения имущества). К мошенничеству относятся действия по несанкционированному приобретению или хищение чужого имущества у физических и юридических лиц. А также в сфере государственных закупок, мошенничество, совершенное группой лиц по предварительному сговору, лицами, пользующимися своим служебным положением, или пользователями информационных систем путем обмана или злоупотребления доверием. Кроме того, мошенничество может совершаться лицом, уполномоченным исполнять государственные обязанности (если речь идет о злоупотреблении полномочиями).

Материалы и методы

Информация о том, как осуществляется деятельность в области анализа и противодействия мошенничеству и других его видов в Казахстане изучена на основе литературных источников, научных статей и интернет-ресурсов. Объектом исследования являются мошенничество и различные его виды. Был использован метод систематического литературного обозрения. С помощью данного метода был осуществлен поиск и отбор литературы на предмет исследования. Был проведён анализ того, какие виды мошенничества существуют в нашей стране и в зарубежных странах (например, Российская Федерация), изучена официальная статистика, предоставленная Министерством внутренних дел РК, как противостоять мошенничеству – как одной из проблем нашей страны. Синтез изученных данных позволил получить объективную картину как о состоянии вопроса изучения экономического мошенничества и комплекса применяемых мер, по его противодействию.

Результаты и их обсуждение

Рассмотрим наиболее распространенные виды мошенничества. Так, мы можем выделить несколько наиболее распространенных видов мошенничества:

1) **Электронное мошенничество.** Благодаря развитию информационных технологий мошенники все чаще используют электронные средства для совершения преступлений. Наиболее популярными являются:

1) Фишинговые атаки. Злоумышленники рассылают электронные письма или СМС-сообщения, имитирующие уведомления от банков, интернет-магазинов или других известных организаций. В таких сообщениях содержится ссылка на поддельный сайт, где жертва вводит свои персональные данные и данные банковской карты [1].

2) Сбои при платежах. Мошенники создают поддельные сайты, похожие на сайты известных интернет-магазинов, и предлагают совершить покупку по заниженной цене. После оплаты товара жертва получает уведомление о том, что произошла ошибка при платеже и необходимо произвести его повторно. В результате деньги списываются с карты жертвы дважды [1].

3) «Угон» аккаунтов в социальных сетях. Злоумышленники взламывают аккаунты пользователей в социальных сетях и начинают рассылать сообщения от их имени, прося о финансовой помощи. Жертвы, получив такое сообщение от знакомого человека, зачастую переводят деньги на указанный счет.

2) Мошенничество с банковскими картами. С развитием безналичных расчетов возросло количество мошеннических операций с банковскими картами. Злоумышленники используют (в большинстве случаев) следующие схемы:

1) Скимминг – мошенники устанавливают на банкоматах специальные устройства, которые считывают данные банковских карт жертв. Получив информацию о карте, они могут изготовить ее дубликат и снять с нее деньги.

2) Фишинг - злоумышленники рассылают СМС-сообщения или электронные письма, в которых просят жертв предоставить данные своей банковской карты.

3) **Лотереи**: уличные лотереи, игра в наперстки и т.д. Такие уличные аферы все еще в силе. Люди, желающие поучаствовать в акциях, принимают участие в любой лотерее или игре в наперстки. Механизм заманивания людей прост: "случайный прохожий" на глазах у толпы выигрывает крупную сумму денег. Такие трюки привлекают любителей халявы и азартных игр. Иногда схема изначально организована так, что человек даже получает прибыль за участие в процессе, но в итоге жертва проигрывает из-за азарта.

3) **Мошенничество с азартными играми.** К сожалению, в нашей стране существуют люди, которые так иначе увлекаются азартными играми, хотя по действующему законодательству Республики Казахстан – это запрещено. На вокзалах, в поездах и других многолюдных местах часто можно встретить опытных карточных игроков. Они оттачивают свое мастерство, выигрывая у доверчивых людей.

1) Подтасовывание карт. Мошенники заранее помечают карты, чтобы знать, какой выпадет в следующий раз.

2) Психологическое давление. Злоумышленники создают атмосферу азарта и подстегивают жертву продолжать игру, даже если она проигрывает.

3) Использование подставных лиц. Мошенники могут привлечь в игру подставное лицо, которое будет подыгрывать злоумышленнику и забирать всю ставку.

Мировой опыт борьбы с мошенничеством. Борьба с мошенничеством является постоянной проблемой для правительств, бизнеса и общественности во всем мире. Мошенничество затрагивает многие аспекты жизни - от финансовых махинаций и кражи личных данных до мошенничества в сфере онлайн-торговли и обмана потребителей. В каждой стране существуют свои законы и институты для борьбы с мошенничеством. В большинстве стран существуют специализированные органы по борьбе с преступлениями в сфере финансовых операций и мошенничеством. Эти органы часто сотрудничают с международными организациями, такими как Интерпол, для выявления и пресечения мошеннических схем. Компании и организации также играют важную роль в борьбе с мошенничеством. Многие компании создают специальные отделы по борьбе с мошенничеством, которые отслеживают подозрительные операции и сообщают о них в правоохранительные органы. Банки и финансовые учреждения внедряют новые технологии и системы безопасности, такие как двухфакторная аутентификация, биометрические технологии, а также совершенствуют антифрод системы. Ряд международных организаций, включая ООН и Всемирный банк, активно работают над разработкой и внедрением мер по укреплению законов и политики в области борьбы с мошенничеством по всему миру [3].

Опыт Казахстана в борьбе с мошенничеством. Граждане Казахстана обеспокоены ростом числа преступлений против собственности (кражи, мошенничество) и все большей изощренностью методов мошенничества и высокой частотой мошеннических инцидентов. Рассмотрим данные о регистрации мошенничества в официальной статистике компетентного органа - Комитета по правовой статистике и специальным учетам Генеральной Прокуратуры Республики Казахстан. Период, охватываемый исследованием - 2015-2021 годы (см. рисунок 1) [4].

Как видно, наблюдается снижение с 2015 по 2017 год, плавный рост с 2018 по 2019 год, и резкий скачек с 2020 года количества зарегистрированных случаев мошенничества в Казахстане.

На наш взгляд, тенденция роста количества зарегистрированных случаев мошенничества во многом связана с ростом компьютерной грамотности, повышением доступности интернет ресурсов и технологий, а также всеобщим переходом на онлайн обучение и оказание услуг, в связи с пандемией Коронавируса.

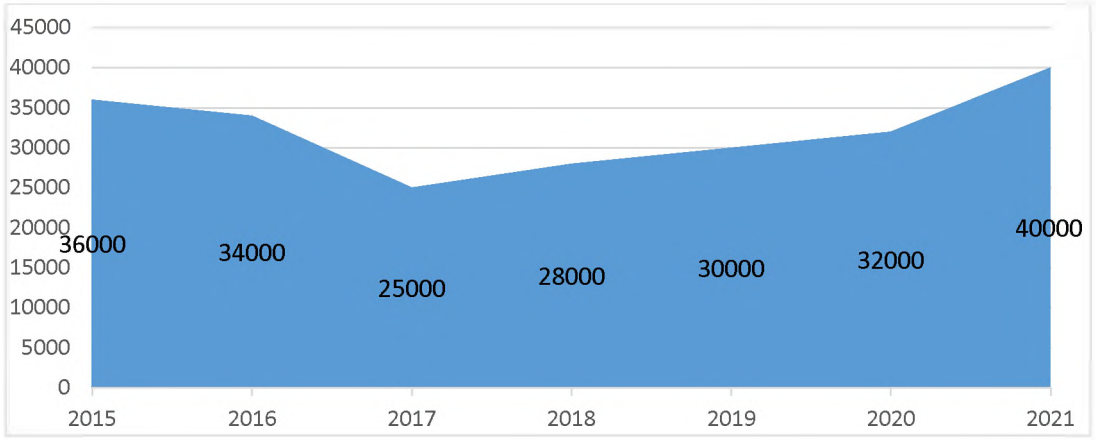

Рисунок 1. Динамика зарегистрированных мошенничеств в Казахстане за 2015-2021 гг.

Принятие концепции кибербезопасности «Cybershield of Kazakhstan» и национальной программы «Digital Kazakhstan» произошло в 2017 году. Так утвердился проект плана мероприятий по реализации концепции кибербезопасности «Cybershield of Kazakhstan», который включает в себя институциональные и законодательные меры, организационные и технические мероприятия, направленные на управление человеческим потенциалом и популяризацию мер безопасности в использовании информационных технологий. Несмотря на принимаемые меры киберпреступность не прекращала увеличиваться в числе (см. табл. 1) [4].

Таблица 1. Структура зарегистрированных мошенничеств в Республике Казахстан

Сферы и способы мошенничества	2018 г.	2019 г.	2020 г.	2021 г.
Путем займа денежных средств	44	67	42	122
В сфере кредитования	-	5	8	87
В сфере страхования	-	-	-	-
С использованием платежных карт	32	67	467	352
Интернет-мошенничество	516	7768	14219	21404
Связанное с недвижимостью	-	2	2	4
В сфере земельных правоотношений	-	-	-	4
Всего выявлено фактов мошенничества	29283	32287	33760	41084

Можно увидеть, что одним из основных видов экономических мошенничеств являются интернет-мошенничества. С 2018 по 2021 год наблюдается ежегодное увеличение преступлений в интернете. На сегодняшний день, наверное, нет ни одного пользователя социальных сетей, кому не звонили или не присылали бы сообщения мошенники. 2021 год стал переломным моментом, в борьбе с интернет-мошенниками.

В 2022 году было зафиксировано 20,6 тысячи преступлений в сфере интернет-мошенничества. Как отмечают аналитики, это число снизилось впервые с 2018 года. Однако, судя по всему, ущерб, нанесенный преступниками, по-прежнему очень велик и составляет более 20 миллиардов тенге.

В 2023 году зарегистрировано 13746 интернет-мошенничеств, в результате которых пострадало более 13,5 тыс. граждан, из них 70% жители городов (9613), остальные 30% сельской местности (4118). Общий нанесенный ущерб гражданам составляет 11,355 млрд тенге. Можно сделать выводы, что в 2023 году произошло

снижение преступлений в данной области благодаря усилению государственных мер противодействия.

Не лучше обстоят дела и в других странах. Возьмем для примера Российскую Федерацию. Так, по данным ИНТЕРФАКС.ру в 2023 году мошенники похитили у клиентов российских банков 15,7 млрд рублей. Это на 11,5% больше, чем в 2022 году (14,2 млрд рублей). Одна из возможных причин такого роста — более изощренные и подготовленные атаки телефонных мошенников.

В 2023 году было зафиксировано 984,8 тыс. мошеннических операций с использованием платежных карт. Наибольший объем средств (7,2 млрд рублей) был похищен именно с помощью карт. Частые схемы включают в себя фишинговые сообщения, призывающие пользователей ввести данные своей карты, а также звонки от лже-сотрудников банка, пытающихся выманить конфиденциальную информацию.

Кроме того, мошенники активно использовали другие каналы:

1) Операции по счетам (без карт): 85,3 тыс. операций на сумму 4,65 млрд рублей.
2) Система быстрых платежей (СБП): 82,4 тыс. операций на сумму 3,3 млрд рублей.
3) Электронные кошельки: 11,7 тыс. операций на сумму 105,2 млн рублей.

Несмотря на рост активности мошенников, банкам удалось вернуть клиентам 1,4 млрд рублей (8,7% от общего объема украденных средств). Это вдвое больше, чем в 2022 году (4,4%, или 618,4 млн руб.). Улучшение показателей по возврату денег может быть связано с более оперативной реакцией банков на мошеннические операции и возросшей осведомленностью клиентов о признаках финансового мошенничества.

С каждым годом мошенники становятся все более изощренными в своих методах. Они используют различные каналы общения, адаптируют свои схемы к новым технологиям и совершенствуют методы социальной инженерии, чтобы втереться в доверие к жертвам. Банкам приходится постоянно совершенствовать свои системы безопасности и повышать финансовую грамотность клиентов, чтобы противостоять растущей угрозе мошенничества.

В современном мире, где цифровые технологии прочно вошли в наши жизни, мошенничество и злоупотребления приобрели новые масштабы и формы. США и другие развитые страны не являются исключением из этой тревожной тенденции.

Согласно недавним данным Федеральной торговой комиссии США (FTC), в прошлом году было зарегистрировано около 2,2 миллиона жалоб на мошеннические действия, что на 30% больше, чем годом ранее. Треть этих жалоб привела к реальным финансовым потерям заявителей, которые в совокупности превысили 3,3 миллиарда долларов.

Заместитель директора FTC М. Вака отмечает, что мошенничество принимает различные формы, включая мошенничество с использованием кредитных карт, фишинг-атаки, аферы с технической поддержкой и инвестиционное мошенничество. Злоумышленники используют сложные методы, чтобы обмануть потребителей и завладеть их личными данными, сбережениями и даже идентичностью.

Рост онлайн-платформ и социальных сетей предоставил мошенникам новую среду для осуществления своей деятельности. Они создают поддельные веб-сайты, рассылают фишинговые электронные письма и используют социальные сети, чтобы обмануть ничего не подозревающих пользователей.

Мошенничество не только наносит финансовый ущерб отдельным лицам, но и подрывает доверие к цифровой экономике. Потребители становятся более

подозрительными и неохотно совершают покупки или делятся своей личной информацией в сети.

Чтобы бороться с растущей угрозой мошенничества, такие организации, как FTC, предпринимают ряд мер:

1) Проведение расследований и судебных разбирательств против мошеннических операций;

2) Повышение осведомленности потребителей о мошеннических схемах;

3) Сотрудничество с правоохранительными органами для выявления и пресечения деятельности мошенников.

Чтобы защитить себя от мошенничества, потребителям рекомендуется:

1) Быть бдительными и обращать внимание на любые подозрительные электронные письма, сообщения или звонки;

2) Никогда не предоставлять свою личную информацию в ответ на незапрошенные сообщения;

3) Быть осторожными при совершении покупок или инвестиций в незнакомых компаниях;

4) Использовать надежные пароли и двухфакторную аутентификацию для своих онлайн-аккаунтов;

5) Сообщать о любых подозрительных действиях в правоохранительные органы или FTC.

Мошенничество в эпоху цифровых технологий — это серьезная проблема, которая требует постоянного внимания и совместных усилий со стороны регулирующих органов, правоохранительных органов и самих потребителей. Понимая схемы мошенников и принимая надлежащие меры предосторожности, мы можем защитить себя от их преступных действий и сохранить безопасность нашей цифровой жизни.

Заключение

Важной частью борьбы с мошенничеством является повышение осведомленности граждан о способах и последствиях мошенничества. Развитие правовой культуры общества и повышение уровня правосознания граждан также играют важную роль в борьбе с мошенничеством. В этой связи правительство Казахстана проводит информационные кампании, направленные на предотвращение мошенничества, и обучает население методам выявления и предотвращения мошенничества. Однако, несмотря на эти достижения, Казахстан сталкивается с проблемами в борьбе с мошенничеством. В частности, сложность и транснациональный характер некоторых мошеннических схем создает проблемы с их выявлением и пресечением. В целом, Казахстан активно борется с мошенничеством и добился определенного прогресса в этой области. Однако проблемы остаются, и необходимы постоянные усилия всего мирового сообщества для эффективной борьбы с мошенничеством и защиты интересов населения и экономики.

Литература:

1. Мошеннические схемы в продажах, которые разоряли бизнес в 2019 году. URL: https://www.kom-dir.ru/article/1706-moshennicheskie-shemy-v-prodajah (дата обращения: 10.05.2024).
2. Корпоративное мошенничество. URL: https://www.cfin.ru/management/practice/Fraud_triangle.shtml. (дата обращения: 02.05.2024).
3. Взгляд в будущее с умеренным оптимизмом. URL: https://www.pwc.ru/ru/recs2019.pdf. (дата обращения: 02.05.2024).
4. Финпром.кз. URL: https://finprom.kz/ (дата обращения: 05.05.2024).

References:

1. Fraudulent sales schemes that ruined the business in 2019. URL: https://www.kom-dir.ru/article/1706-moshennicheskie-shemy-v-prodajah (data obrashcheniya: 05.10.2024).
2. Corporate fraud. URL: https://www.cfin.ru/management/practice/Fraud_triangle.shtml. (data obrashcheniya: 05.02.2024).
3. A look into the future with moderate optimism. URL: https://www.pwc.ru/ru/recs2019.pdf. (data obrashcheniya: 05.02.2024).
4. Finprom.kz. URL: https://finprom.kz/ (data obrashcheniya 05.05.2024).

Information about the authors:

Umurzakov I.G. – corresponding author, student, Kozybayev University, Petrolpavlovsk, Kazakhstan; e-mail: ibrayumurzakov2003@mail.ru;

Protasova O.V. – senior lecturer, «Economics and accounting» chair , master, Kozybayev University, Petrolpavlovsk, Kazakhstan; email: protasovaov@mail.ru;

Salturina A.M. – head of project office, Kazakhstan Technology Commercialization Center LLP, Astana, Kazakhstans; e-mail: s_ardak88@mail.ru.