Торайғыров университетінің
ҒЫЛЫМИ ЖУРНАЛЫ

НАУЧНЫЙ ЖУРНАЛ
Торайгыров университа

ТОРАЙҒЫРОВ УНИВЕРСИТЕТІНІҢ ХАБАРШЫСЫ

Экономикалық сериясы

1997 жылдан бастап шығады

TORAIGHYROV UNIVERSITY

ВЕСТНИК ТОРАЙГЫРОВ УНИВЕРСИТЕТА

Экономическая серия

Издается с 1997 года

ISSN 2710-3552

№ 2 (2025)
Павлодар

НАУЧНЫЙ ЖУРНАЛ
Торайгыров университета

Экономическая серия
выходит 4 раза в год

СВИДЕТЕЛЬСТВО
о постановке на переучет периодического печатного издания,
информационного агентства и сетевого издания
№ KZ93VPY00029686

выдано
Министерством информации и коммуникаций
Республики Казахстан

Тематическая направленность
публикация материалов в области экономики, управления,
финансов, бухгалтерского учета и аудита

Подписной индекс – 76133

https://doi.org/10.48081/NVZW5116

Бас редакторы – главный редактор
Давиденко Л. М.
доктор PhD

Заместитель главного редактора — Гребнев Л. С., *д.э.н., профессор*
Ответственный секретарь — Шеримова Н. М., *доктор PhD*

Редакция алқасы – Редакционная коллегия

Шмарловская Г. А.,	*д.э.н., профессор (Беларусь);*
Кунязов Е. К.,	*доктор PhD, доцент;*
Алмаз Толымбек,	*доктор PhD, профессор (США);*
Мукина Г. С.,	*доктор PhD,ассоц. профессор, доцент;*
Дугалова Г. Н.	д.э.н., профессор
Алтайбаева Ж. К.,	*к.э.н.*
Мусина А. Ж.,	*к.э.н., ассоц. профессор, доцент;*
Титков А. А.,	*к.э.н., доцент;*
Шокубаева З. Ж.	*технический редактор.*

За достоверность материалов и рекламы ответственность несут авторы и рекламодатели
Редакция оставляет за собой право на отклонение материалов
При использовании материалов журнала ссылка на «Вестник Торайгыров университета» обязательна

© Торайгыров университет

МРНТИ 06.73.55

https://doi.org/10.48081/WJLV9941

Б. Б. Суханбердина[1], Г. К. Курманова[2],
Б. А. Уразова[3], А. Ж. Утешкалиева[4]
[1,2,3,4]Западно-Казахстанский инновационно-технологический университет, Республика Казахстан, г. Уральск
[1]ORCID: https://orcid.org/0000-0002-8375-6350
[2]ORCID: https://orcid.org/0000-0002-9052-2990
[3]ORCID: https://orcid.org/0000-0001-9284-3301
[4]ORCID: https://orcid.org/0009-0002-0425-3817
*e-mail: suhanb@mail.ru

ФИНАНСОВОЕ МОШЕННИЧЕСТВО В УСЛОВИЯХ ЦИФРОВИЗАЦИИ БАНКОВСКИХ УСЛУГ

В современных условиях проблема финансового мошенничества, подрывающая экономическую и социальную стабильность Республики Казахстан, нарастает в свете дальнейшей цифровизации экономики. В ходе исследования выявлено что, несмотря на процесс постоянного повышения уровня банковской защиты конфиденциальных данных клиентов и финансовой базы данных, в сети Интернет с каждым днем появляются все новые личные данные клиентов банков, номера счетов и многое другое. Растут обороты финансового мошенничества с использованием дистанционных услуг и вовлечением обманутых граждан в мошеннические схемы. По мере того, как повышаются меры защиты банковской информации, совершенствуются и способы взлома систем защиты мошенниками. Усиливается тенденция мошеннических атак в большей степени не на банковские системы защиты информации, а непосредственно на клиентов банков. В статье проанализированы каналы осуществления мошеннических операций, теневой онлайн рынок скомпрометированных записей о платежных картах (даркнет), распространенные виды интернет-мошенничества, система мер и механизмов противодействия финансовому мошенничеству и повышения безопасности банковской информации, система антифрод-мониторинга Национального банка РК и др. Обосновано, что полностью обезопасить финансово-платежные системы и операции от финансового мошенничества невозможно, поскольку любые системы

безопасности со временем взламываются хакерами. Поэтому вопросы финансовой безопасности в большей степени заключаются в выявлении путей снижения рисков. Представлен комплекс мер по дальнейшему совершенствованию системы безопасности банковской информации, цифровых банковских и платежных платформ.

Ключевые слова: финансовое мошенничество, цифровизация банковских услуг, кибермошенничество, финансовая грамотность.

Введение

В условиях глобальной цифровизации финансово-банковский сектор экономики Казахстана активно внедряет IT-технологии в свою деятельность. Наряду с повышением доходности в результате внедрения новых технологий банки и их клиенты сталкиваются с повышенными рисками. Актуальность темы исследования определяется тем, что цифровизация банковских услуг создает благоприятные условия для реализации мошеннических операций с использованием Интернета. Уязвимыми для кибератак в основном являются платёжные карты, мобильные приложения, денежные переводы.

В настоящее время финансовое кибермошенничество процветает во всем мире, приобретая транснациональные черты. В 2023 году в странах ЕС ущерб от мошенничества в сфере платежей превысил 5 млрд. евро, а в США, согласно данным Американской банковской ассоциации, совокупные потери составили почти 11 млрд. долларов, при этом 3 млрд. долларов приходится на утечку персональных данных клиентов банков. Значительный вклад в этот процесс вносят инновационные технологии, такие как искусственный интеллект и нейронные сети, которые используются мошенниками для осуществления высокотехнологичных атак, например, с применением технологии DeepFake.

Вопрос финансового мошенничества в условиях цифровизации банковских услуг на сегодняшний день является предметом активных исследований, однако степень его изученности остаётся недостаточной для полного понимания всех аспектов и угроз, связанных с данным явлением. Существующие работы в основном фокусируются на отдельных аспектах проблемы, оставляя без внимания целый ряд важных факторов, влияющих на развитие и профилактику финансовых мошенничеств в условиях цифровой трансформации банковской сферы.

Целью исследования является анализ финансового мошенничества, связанного с использованием цифровых технологий в банковской сфере, и разработка рекомендаций по усилению защиты от мошенничества в условиях дальнейшей цифровизации банковских услуг в Республике Казахстан.

Объектом исследования является финансово-банковская сфера, а предметом – процессы цифровизации, которые изменяют способы взаимодействия между банками и их клиентами, а также создают новые риски и угрозы в сфере банковских услуг.

Материалы и методы

Проведение анализа сущности финансового мошенничества, его особенностей и общих тенденций развития осуществлялось путем обзора научной литературы. Особое внимание учеными и практиками уделяется вопросам влияния финансовой киберпреступности на экономику и общество [1; 2; 3; 4]. Исследуются направления совершенствования государственной политики в области борьбы с киберпреступлениями [5]; [6]. Ряд ученых приходит к выводу, что технологии, способствующие росту финансового мошенничества, могут быть использованы и для борьбы с ним. Для повышения эффективности борьбы с мошенничеством и защиты банковской информации необходимо осуществлять совместные усилия на международном уровне [7; 8].

В целом обзор литературы показывает, что исследования финансового мошенничества проводятся в разных направлениях, но их объединяет актуальность проблемы и необходимость более внимательного, всестороннего и постоянного ее изучения.

Практическая часть исследования проводилась на основе данных Бюро национальной статистики Агентства по стратегическому планированию и реформам Республики Казахстан, официальных отчетов различных государственных и финансовых учреждений, включая Национальный банк Республики Казахстан, Агентство Республики Казахстан по регулированию и развитию финансового рынка, а также компании Recorded Future.

В процессе исследования применялись различные методы научных исследований: обобщение и группировка данных для выявления общих тенденций в сфере финансового мошенничества; метод классификации для выделения различных типов мошеннических схем, использующих цифровые технологии; табличный и графический анализ данных для наглядного представления статистических результатов, таких как рост числа случаев мошенничества и ущерба от них; экономический анализ для оценки финансовых потерь и выявления экономических последствий финансового мошенничества; синтез для обобщения результатов и разработки рекомендаций по улучшению защиты от мошенничества.

Результаты и обсуждение

В Казахстане интернет-мошенничество стало рассматриваться как подвид мошенничества с 2018 года. Анализ данных о случаях финансового

мошенничества, включая данные о росте интернет-мошенничества и суммах ущерба показывает, что стремительное внедрение новых технологий в финансово-банковскую сферу экономики Республики Казахстан поставило под вопрос обеспечение безопасности банковской информации о клиентах и счетах. Мошенники активно пользуются уязвимостями цифровых банковских и платежных платформ (рисунок 1).

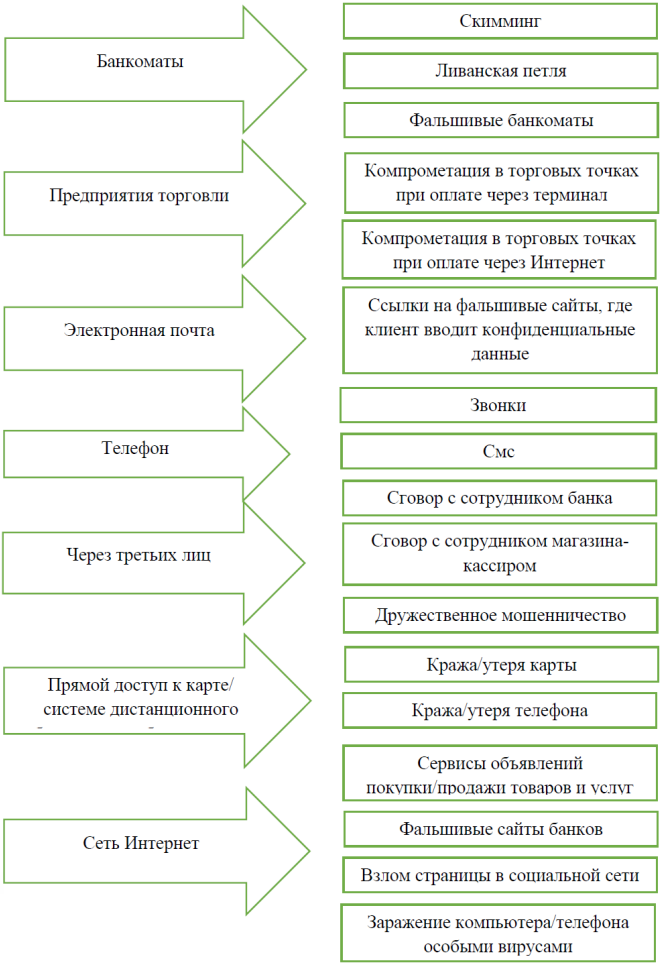

Рисунок 1 – Каналы проведения мошеннических операций
Примечание: Составлено авторами.

Среди наиболее часто встречающихся форм интернет-мошенничества выделяются следующие:

– вишинг – сбор персональных данных через телефонные звонки;

– смишинг – мошенничество посредством СМС-сообщений, например, уведомления о выигрыше в лотерее или конкурсе;

– содействие в обналичивании товарных кредитов;

– предложение посреднических услуг при оформлении кредитов;

– помощь в инвестициях в различные проекты, ценные бумаги и прочее;

– мошенничество, когда «сотрудник банка» просит установить на мобильное устройство определенное приложение;

– фишинг – извлечение личных данных через фальшивые веб-сайты;

– получение денежных средств за товары и услуги через ложные интернет-ресурсы;

– хищение средств с банковских карт и другие подобные схемы.

Мошеннические схемы, осуществляемые с использованием современных технологий, становятся все более сложными и разнообразными. Одним из методов является представление мошенников в качестве сотрудников банков или колл-центров, занимающихся предотвращением финансовых правонарушений. В ходе телефонных разговоров мошенники информируют жертв о якобы происходящих операциях по списанию средств с их платежных карт, при этом утверждают, что для сохранения остатка необходимо перевести деньги на другой счет. В результате таких манипуляций пострадавшие раскрывают свои персональные данные, что позволяет мошенникам осуществить несанкционированные транзакции с их карт.

Распространенной практикой также является рассылка фальшивых ссылок через электронную почту или SMS-сообщения, ведущих на поддельные веб-сайты. При переходе по этим ссылкам и заполнении форм на ложных платформах граждане без осознания передают информацию, предоставляющую злоумышленникам доступ к их личным кабинетам в мобильных банковских приложениях. Особенно активно такие схемы были использованы в период пандемии COVID-19, когда преступники использовали имя Всемирной организации здравоохранения для рассылки вредоносных писем и сообщений, что в итоге позволяло им получить доступ к учетным данным пользователей.

Для маскировки своих действий мошенники зачастую привлекают случайных людей, выполняющих роль посредников, как правило, под воздействием обмана или за вознаграждение. Эти участники, называемые

дропами или дропперами, обычно получают украденные средства на свои счета, после чего переводят их на счета мошенников.

Широко используют мошенники социальные сети и мессенджеры. В первой кредитной организации зафиксировано более 10 000 случаев мошенничества, связанных с «чисткой» кредитной истории и оформлением кредита с гарантией.

В последние годы в Казахстане активно развивается сектор электронной торговли, что привело к увеличению числа мошенничеств в этой области (рисунок 4). Онлайн-магазины, предлагающие товары по ценам, существенно ниже рыночных, часто используют схемы, обещающие возврат средств в случае несоответствия товаров заявленным характеристикам или выявления дефектов. Злоумышленники создают фальшивые интернет-магазины, размещают ссылки на несуществующие торговые платформы, требуя предоплату за товар. После получения средств они прекращают всякое взаимодействие с клиентами, оставляя их без компенсации.

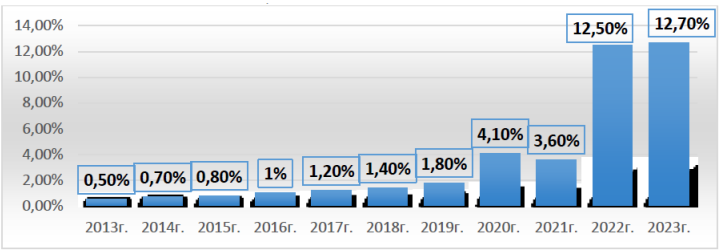

Рисунок 4 – Динамика развития электронной торговли в Казахстане, в процентах от общего объема розничной торговли

Примечание: Составлено авторами на основе источника [9].

Анализ данных, представленных Бюро национальной статистики Республики Казахстан, свидетельствует о значительном увеличении числа финансовых махинаций, осуществляемых с использованием интернет-технологий (рисунок 2,3).

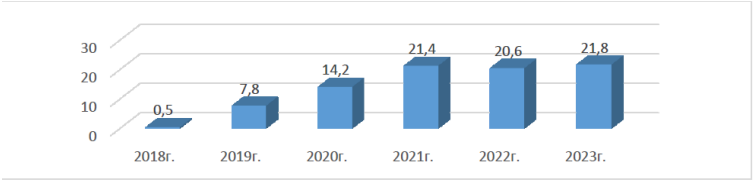

Рисунок 2 – Количество финансовых махинаций в Республике Казахстан, связанных с интернет-мошенничеством, тыс. ед.
Примечание: Составлено авторами на основе источника [9].

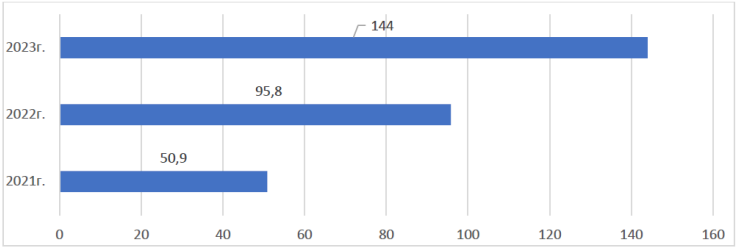

Рисунок 3 – Сумма ущерба от финансового мошенничества в целом по Республике Казахстан, млрд. тенге
Примечание: Составлено авторами на основе источника [9].

На данный момент официальная статистика в Республике Казахстан только начинает фиксировать данные о масштабах финансового мошенничества, осуществляемого с использованием Интернета. В связи с этим, детализированная информация как по видам мошенничества, так и по регионам страны, пока отсутствует. Это обстоятельство ограничивает возможность проведения как количественного, так и качественного анализа динамики форм и видов, а также региональных особенностей развития финансового мошенничества в Республике Казахстан.

Анализ имеющихся данных показал, что в настоящее время финансовое мошенничество приобрело значительный размах не только в Республике Казахстан, но и во всем мире. Вследствие роста финансового мошенничества в ряде стран мира сформировался значительный теневой онлайн-рынок, специализирующийся на торговле скомпрометированными данными о платежных картах. Этот рынок является частью даркнета, который представляет собой сегмент черного рынка в интернете.

В настоящее время на платформе даркнета активно осуществляется продажа таких данных по всему миру. Исследования теневого рынка скомпрометированных платежных карт проводятся компанией Recorded Future в рамках проекта Insikt. Результаты этих исследований представлены на рисунке 5.

Повышение объемов продаж скомпрометированных записей о платежных картах на теневом рынке в 2020 и 2021 годах объясняется ростом онлайн покупок, спровоцированных пандемией. Рост продаж в 2023 году произошел в связи с увеличением количества хищений личных данных клиентов банков по разным каналам.

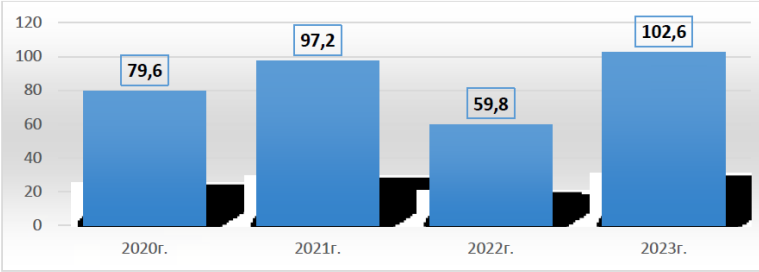

Рисунок 5 – Количество проданных скомпрометированных записей о платежных картах в Даркнете, млн. ед.

Примечание: Составлено авторами на основе источника [10].

В рамках международных платежных систем существуют общие рекомендации по мерам противодействия мошенникам. Платежные системы советуют свои клиентам не пользоваться платежными картами при оплате за товары и услуги в странах, где зафиксирован высокий уровень мошенничества.

К странам с высоким уровнем финансового мошенничества относятся:

– страны Восточной Европы: Болгария, Польша, Румыния;

– страны Азиатско-Тихоокеанского региона: Индонезия, Малайзия, Таиланд, Сингапур, Филиппины;

– страны Ближнего Востока: Ирак, Иран, Сирия, Палестина;

– страны Южной Америки: Бразилия, Аргентина, Перу, Чили.

В ряде государств рекомендуется ограничивать использование платежных карт исключительно крупными торговыми точками, банками, международными гостиничными сетями и аэропортами. Для снятия наличных средств наиболее безопасным вариантом является

использование банкоматов, расположенных в учреждениях, таких как банки, аэропорты, гостиницы и крупные торговые центры.

В Казахстане, как и в других странах, предпринимаются меры по противодействию финансовому мошенничеству. В целях борьбы с финансовым мошенничеством, осуществляемым с помощью сети Интернет, в 2017 году в Казахстане была разработана и внедрена концепция «Киберщит Казахстана», направленная на комплексную защиту информации государственных органов, организаций и граждан [11]. В рамках этой инициативы в законодательство страны был введен термин «киберстрахование», которое предназначено для компенсации убытков, возникших в результате деятельности интернет-мошенников.

В 2018 году в Казахстане был основан Национальный координационный центр информационной безопасности, основным назначением которого является защита информационных платформ и сетей государственных органов, а также объектов, имеющих стратегическое значение для страны.

В 2022 году с целью повышения уровня безопасности финансового рынка Казахстана была осуществлена интеграция единой технологической платформы Национального банка с автоматизированной системой обработки информации о событиях и инцидентах в области информационной безопасности на финансовом рынке – «Qainar» (АСОИ «Qainar»).

Система «Qainar» осуществляет онлайн-мониторинг всех операций на финансовом рынке, выявляя потенциальные мошеннические действия. В 2023 году деятельность системы «Qainar» в области информационной безопасности была преимущественно ориентирована на предотвращение кибератак, что составило 71,2% от общего числа инцидентов (рисунок 6).

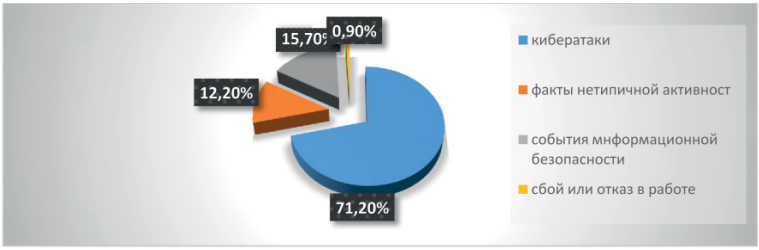

Рисунок 6 – Направления работы системы «Qainar» в 2023 году
Примечание: Составлено авторами на основе источника [12].

В 2023 году системой «Qainar» было выдано 104 предупреждения об угрозах информационной безопасности, 78 предупреждений

об уязвимостях информационной безопасности, отработано 86 информационных инцидентов, возникших в финансовых организациях, в том числе 55 DDoS-атак (рисунок 7). По результатам работы системы «Qainar» в 2023 году было выявлено 32 мошеннических интернет-ресурса. Информация о данных платформах была передана в компетентные органы, в частности, в Министерство культуры и информации РК, для дальнейшей блокировки соответствующих ресурсов.

Активизация мошеннических атак вынуждает финансовые учреждения объединяться и действовать совместно. Это обусловлено тем, что современные финансовые мошенники обладают капиталом, значительно превышающим финансовые возможности отдельных банков. В настоящее время мошеннические схемы часто не осуществляются отдельными индивидами, а представляют собой деятельность организованных преступных групп, в состав которых могут входить десятки или даже сотни участников.

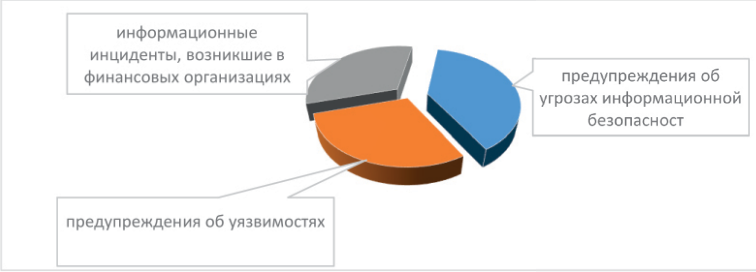

Рисунок 7 – Зафиксированные и отработанные события информационной безопасности в системе «Qainar» в 2023 году

Примечание: Составлено авторами на основе источника [12].

Одной из эффективных систем защиты от финансовых мошеннических схем во многих странах признается система антифрод-мониторинга. Такая система была запущена и в Казахстане в августе 2024 года. Антифрод-центр был создан по инициативе Национального банка и получил название «Центр по обмену данными о мошеннических транзакциях».

Единая система антифрод-мониторинга представляет собой онлайн-систему, обнаруживающую подозрительные звонки и операции в режиме реального времени. Она позволяет мгновенно предупредить коммерческий банк о подозрительной финансовой операции по счету конкретного клиента банка в момент ее совершения.

Совершенствование системы происходит на основе пополнения ее базы данных информацией, которую загружают коммерческие банки-участники системы антифрод. В сущности, единая система антифрод-мониторинга представляет собой объединение различных антифрод-платформ банков-участников.

Система антифрод-мониторинга обладает комплексностью, системностью, детальностью и другими значимыми характеристиками, позволяющими эффективно бороться с мошенничеством с кредитами (рисунок 8).

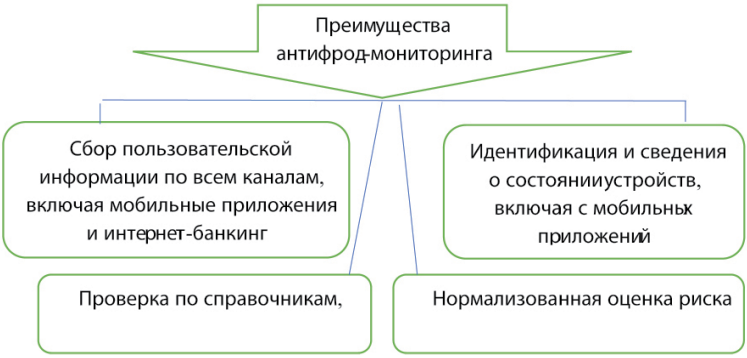

Рисунок 8 – Основные преимущества использования антифрод-мониторинга

Примечание: Составлено авторами.

К настоящему времени с помощью системы антифрод-мониторинга было приостановлено в процессе оформления свыше 17 млн. тенге кредитных средств клиентов коммерческих банков. Однако у системы антифрод-мониторинга есть слабые стороны. В основном система обрабатывает уже заверенные финансовые операции. Например, кредит уже оформлен и выдан. Система может отреагировать на такие подозрительные операции как перевод полученного кредита сразу на другие счета.

На сегодняшний день борьба с мошенничеством представляет собой одну из приоритетных задач для коммерческих банков. Каждое финансовое учреждение разрабатывает и внедряет индивидуальную политику, направленную на защиту конфиденциальных данных клиентов и обеспечение безопасности финансовых баз данных.

Среди основных путей снижения рисков при операциях с платежными картами, которые используют банки можно отметить такие как:

– автоматическое блокирование платежной карты после трехкратного неверно указанного PIN-кода;

– возможность установки лимита на расходные, переводные, кредитные операции по платежной карте;

– мониторинг операций по платежным картам с целью выявления подозрительных, мошеннических операций;

– возможность установления автоматических уведомлений (СМС или push-оповещения) о движении средств по карточному счету;

– требование периодически обновлять пароли и коды быстрого доступа в мобильных банковских приложениях;

– оповещение клиентов - владельцев карт на официальных сайтах, в расчетно-кассовых центрах, через рассылки и мессенджеры о разных видах мошенничества и способах защиты от них;

– использование камер на банкоматах;

– установка антискиммерных модулей;

– ограничение доступа сотрудников банка к персональным данным пользователей платежных карт;

– смс уведомление при высылке одноразового кода о том, чтобы не сообщать его никому, включая сотрудников банка;

– при обнаружении несанкционированной операции банки проводят претензионную работу;

– предложение виртуальной карты для проведения платежных операций в Интернет;

– оповещение о попытке входа в систему дистанционного банковского обслуживания с незарегистрированных устройств и т.п.

Коммерческие банки также продолжают совершенствовать методы защиты платежных карт, включая следующие инновационные подходы:

– нанесение дополнительных защитных полос с уникальными узорами, выполненными с использованием магнитных чернил;

– идентификация карт с помощью долгоживущих радиоизотопов;

– использование специального пластика для производства карт, обладающего высокой чувствительностью к изменениям температуры и давления, что затрудняет манипуляции с картой.

Исследование направлений финансовых мошенничеств позволило выявить тенденцию, согласно которой в последние годы мошеннические атаки становятся всё более ориентированными не на банковские учреждения, а на их клиентов. Мошенники используют доверчивость

и уязвимости граждан, воздействуя на их страхи и недостаточную осведомленность. В этом контексте вопросы финансового мошенничества и минимизации рисков, связанных с проведением финансово-платежных операций, требуют внимания как со стороны банков, так и со стороны пользователей. Регулярное соблюдение базовых правил безопасности при использовании финансовых инструментов и онлайн-платформ зачастую оказывается достаточной мерой для предотвращения мошенничества и защиты денежных средств.

Поскольку основной способ оплаты товаров в интернете осуществляется с использованием банковских карт, среди основных методов минимизации рисков мошенничества клиенты банков могут применять различные защитные механизмы, включая мониторинг операций, установку лимитов на сумму оплаты и другие аналогичные меры.

Мониторинг транзакций является одним из наиболее эффективных методов снижения финансовых рисков. Постоянный контроль как за расходными, так и за доходными операциями позволяет владельцам банковских счетов отслеживать движение средств и своевременно выявлять несанкционированные действия.

В случае, если держатель платежной карты уведомляет банк о несанкционированном списании средств в течение 24 часов после завершения операции, финансовое учреждение обязано возместить сумму незаконных списаний при условии соблюдения владельцем карты всех установленных норм безопасного использования платежных инструментов. В процессе рассмотрения заявления банк проводит проверку на предмет нарушений условий безопасного использования, и в случае отсутствия таковых компенсация ущерба будет произведена.

Дополнительно банки рекомендуют избегать хранения крупных сумм на одной карте, особенно если она используется для регулярных платежей. Рекомендуется ограничивать баланс на таких картах и пополнять их по мере необходимости через переводы с других карт или депозитных счетов. В случае утечки конфиденциальных данных клиента в руки мошенников, они могут воспользоваться этой информацией для доступа к мобильным банковским приложениям и осуществления различных операций, включая оформление кредитов. Для предотвращения подобных ситуаций банки советуют своим клиентам регулярно проверять свою кредитную историю. Это можно сделать через онлайн-платформу egov.kz, в Центре обслуживания населения или в других специализированных учреждениях.

Банки рекомендуют своим клиентам устанавливать лимиты на суммы, которые могут быть потрачены не только для оплаты товаров и услуг через

интернет, но и для любых переводов денежных средств. Установление таких лимитов, например, для ежедневных расходов, представляет собой эффективный инструмент контроля за собственными затратами и одновременно служит дополнительной мерой защиты от кибератак со стороны мошенников.

В качестве дополнительной меры безопасности для пользователей платежных карт банки предлагают оформление страхового полиса. Данный полис предназначен для компенсации убытков владельца карты, которые могут возникнуть в результате мошеннических операций, если:

– платежная карта была потеряна в результате грабежа или разбоя, после которых с нее были списаны средства или на нее были оформлены кредиты;

– платежная карта была оформлена и был получен PIN-код под угрозой жизни или здоровью и по ней были совершены операции;

– наличные денежные средства были утеряны в результате грабежа, разбоя в течении двух часов после снятия средств в банкомате;

– платежная карта утеряна в результате размагничивания или других случайных физических повреждений;

– операции были совершены по поддельной платежной карте, но с действительными реквизитами;

– платежная карта утеряна в результате технической неисправности банкомата и т.п.

Страховой полис не распространяется на убытки, возникшие в результате нарушения владельцем карты правил безопасного использования платежных средств, включая случаи, когда конфиденциальная информация была передана третьим лицам.

Исследование показывает, что несмотря на имеющиеся достижения в области защиты финансово-платежных систем от мошенников, банки, регуляторы и технологические компании должны и далее активно сотрудничать в создании и внедрении эффективных решений по борьбе с финансовым мошенничеством. Рекомендуется реализация следующих комплексных мер:

1 Присоединение Республики Казахстан к Будапештской конвенции о компьютерных преступлениях, поскольку финансовое кибермошенничество обладает транснациональным характером.

2 Интеграция международных стандартов защиты данных и борьбы с киберпреступностью. Следует активно участвовать в международных инициативах по защите персональных данных и борьбе с киберпреступностью, таких как GDPR в Европейском Союзе, что позволит

Казахстану адаптировать свои подходы к международным стандартам и повысить доверие иностранных партнеров.

3 Создание и развитие специализированных центров для борьбы с финансовыми киберугрозами. Организация центров, занимающихся исключительно расследованием киберпреступлений в сфере финансов, с привлечением экспертов по цифровой безопасности, аналитиков и специалистов по обработке данных. Эти центры могут служить как для профилактики, так и для расследования уже произошедших инцидентов.

4 Совершенствование работы Антифрод-центра, в том числе через расширение его технологических возможностей с использованием открытых программных интерфейсов (API), автоматизацию бизнес-процессов, а также внедрение технологий искусственного интеллекта для повышения эффективности выявления подозрительных транзакций.

5 Совершенствование систем защиты банковских транзакций и баз данных, включая внедрение антискимминговых модулей в банкоматах, расширение применения биометрических и нейронно-сетевых систем для повышения уровня безопасности при осуществлении банковских операций, использование блокчейн-технологий для защиты данных.

6 Разработка и внедрение стандартов безопасности для мобильных приложений и онлайн-банкинга. Учитывая растущее количество пользователей мобильных банковских сервисов, важно создать строгие стандарты безопасности для этих приложений, включая двухфакторную аутентификацию, постоянные обновления ПО и шифрование данных на всех уровнях.

7 Ужесточение контроля за аутентификацией транзакций. Введение обязательных требований к многоуровневой аутентификации для крупных финансовых операций, что позволит значительно снизить риски несанкционированного доступа и операций.

8. Стимулирование сотрудничества между частными и государственными учреждениями в сфере защиты от киберугроз. Важным шагом будет укрепление партнерских отношений между частными финансовыми организациями и государственными учреждениями для обмена опытом, информации о текущих угрозах и совместной разработки эффективных решений по безопасности.

9 Повышение уровня финансовой грамотности среди населения, что является актуальной задачей не только для Казахстана, но и для других стран. Финансовая неграмотность зачастую становится самой уязвимой точкой в денежно-финансовом обороте страны, так как основная тактика мошенников заключается в использовании незнания принципов работы

финансового рынка, отдельных платежных инструментов, а также наивности и неопытности физических лиц, являющихся участниками финансово-платежных операций.

В целях повышения финансовой грамотности населения необходимо использовать многоканальный подход, способствующий максимальному охвату населения: создание банковских обучающих приложений по цифровой и киберграмотности, разработка электронных финансовых планировщиков и приложений для обратной связи, проведение регулятором и банками второго уровня онлайн-викторин, конкурсов в социальных сетях и на интернет-ресурсах по цифровой грамотности и защиты от рисков, проведение Национальным банком и банками второго уровня образовательных кампаний об основных видах кибермошенничества и т.п. [13].

Эти меры в совокупности будут способствовать значительному укреплению защиты финансовых транзакций, повышению уровня доверия со стороны граждан и бизнеса, а также снижению рисков, связанных с финансовым кибермошенничеством в условиях дальнейшей цифровизации банковских услуг.

Выводы

Проведенное исследование позволяет сделать вывод, что внедрение современных информационных технологий способствует повышению эффективности банковских операций и улучшению обслуживания клиентов, но, с другой стороны, создает новые угрозы, в том числе в виде растущего числа случаев финансового мошенничества. Несмотря на постоянное совершенствование мер и форм противодействия финансовому мошенничеству в Республике Казахстан проблема борьбы с цифровым мошенничеством остается актуальной. Исследование природы и особенностей финансового мошенничества в условиях цифровизации банковских услуг показывает, что только эффективное взаимодействие всех участников финансово-денежного оборота может значительно снизить риски финансовых потерь. В целом, исследование подчеркивает необходимость дальнейшего изучения проблемы финансового мошенничества и методов борьбы с ним в контексте дальнейшей цифровизации банковских услуг для выявления путей безопасного функционирования цифровых банковских и платежных платформ.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 **Ramadani, S., Putera, A.** Impact of cybercrime on technological and financial developments // International journal for innovative research in multidisciplinary field. – 2018. – P. 341–344. [Электронный ресурс]. – URL: https://www.researchgate.net/publication/329001306_Impact_of_cybercrime_on_technological_and_financial_developments.

2 **Bossler, A. M., Berenblum, T.** Introduction : new directions in cybercrime research, 2019 [Электронный ресурс]. – URL: https://www.tandfonline.com/doi/epdf/10.1080/0735648X.2019.1692426?needAccess=true.

3 **Rossy, Q., Ribaux, O.** Orienting the development of crime analysis processes in police organizations covering the digital transformations of fraud mechanisms // European journal on criminal policy and research. – 2020. – 26(3). [Электронный ресурс]. – URL: https://serval.unil.ch/resource/serval:BIB_D1B9E966E9C6.P001/REF.pdf.

4 **Головинов, О. Н., Погорелов, А. В.** Киберпреступность в современной экономике : состояние и тенденции развития. – 2016. [Электронный ресурс]. – URL: https://cyberleninka.ru/article/n/kiberprestupnost-v-sovremennoy-ekonomike-sostoyanie-i-tendentsii-razvitiya.

5 **Дадалко, В. А.** Методы противодействия рискам кассового мошенничества как инструмент обеспечения экономической безопасности организации. – 2017. [Электронный ресурс]. – URL: https://cyberleninka.ru/article/n/metody-protivodeystviya-riskam-kassovogo-moshennichestva-kak-instrument-obespecheniya-ekonomicheskoy-bezopasnosti-organizatsii

6 **Петрякова, Л. А.** Проблемы квалификации мошенничества в банковской сфере. – 2020. [Электронный ресурс]. – URL: https://cyberleninka.ru/article/n/problemy-kvalifikatsii-moshennichestva-v-bankovskoy-sfere

7 **Achim, M. V., Borlea, S. N. McGee, R. W., Muresan, G. M., Safta, I. L., Vaidean, V. L.** Financial crime : a literature review. 2020 [Электронный ресурс]. – URL: https://www.researchgate.net/publication/366090442_Financial_Crime_A_Literature_Review

8 **Nicholls, J., Kuppa, A., Le-Khac, N. A.** Financial cybercrime : a comprehensive survey of deep learning approaches to tackle the evolving financial crime landscape. – 2021 [Электронный ресурс]. – URL: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9642993

9 Бюро национальной статистики Агентства по стратегическому планированию и реформам Республики Казахстан [Электронный ресурс]. – URL: https://stat.gov.kz/ru/

10 Insikt Group is Recorded Future's. [Электронный ресурс]. – URL: https://www.recordedfuture.com/research/insikt-group.

11 Об утверждении Концепции кибербезопасности («Киберщит Казахстана»). Постановление Правительства Республики Казахстан от 30 июня 2017 года № 407 [Электронный ресурс]. – URL: https://adilet.zan.kz/rus/docs/P1700000407.

12 Национальный Банк Республики Казахстан [Электронный ресурс]. – URL: https://www.nationalbank.kz/ru

13 **Суханбердин, Б. Б., Құрманова, Г. К., Утешқалиева, А. Ж.** Платежные карты в системе безналичных расчетов Республики Казахстан // Мемлекеттік аудит – Государственный аудит. – 2023. – № 4 (61). – С. 47–60. [Электронный ресурс]. – URL: https://gov-audit.kz/index.php/ma/article/view/149/140.

REFERENCES

1 **Ramadani, S., Putera, A.** Impact of cybercrime on technological and financial developments. // International journal for innovative research in multidisciplinary field, 2018. 341–344. [Electronic resource]. – URL: https://www.researchgate.net/publication/329001306_Impact_of_cybercrime_on_technological_and_financial_developments.

2 **Bossler, A. M., Berenblum, T.** Introduction: new directions in cybercrime research, 2019. [Electronic resource]. – URL: https://www.tandfonline.com/doi/epdf/10.1080/0735648X.2019.1692426?needAccess=true.

3 **Rossy, Q., Ribaux, O.** Orienting the development of crime analysis processes in police organizations covering the digital transformations of fraud mechanisms // European journal on criminal policy and research/ – 2020. – 26(3). [Electronic resource]. – URL: https://serval.unil.ch/resource/serval:BIB_D1B9E966E9C6.P001/REF.pdf.

4 **Golovinov, O. N., Pogorelov, A. V.** Kiberprestupnost v sovremennoi ekonomike: sostoyanie i tendentsii razvitiya [Cybercrime in the modern economy: state and development trends] 2016. [Electronic resource]. – URL: https://cyberleninka.ru/article/n/kiberprestupnost-v-sovremennoy-ekonomike-sostoyanie-i-tendentsii-razvitiya.

5 **Dadalko, V. A.** Metody protivodeystviya riskam kassovogo moshennichestva kak instrument obespecheniya ekonomicheskoy bezopasnosti organizatsii [Methods for countering the risks of cash fraud as a tool for ensuring the economic security of an organization]. – 2017. [Electronic resource]. – URL: https://cyberleninka.ru/article/n/metody-protivodeystviya-riskam-kassovogo-moshennichestva-kak-instrument-obespecheniya-ekonomicheskoy-bezopasnosti-organizatsii.

6 **Petryakova, L. A.** Problemy kvalifikatsii moshennichestva v bankovskoy sfere [Problems of qualifying fraud in the banking sector] 2020. [Electronic resource]. – URL: https://cyberleninka.ru/article/n/problemy-kvalifikatsii-moshennichestva-v-bankovskoy-sfere.

7 **Achim, M. V., Borlea, S. N. McGee, R. W., Muresan, G. M., Safta, I. L., Vaidean, V. L.** Financial crime : A literature review. – 2020. [Electronic resource]. – URL: https://www.researchgate.net/publication/366090442_Financial_Crime_A_Literature_Review.

8 **Nicholls, J., Kuppa, A., Le-Khac, N. A.** Financial cybercrime: a comprehensive survey of deep learning approaches to tackle the evolving financial crime landscape. – 2021. [Electronic resource]. – URL: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9642993.

9 Byuro natsional'noi statistiki Agentstva po strategicheskomu planirovaniyu i reformam Respubliki Kazakhstan [Bureau of National Statistics Agency for Strategic Planning and Reforms of the Republic of Kazakhstan] [Electronic resource]. – URL: https://stat.gov.kz/ru/.

10 Insikt Group is Recorded Future's. [Electronic resource]. – URL: https://www.recordedfuture.com/research/insikt-group.

11 Ob utverzhdenii Kontseptsii kiberbezopasnosti («Kiberschit Kazakhstana»). Postanovlenie Pravitelstva Respubliki Kazakhstan ot 30 iyunya 2017 goda № 407 [On approval of the Cyber Security Concept («Cyber Shield of Kazakhstan»). Decree of the Government of the Republic of Kazakhstan dated June 30, 2017 No. 407] [Electronic resource]. – URL: https://adilet.zan.kz/rus/docs/P1700000407.

12 Natsionalnyi Bank Respubliki Kazakhstan [National Bank of the Republic of Kazakhstan] [Electronic resource]. – URL: https://www.nationalbank.kz/ru.

13 **Sukhanberdina, B. B., Kurmanova, G. K., Uteshkalieva, A. Sh.** Plateshnye karty v sisteme beznalichnyh raschetov Respubliki Kazakhstan [Payment cards in the non-cash payment system of the Republic of Kazakhstan] // Memlekettik audit – Gosudarstvennyi audit. – 2023. – № 4 (61). – P. 47–60.

[Electronic resource]. – URL: https://gov-audit.kz/index.php/ma/article/view/149/140.

Поступило в редакцию 24.01.25.
Поступило с исправлениями 07.04.25.
Принято в печать 30.04.25.

**Б. Б. Суханбердина[1], Г. К. Курманова[2],*
Б. А. Уразова[3], А. Ж. Утешкалиева[4]
[1,2,3,4]Батыс Қазақстан инновациялық-технологиялық университеті,
Қазақстан Республикасы, Орал қ.
24.01.25 ж. баспаға түсті.
07.04.25 ж. түзетулерімен түсті.
30.04.25 ж. басып шығаруға қабылданды.

БАНКТІК ҚЫЗМЕТТЕРДІ ЦИФРЛАНДЫРУ ЖАҒДАЙЫНДАҒЫ ҚАРЖЫЛЫҚ АЛАЯҚТЫҚ

Қазіргі жағдайда Қазақстан Республикасының экономикалық және әлеуметтік тұрақтылығына нұқсан келтіретін қаржылық алаяқтық проблемасы экономиканы одан әрі цифрландыру тұрғысынан өсуде. Зерттеу барысында клиенттердің құпия деректерін және қаржылық деректер базасын банктік қорғау деңгейін үнемі арттыру процесіне қарамастан, Интернет желісінде күн сайын банк клиенттерінің барлық жаңа жеке деректері, шот нөмірлері және т.б. пайда болатыны анықталды. Қашықтықтан қызмет көрсетуді пайдалану және алданған азаматтарды алаяқтық схемаларға тарту арқылы қаржылық алаяқтық айналымы өсуде. Банктік ақпаратты қорғау шаралары жоғарылаған сайын, алаяқтардың қорғаныс жүйелерін бұзу тәсілдері де жетілдірілуде. Алаяқтық шабуылдардың тенденциясы көбінесе ақпаратты қорғаудың банктік жүйелеріне емес, тікелей банк клиенттеріне артады. Мақалада алаяқтық операцияларды жүзеге асыру арналары, төлем карталары туралы бұзылған жазбалардың көлеңкелі онлайн нарығы (Darknet), интернет-алаяқтықтың кең таралған түрлері, қаржылық алаяқтыққа қарсы іс-қимыл шаралары мен тетіктері және банктік ақпараттың қауіпсіздігін арттыру жүйесі, ҚР Ұлттық Банкінің антифрод-мониторинг жүйесі және т. б. талданды. қаржылық алаяқтық

мүмкін емес, өйткені кез-келген қауіпсіздік жүйесін уақыт өте келе хакерлер бұзады. Сондықтан қаржылық қауіпсіздік мәселелері тәуекелдерді азайту жолдарын анықтау болып табылады. Банктік ақпараттың, цифрлық банктік және төлем платформаларының қауіпсіздік жүйесін одан әрі жетілдіру жөніндегі шаралар кешені ұсынылды.

Кілтті сөздер: қаржылық алаяқтық, банктік қызметтерді цифрландыру, кибер алаяқтық, қаржылық сауаттылық.

**B. B. Sukhanberdina[1], G. K. Kurmanova[2],*
B. A. Urazova[3], A. J. Uteshkalieva[4]
[1,2,3,4]West Kazakhstan Innovative-technological University,
Republic of Kazakhstan, Uralsk.
Received 24.01.25.
Received in revised form 07.04.25.
Accepted for publication 30.04.25.

FINANCIAL FRAUD IN THE CONTEXT OF DIGITALIZATION OF BANKING SERVICES

In modern conditions, the problem of financial fraud, undermining the economic and social stability of the Republic of Kazakhstan, is growing in the light of further digitalization of the economy. The study revealed that, despite the process of constantly increasing the level of bank protection of confidential customer data and the financial database, new personal data of bank customers, account numbers and more are appearing on the Internet every day. The volume of financial fraud involving remote services and the involvement of deceived citizens in fraudulent schemes is growing. As measures to protect banking information are being improved, the methods of hacking security systems by fraudsters are also being improved. The trend of fraudulent attacks is increasing, not against banking information security systems, but directly against bank customers. The article analyzes the channels of fraudulent transactions, the shadow online market of compromised payment card records (darknet), common types of online fraud, a system of measures and mechanisms to combat financial fraud and improve the security of banking information, the anti-fraud monitoring system of the National Bank of the Republic of Kazakhstan, etc. It is proved that it is impossible to fully secure financial and payment systems

and operations from financial fraud, since any security systems are eventually hacked by hackers. Therefore, financial security issues are more about identifying ways to reduce risks. A set of measures is presented to further improve the security system of banking information, digital banking and payment platforms.

Keywords: financial fraud, digitalization of banking services, cyber fraud, financial literacy.

Теруге 19.05.2025 ж. жіберілді. Басуға 30.06.2025 ж. қол қойылды.
Электронды баспа
17,1 Mb RAM
Шартты баспа табағы 34,8
Таралымы 300 дана. Бағасы келісім бойынша.
Компьютерде беттеген: А. К. Мыржикова
Корректорлар: А. Р. Омарова, Д. А. Кожас
Тапсырыс № 4407

Сдано в набор 19.05.2025 г. Подписано в печать 30.06.2025 г.
Электронное издание
17,1 Mb RAM
Усл.п.л. 34,8. Тираж 300 экз. Цена договорная.
Компьютерная верстка: А. К. Мыржикова
Корректоры: А. Р. Омарова, Д. А. Кожас
Заказ № 4407

«Toraighyrov University» баспасынан басылып шығарылған
Торайғыров университеті
140008, Павлодар қ., Ломов к., 64, 137 каб.

«Toraighyrov University» баспасы
Торайғыров университеті
140008, Павлодар қ., Ломов к., 64, 137 каб.
8 (7182) 67-36-69
e-mail: kereku@tou.edu.kz
www.vestnik.tou.edu.kz
www.vestnik-economic.tou.edu.kz