Научная статья
УДК 338.7

Статья поступила в редакцию 13.04.2025;
одобрена после рецензирования 29.05.2025;
принята к публикации 14.07.2025.

Влияние цифровых финансовых технологий на экономическую безопасность государства

Лев Исакович Ушвицкий[1], Ирина Викторовна Филатова[2]

[1] Северо-Кавказский федеральный университет, Ставрополь, Россия
[2] Главное управление по работе с личным составом Министерства внутренних дел Российской Федерации, Москва, Россия

Аннотация:
Введение. Развитие финансовых технологий и рост цифровизации экономического пространства обусловили резкое увеличение киберпреступлений. Наличие пробелов в законодательстве негативно сказывается на эффективности применения проактивных и адаптивных стратегий противодействия им. Данные тенденции также способствуют росту масштабов теневой экономики и уклонения от уплаты налогов, что отрицательно влияет на уровень экономической безопасности страны. ***Методы.*** Методологическую основу исследования составили компаративный и ретроспективный методы. Это позволило выявить специфику совершения киберпреступлений и определить ключевые направления противодействия им с применением технологий искусственного интеллекта. ***Результаты.*** Обеспечение приемлемого уровня безопасности финансовой системы требует принятия комплексной стратегии, базирующейся на использовании передовых технологий искусственного интеллекта и больших данных. Повышение эффективности взаимодействия государства и бизнеса в части выявления и пресечения преступлений в финансовой сфере позволит обеспечить устойчивое развитие функционирования экономической системы страны, а также повысить уровень экономической безопасности. Расширение международного сотрудничества является ключевым фактором в борьбе с трансграничными финансовыми преступлениями, поскольку оно затрудняет использование сложных схем, предназначенных для обхода мер по противодействию (легализации) отмыванию доходов, полученных преступным путем.

Ключевые слова:
киберпреступления,
искусственный интеллект,
финансовые преступления,
финансовые мошенничества,
финансовые технологии,
цифровые финансовые технологии,
большие данные,
финансовая безопасность,
экономическая безопасность

Для цитирования:
Ушвицкий Л. И., Филатова И. В. Влияние цифровых финансовых технологий на экономическую безопасность государства // Экономическая политика и национальная безопасность. 2025. № 1 (1). С. 85–95.

Информация об авторе:
Ушвицкий Л. И. – доктор экономических наук, профессор,
заслуженный деятель науки Российской Федерации
Северо-Кавказский федеральный университет
(Российская Федерация, 355009, г. Ставрополь, ул. Пушкина, д. 1)
директор института экономики и управления
lushvitckii@ncfu.ru
Филатова И. В. – кандидат экономических наук, доцент
Главное управление по работе с личным составом
Министерства внутренних дел Российской Федерации
(Российская Федерация, 119991, г. Москва, ул. Житная, д. 12а)
заместитель начальника отдела организации научной деятельности
образовательных организаций МВД России управления организации
подготовки кадров
irina.filatova-i@yandex.ru

Original article

The article was submitted April 13, 2025;
approved after reviewing May 29, 2025;
accepted for publication July 14, 2025.

Impact of digital financial technologies on the economic security of the state

Lev I. Ushvitsky[1], Irina V. Filatova[2]

[1] North Caucasus Federal University, Stavropol, Russia
[2] Main Directorate for Work with Personnel of the Ministry of Internal Affairs of the Russian Federation, Moscow, Russia

Abstract:
Introduction. The development of financial technologies and the increase in the digitalisation of the economic space have led to a sharp rise in cybercrime. The presence of gaps in legislation negatively affects the effectiveness of proactive and adaptive strategies to counteract such crimes. These trends also contribute to the growth of the shadow economy and tax evasion, which adversely impacts the level of economic security in the country. ***Methods.*** The methodological basis of the study consisted of comparative and retrospective methods. This approach made it possible to identify the specifics of cybercrimes and determine the key directions of countering them by using artificial intelligence technologies. ***Results.*** Ensuring an acceptable level of security for the financial system requires the adoption of a comprehensive strategy based on the use of advanced artificial intelligence and big data technologies. Enhancing the effectiveness of interaction between the state and businesses in identifying and preventing crimes in the financial sphere will ensure the sustainable development of the country's economic system and improve the level of economic security. Expanding international cooperation is a key factor in combating transnational financial crimes, as it complicates the use of complex schemes designed to circumvent anti-money laundering measures.

Keywords:
cybercrime,
artificial intelligence,
financial crimes,
financial fraud,
financial technologies,
digital financial technologies,
big data,
financial security,
economic security

For citation:
Ushvitsky, Lev I., and Irina V. Filatova. 2025. "Vliyaniye tsifrovykh finansovykh tekhnologiy na ekonomicheskuyu bezopasnost' gosudarstva" ["Impact of digital financial technologies on the economic security of the state"] (In Russ.). *Ekonomicheskaya politika i natsional'naya bezopasnost' [Economic policy and national security]* 1, no. 1 (July): 85–95.

Information about the authors:
Ushvitsky L. I. – Doc. Sci. (Econom.), Professor
Honored Scientist of the Russian Federation
North Caucasus Federal University
(1, Pushkin str., Stavropol, 355009, Russian Federation)
Director of the Institute of Economics and Management
lushvitckii@ncfu.ru
Filatova I. V. – Cand. . Sci. (Econom.), Docent
General Directorate for Personnel Management of the Ministry of the Interior of the Russian Federation
(12a, Zhitnaya str., Moscow, 119991, Russian Federation)
Deputy Head of the Department for Organising Scientific Activities of Educational Institutions of the Ministry of the Interior of Russia,
Department of Personnel Training Organisation
irina.filatova-i@yandex.ru

ВВЕДЕНИЕ

Финансовая сфера играет ключевую роль в экономической безопасности государства, обеспечивая стабильность и эффективность бюджетной и налоговой политики.

В современных условиях в России сложилась парадоксальная ситуация: с одной стороны, существующее экономико-правовое регулирование финансовых отношений не справляется с вызовами, связанными с экспоненциальным ростом цифровой экономики (общемировой тренд), с другой – наблюдается избыточное уголовное и административное регулирование. Данное противоречие создает комплексную проблему, от решения которой зависит экономическая безопасность страны.

Актуальность противодействия финансовым преступлениям определяется рядом ключевых факторов:

– стабильность и развитие экономики, а также экономическая независимость страны напрямую зависят от финансовой системы (Решетов, Фунтикова и Дьячкова 2024);

– существующие меры по борьбе с финансовыми преступлениями недостаточно эффективны. Это связано с несовершенством законодательства, аналитического инструментария, используемого контролирующими органами, не успевающего за развитием цифровой экономики, а также нехваткой квалифицированных специалистов (Хабибулин и др. 2024);

– инструменты и методы, используемые правоохранительными органами при расследовании финансовых преступлений, требуют переоценки (Васюков и Старжинская 2024).

Традиционно к категории финансовых преступлений относят (Лапшин 2011):

– преступления, посягающие на финансовые отношения по формированию бюджетных доходов, связанные с уплатой налогов, сборов и таможенных платежей, с незаконным оборотом акцизных и специальных марок, а также товаров и продукции, подлежащих маркировке;

– преступления в сфере государственных расходов, включая кредитование и страхование;

– преступления в сфере банковской деятельности и денежного обращения;

– преступления в сфере валютного законодательства.

Вместе с тем цифровизация экономического пространства создает новые вызовы для борьбы с финансовыми преступлениями. Преступники активно используют новые онлайн-платформы и услуги, что делает способы совершения преступлений более изощренными и разнообразными. При этом, несмотря на технологический прогресс, основные мотивы и цели финансовых преступлений остаются неизменными.

Одновременно развитие новых финансовых технологий, получивших название «финтех», в России кардинально изменило ландшафт финансовой системы, создав бесшовную связь между традиционным банковским обслуживанием и современными цифровыми решениями.

Тем не менее такое стремительное развитие технологий увеличило риски для всех субъектов финансовых отношений в части появления новых видов мошенничества.

МАТЕРИАЛЫ И МЕТОДЫ

Термин «финтех» (сокращение от «финансовые технологии») обычно относится к набору финансовых услуг, предоставляемых с использованием инновационных технологий. Они объединяют несколько базовых цифровых технологий (Свиридов и Некрасова 2019):

– блокчейн;

– машинное обучение;

– облачные вычисления и распределенный реестр;

– искусственный интеллект.

Таким образом, «финтех» можно рассматривать как текущую тенденцию, которую большинство компаний учитывают для улучшения своих бизнес-моделей и оптимизации операций за счет использования дополнительных вычислительных мощностей, активизации обмена информацией, снижения транзакционных издержек, что в конечном итоге позволяет им получить дополнительные конкурентные преимущества. По определению Банка международных расчетов (*BIS*), «*финтех – это технологически реализованные финансовые инновации, которые могут привести к появлению новых бизнес-моделей, приложений, процессов или продуктов с соответствующим существенным влиянием на финансовые рынки и институты, а также предоставление финансовых услуг*»[1].

В последние годы финтех-индустрия в России пережила значительный подъем, вызванный реализацией на федеральном уровне концепции цифрового правительства, широким распространением мобильного интернета и ростом доходов населения (Эскиндаров и др. 2018). Инновационные технологии, такие как мобильные кошельки, цифровые платежные системы, одноранговое кредитование и чат-боты, не только упростили финансовые транзакции, но и расширили спектр инструментов, имеющихся в распоряжении мошенников.

Коллаборации традиционных финансовых учреждений и финтех-стартапов практически полностью изменили экосистему услуг, сделав ее более доступной и адаптируемой к требованиям физических и юридических лиц, пользующихся цифровыми технологиями. Однако, как отмечалось выше, технический прогресс увеличивает риски, связанные с ростом киберпреступлений. Быстрая интеграция цифровых финансовых услуг открыла новые возможности

[1] *Bank for International Settlements* (website). Accessed April 18, 2025. https://www.bis.org/index.htm.

для противоправной деятельности, включая кибермошенничества, незаконное присвоение личных данных, а также отмывание доходов, полученных преступным путем, и финансирование терроризма. В связи с этим быстрый рост финтех-индустрии актуализировал проблему поиска баланса между инновациями и безопасностью.

Истоки финтеха можно проследить до появления ранних компьютерных технологий в середине XX века, которые начали фундаментально преобразовывать методы обработки и управления финансовыми данными (Эскиндаров и др. 2018). В 1960–70-х гг. банки начали использовать мэйнфреймы для управления бухгалтерским учетом и клиентскими транзакциями, заложив основу цифровых финансовых технологий. Появление банкоматов в 1970-х гг. и компьютеризированных торговых платформ в 1980-х гг. стали следующими важными вехами в развитии финтеха. В 1990-х гг. получил развитие интернет, что привело к появлению онлайн-банкинга, позволив пользователям удаленно контролировать свои транзакции. Мобильный банкинг и соответствующие платежные решения были разработаны в начале 2000-х гг. и способствовали фундаментальному изменению того, как люди прибегают к финансовым услугам.

За последние 10 лет экспоненциальный рост финтеха обеспечивался в основном за счет прогресса в области искусственного интеллекта, технологии блокчейн и анализа больших данных. Как стартапы, так и традиционные банковские учреждения используют данные технологии для разработки передовых финансовых товаров и услуг, включая платформы кредитования *P2P*, робоэдвайзеров, криптовалютные биржи и приложения для мобильных платежей.

Таким образом, ключевые достижения финтеха, которые необходимо принимать во внимание при решении проблемы противодействия финансовым преступлениям в контексте обеспечения экономической безопасности, заключаются в следующем:

– технологии искусственного интеллекта автоматизировали процессы и рутинные задачи, что значительно повысило производительность операций, минимизировало влияние человеческого фактора и позволило экспертам акцентировать внимание на более важных обязанностях;

– внедрение облачных вычислений значительно расширило временные и локальные возможности для финансовых компаний, а также сократило их издержки доступа к финансовым данным, поддерживая удаленную работу и улучшая сотрудничество между учреждениями и их клиентами независимо от их местонахождения;

– передовые программные решения в области бухгалтерского учета обеспечивают оптимизацию процессов налогообложения, минимизацию ошибок и сокращение времени, необходимого для соблюдения нормативных требований, что способствует повышению точности и надежности финансовой отчетности;

– мобильные приложения, предназначенные для цифровых платежей, произвели революцию в способах взаимодействия компаний за счет ускорения обмена информацией и снижения необходимости в осуществлении рутинных задач;

– технология блокчейн благодаря своей децентрализованной структуре позволила объединить множество заинтересованных сторон в единую безопасную, прозрачную и неизменяемую базу данных. Это значительно ускорило мониторинг финансовых транзакций, снизило вероятность мошенничества и повысило доверие между участниками за счет обеспечения целостности данных.

С ростом цифровой экономики мошенники все чаще прибегают к классическим схемам Понци и другим финансовым аферам.

Как пример можно привести следующие случаи совершения преступлений:

– криптовалютная пирамида *OneCoin* (ущерб составил около 4 млрд долл.)[2];

[2] Co-Founder Of Multi-Billion-Dollar Cryptocurrency Pyramid Scheme «OneCoin» Pleads Guilty. n.d. "*U.S. Department of Justice*", Washington (website). Accessed April 18, 2025. https://www.justice.gov/usao-sdny/pr/co-founder-multi-billion-dollar-cryptocurrency-pyramid-scheme-onecoin-pleads-guilty.

– крипто-пирамида *BitConnect* (ущерб составил около 2 млрд долл.)[3];
– мошенническая криптосхема *PlusToken* (ущерб составил около 3 млрд долл.)[4].

Злоумышленники привлекают средства под видом перспективных инвестиций (новая криптовалюта, платформа *DeFi*, майнинговая ферма, «инновационный» форекс-фонд) и обещают стабильный высокий доход и выплаты за привлечение новых участников. Пока приток средств продолжается, схема выплачивает «доход» старым вкладчикам за счет новых, создавая иллюзию легитимности. Как только поток денег иссякает, организаторы скрываются с остатком кассы. По мере роста курсов криптовалют в 2017 году и особенно в 2020–2021 гг. крипто-инвестиционные мошенничества вышли на первое место в мире по объемам хищений.

Различные формы мошенничества с платежными инструментами, кредитами и банковскими транзакциями также трансформировались под влиянием технологий. Использование банковских карт остается одной из основных категорий мошенничества. В середине 2010-х гг. во всем мире наблюдалась волна компрометации платежных данных через взломы торговых сетей и установку скиммеров на банкоматы. Однако по мере внедрения чипованных карт (*EMV*) и токенизации платежей (“*card-present*”) фрод-операции стало использовать сложнее (Kovács and David 2016). С 2015 года на первый план вышли операции мошенничества без физического предъявления карты (*CNP fraud*), т. е. с использованием украденных в интернете личных данных. К 2022 году более 80 % всех убытков от карточного мошенничества приходилось на онлайн-транзакции (Bodker et al. 2022). Появилась целая подпольная экономика «дропов» – подставных лиц или адресов, на которые заказываются товары по украденным картам с целью их последующей перепродажи. В ответ были внедрены технологии *3D-Secure* (дополнительная аутентификация покупателя), анализ поведенческих биометрических параметров при платеже и системы ИИ-скоринга транзакций (позволяют в режиме реального времени принимать решение о подозрительности операций) (Martincevich, Črnjević and Klopotan 2020). В результате в 2024 году наблюдалось снижение карточного онлайн-фрода, но в целом масштаб киберугроз в финтехе в мире не снижается (таблица 1). При этом по итогам 2024 года мошенники украли у российских граждан не менее 295 млрд рублей[5].

Таблица 1

Структура киберпреступлений в финансовой сфере в разрезе регионов мира в 2024 г.

Table 1

Structure of Cybercrime in the Financial Sector by Regions of the World in 2024

млрд долл.
billion USD

Вид преступления	Америка	Европа	Азиатско-Тихоокеанский регион
Мошенничество с платежами	102,6	94	190,2
Мошенничество с кредитными картами	13,6	3,1	11,9
Кибермошенничество с использованием интернета	5	3,1	1,9
Мошенничество с трудоустройством	1,6	1,7	0,6
Мошенничество с авансовыми платежами	4,7	8,2	6,2
Мошенничество с выдачей себя за другого человека	1,6	1,4	3,8

Источник: *рассчитано авторами по данным отчета о глобальных финансовых преступлениях*[6].

[3] BitConnect Founder Indicted in Global $2.4 Billion Cryptocurrency Scheme. n.d. “*U.S. Department of Justice*”, Washington (website). Accessed April 18, https://www.justice.gov/archives/opa/pr/bitconnect-founder-indicted-global-24-billion-cryptocurrency-scheme.

[4] The PlusToken Cryptocurrency Scheme: Architecture and Exposure. n.d. “*Okta*”, Las Vegas (website). Accessed April 18, 2025. https://www.okta.com/identity-101/plus-token/ (дата обращения: 18.04.2025).

[5] Сбербанк: по итогам 2024 года мошенники украли у россиян не менее 295 млрд руб. // *Вести.Ру* : [сетевое издание]. URL: https://www.vesti.ru/article/4537994 (дата обращения: 07.06.2025).

[6] Global Financial Crime Report. n.d. “*Nasdaq*”, New York (website). Accessed April 18, 2025. https://static.poder360.com.br/2024/03/relatorio-crimes-financeiros-nasdaq-2024.pdf.

Особого внимания заслуживает мошенничество с личностями и кредитами (*Synthetic Identity Fraud*), которое в настоящее время является самым быстрорастущим видом преступлений в финансовом секторе экономики. Преступники комбинируют реальные и фальшивые данные (например, придумывают несуществующего человека, присваивая ему украденный номер социального страхования) и успешно проходят скоринг в банках, получая кредитные карты и займы и не возвращая их в дальнейшем (Richardson and Waldron 2019). Банки пытаются бороться с преступными схемами, внедряя более тщательную проверку новых клиентов, анализ цифровых следов (например, соответствие *IP*-адреса заявленному городу, проверка истории кредитного бюро и т. д.), однако данные случаи становятся все более частым явлением.

Особенности совершения и специфика противодействия наиболее распространенным видам финансовых киберпреступлений представлены в таблице 2.

Таблица 2

Специфика совершения и противодействия финансовым кибепреступлениям

Table 2

Specifics of Committing and Countering Financial Cybercrime

Схема	Описание	Противодействие
Фишинговые атаки	Получение конфиденциальных данных или выполнение нужных мошеннику действий обманным путем. Используются электронная почта, письма, сайты-клоны, сообщения в мессенджерах	Программы обучения сотрудников, почтовые фильтры, повышение финансовой грамотности населения
Мошенничество с банковскими картами	Компрометация платежных данных через взломы торговых сетей и установку скиммеров на банкоматы	Технология вроде 3D-Secure, анализ поведенческих биометрических параметров, системы AI-скоринга транзакций
Мошенничество с личностью	Комбинирование реальных и фальшивых данных для прохождения скоринга в банках и получения кредитных карт и займов, которые не возвращаются	Особая проверка новых клиентов, анализ цифровых следов, проверка истории кредитного бюро
Внутренние взломы банковских систем	Кража денежных средств или конфиденциальной информации инсайдерами	Усиление требований безопасности к банкам-участникам со стороны SWIFT

Источник: *составлено авторами на основе массива данных научных источников.*

Технологическое противодействие финансовым киберпреступлениям в банках в основном сосредоточено в сфере мониторинга транзакций и реализации мер обеспечения кибербезопасности инфраструктуры.

С позиции комплаенса и регулятивных мер необходимо выделить следующее:

– политика *KYC* (*Know Your Customer*) – идентификация клиентов при открытии счетов, проверке документов и выяснении источников происхождения средств;

– *ongoing monitoring* – постоянный мониторинг активностей клиента на предмет аномальных транзакций;

– мониторинг транзакций – автоматизированные программные комплексы, которые анализируют операции клиентов в режиме реального времени или ретроспективно по заданным правилам и поведенческим паттернам;

– защита собственных систем от взлома – многофакторная аутентификация для доступа к *ERP*-системам, шифрование данных;

– сегментация сетей "*Security Operations Center*" (*SOC*) – центры мониторинга, отслеживающие попытки вторжений, фишинговых атак и т. д.;

– меры онлайн-защиты клиентов, связанные с внедрением токенизации карт, *push*-уведомлений о подозрительных логинах, лимитов на операции по умолчанию, инструментов анализа действий пользователя в интернет-банке;

– защита от инсайдеров и мошенничества сотрудников – системы отслеживания действий персонала, разделение обязанностей, чтобы один сотрудник не мог самостоятельно провести операцию с высоким уровнем риска.

РЕЗУЛЬТАТЫ И ОБСУЖДЕНИЕ

Одним из самых перспективных направлений в борьбе с финансовыми киберпреступлениями считается применение технологий больших данных и искусственного интеллекта. Компании финансового сектора начали активно внедрять их для обнаружения и предотвращения мошенничества, т. к. указанные технологии способны анализировать практически любые объемы транзакций в режиме реального времени, выявляя аномалии, а также обучаться на новых паттернах атак и предсказывать действия злоумышленников.

В глобальном масштабе банки достаточно активно используют ИИ-инструменты – от простых алгоритмов до нейросетей. Согласно исследованию Аль Досари и др., к 2024 году 83 % банков во всем мире применяли машинное обучение для обнаружения финансовых преступлений, около 72 % – технологии обработки естественного языка (например, для анализа текстовых описаний операций), 67 % – методы глубокого обучения (AL-Dosari, Khalifa and Kucukvar 2022).

Банк HSBC совместно с компанией *Google* создал систему искусственного интеллекта под названием "*Dynamic Risk Assessment*" для мониторинга транзакций на предмет финансовых преступлений[7], которая анализирует профили клиентов, связи между счетами, поведение в онлайн-банкинге и выдает динамическую оценку риска операций. *JPMorgan Chase* осуществляет анализ содержания корпоративных переписок с целью выявления признаков попыток мошенничества, используя большие языковые модели (*LLM*)[8]. *Mastercard* в своей системе платежных систем применяет ИИ-алгоритм *Decision Intelligence*, который обрабатывает до 1 триллиона точек данных, чтобы оценить вероятность того, что транзакция по карте является мошеннической. Данный инструмент учитывает максимально широкий спектр информации: от статистики по торговой точке и устройству, до времени суток и ретроспективного поведения держателя карты[9].

В рассмотренных технологиях критически важную роль играют большие данные, так как эффективность ИИ-алгоритмов зависит от количества и качества информации, необходимой для обучения (Sabharwal 2014; Савин и Мурзин 2024). Накопленные массивы транзакций позволяют обучать *LLM*-модели, которые могут выявлять редкие и новые типы мошенничества. Например, модель "*graph analytics*" способна строить социальные графы транзакций с целью выявления сети счетов, через которые проходят денежные средства в рамках схем отмывания доходов, полученных преступным путем, несмотря на то, что каждая транзакция по отдельности не подает подозрительных сигналов (Marasi and Ferretti 2024).

Большие данные также активно используются для поведенческого анализа. Системы мониторинга собирают тысячи параметров о действиях пользователей в мобильном банке (скорость набора текста, угол наклона телефона и пр.), что позволяет ИИ отличить реального пользователя от бота или мошенника, который хоть и знает пароль, но ведет себя иначе.

[7] Harnessing the power of AI to fight financial crime. n.d. "HSBC", UK (website). Accessed April 18, 2025. https://www.hsbc.com/news-and-views/views/hsbc-views/harnessing-the-power-of-ai-to-fight-financial-crime#:~:text=Harnessing%20the%20power%20of%20AI,HSBC%20as%20Dynamic%20Risk%20Assessment.

[8] Fraudulent Email Examples. n.d. "JPMorgan", New York (website). Accessed April 18, 2025. https://www.jpmorgan.com/disclosures/email.

[9] Decision intelligence – Mastercard. n.d. "Mastercard", New York (website). Accessed April 18, 2025. https://b2b.mastercard.com/ai-and-security-solutions/fraud-and-decisioning/decision-intelligence/.

Подобные поведенческие биометрические решения позволяют пресекать фишинговые атаки, когда злоумышленники завладели учетными данными пользователя (таблица 3).

Таблица 3

Примеры использования искусственного интеллекта в противодействии финансовым киберпреступлениям

Table 3

Examples of Using Artificial Intelligence in Countering Financial Cybercrimes

Инструменты	Описание	Примеры
ИИ-платформы для выявления *AML*/фрода	Мониторинг транзакций на предмет финансовых преступлений и динамическая оценка риска операций	Система ИИ "*Dynamic Risk Assessment*", внедренная компаниями *HSBC* и *Google*
LLM-модели анализа корпоративной почты	Анализ содержания корпоративных переписок и выявления признаков попыток мошенничества и фишинга	Система *email-alert*, внедренная банком *JPMorgan Chase*
ИИ-система мониторинга транзакций	Оценивает вероятность того, что транзакция по карте является мошеннической	ИИ-алгоритм "*Decision Intelligence*", используемый компанией *Mastercard*
ИИ-модели графоаналитических связей	Построение социальных графов транзакций для выявления сети счетов, используемых для отмывания доходов	Система анализа больших данных "*Graph analytics*"

Источник: *составлено авторами на основе* (Gargano and Pauwels 2024; Santoso 2024).

Поскольку многие финансовые киберпреступления имеют транснациональный характер, ключевым элементом стратегии борьбы с ними является международное сотрудничество, когда финансовые институты и регуляторы разных стран объединяют усилия, чтобы совместно пресекать мошенничества, отслеживать похищенные средства и привлекать виновных к ответственности.

Обмен данными о киберугрозах в рамках отраслевых организаций, таких как *Financial Services Information Sharing and Analysis Center* (*FS-ISAC*), позволяют банкам в режиме реального времени делиться информацией о новых типах атак, индикаторах компрометации, подозрительных *IP*-адресах и т. д. Например, сообщение о появлении новых фишинговых компаний, нацеленное на клиентов интернет-банкинга, быстро распространяется, и другие банки могут заранее предупредить своих пользователей[10]. В результате заметно повышается скорость реакции на новые угрозы.

Взаимодействие в расследовании конкретных инцидентов особенно актуально для случаев отмывания доходов, полученных преступным путем, через сложные схемы, когда требуется информация из источников в разных юрисдикциях. Для этого существуют *fits – Financial Intelligence Units* (*FIU*), объединенные в Эгмонтскую группу, через которую проходят все отчеты о подозрительных счетах[11]. В результате такая координация помогает выявлять международные преступные сети. Сетевая природа киберпреступлений в финансовой сфере предопределяет важность сотрудничества не только банков и правоохранительных органов, но и криптобирж, аналитических и аудиторских фирм и т. д. Создаются международные коалиции по киберрасследованиям, например, Центральные банки *G7* создали форум *Cyber Expert Group*, где обсуждаются сценарии реагирования на кибератаку, способную вызвать глобальный финансовый кризис.

[10] Navigating Cyber 2024 : Annual Threat Review and Predictions. n.d. "FS-ISAC", Reston (website). Accessed April 18, 2025. https://www.fsisac.com/navigatingcyber2024.

[11] G7 Cyber Expert Group conducts cross-border coordination exercise in the financial sector. n.d. "*European Central Bank*", Frankfurt am Main (website). Accessed April 18, 2025. https://www.bankingsupervision.europa.eu/press/pr/date/2024/html/ ssm.pr240423~0f5ed951ef.en.html.

Однако различия в национальных законодательствах, особенно в сфере защиты персональных данных и финансовой тайны, создают препятствия для международного обмена информацией и затрудняют координацию между странами.

Финансовая тайна также ограничивает объемы информации, которые банк может раскрыть иностранным коллегам. Смягчение и устранение таких барьеров осуществляется в рамках *Financial Action Task Force* (*FATF*), когда можно делиться информацией о клиентах, если это необходимо для предотвращения преступления. На международном уровне многие страны заключают двусторонние соглашения об обмене финансовой информацией.

В результате финансовые институты постепенно переходят от изолированного противостояния киберугрозам к коллективной безопасности. Банки все чаще действуют консолидированно через:

– создание ассоциаций банкиров;
– лоббирование создания общих центров данных о мошенничествах;
– участие в международных операциях;
– обмен лучшими практиками.

Такой подход снижает привлекательность использования транснациональных преступных сетей, а также усложняет перевод финансовых средств в оффшорные юрисдикции.

ЗАКЛЮЧЕНИЕ

Существенным препятствием противодействия финансовым преступлениям в условиях цифровизации экономического пространства является постоянно меняющийся характер киберугроз. Взаимосвязанность цифровых сетей предлагает выгодную среду для квалифицированных преступников, чтобы использовать слабые места финтеха. Растущая сложность фишинговых атак, шпионских программ и программ-вымогателей представляет серьезную угрозу как для потребителей, так и для финансовых учреждений. Из-за больших объемов конфиденциальных и финансовых данных, которыми они управляют, финтех-бизнес становится привлекательной целью для злоумышленников, желающих получить несанкционированный доступ к информации.

Кроме того, стремительная скорость, с которой развиваются технологии, приводит к тому, что в законодательной базе появляются новые пробелы. Отсутствие комплексного нормативного правового регулирования, специально разработанного для финтех-сектора экономики, создает возможности для регулятивного арбитража и не позволяет предотвращать финансовые преступления, используя проактивные или адаптивные стратегии.

В Российской Федерации контролирующие и правоохранительные органы в настоящее время особое внимание уделяют цифровым платежным системам, платформам однорангового кредитования и деятельности по краудфандингу. Данные меры регулирования направлены на:

– гарантирование защиты потребителей;
– обеспечение безопасности данных;
– достижение системной стабильности в финансовой отрасли.

Кроме того, продвижение Центральным банком Российской Федерации технологии Единого платежного интерфейса (*UPI*) и принципа *e-KYC* (знай своего клиента) упростили процесс подключения новых клиентов, повысив эффективность финансовых транзакций и укрепив протоколы безопасности. Введение «нормативных песочниц», которые обеспечивают регулируемую среду для финтех-бизнеса при внедрении новых решений, также демонстрирует прогрессивный подход российских органов власти в продвижении инноваций с одновременным соблюдением строгих правовых ограничений.

Для минимизации рисков и угроз, связанных с преступлениями в финтех-индустрии, необходимо принять совместную стратегию, которая предполагает участие государственных структур, регулирующих органов, финансовых учреждений и специалистов по технологиям. Обмен информацией и сотрудничество способны помочь в создании эффективных контрмер для борьбы с возникающими опасностями. Более того, использование передовых технологий, таких как искусственный интеллект, машинное обучение и блокчейн, может повысить надежность финтех-платформ в борьбе с мошенническими операциями.

Интеграция технологий обнаружения аномалий на основе ИИ может улучшить способность оперативно обнаруживать и предотвращать незаконные транзакции. Блокчейн,

характеризующийся распределенной и неизменной записью, обеспечивает прозрачность и прослеживаемость, что делает его мощным инструментом в борьбе с киберпреступлениями, гарантируя целостность финансовых транзакций. Кроме того, реализация образовательных инициатив среди граждан и кампаний по повышению осведомленности может позволить пользователям выявлять и сообщать о возможных рисках, т. е. способствовать созданию совместной защиты от фишинговых атак и прочих видов мошеннических операций.

Быстрый переход России к цифровизации экономических отношений требует более тщательного рассмотрения взаимозависимости между финансовыми технологиями и киберпреступлениями. Несмотря на то, что достижения финтеха обеспечивают потенциал для экономического расширения прав и возможностей, крайне важно адекватно оценивать опасности, связанные с кибератаками и финансовыми преступлениями. Для обеспечения безопасности финансовой системы необходимо принять комплексную стратегию, которая будет включать в себя прозрачные нормативные рамки, передовые технические решения и совместные инициативы государства и бизнеса, что позволит повысить эффективность функционирования экономической системы страны, а также уровень экономической безопасности.

СПИСОК ИСТОЧНИКОВ / REFERENCES

Васюков В. Ф., Старжинская А. Н. Об оперативно-розыскных и следственных мерах противодействия легализации преступных доходов с использованием криптовалют // *Российское право: образование, практика, наука*. 2024. № 4. С. 68–78. https://doi.org/10.34076/2410-2709-2024-142-4-68-78.

Vasyukov, Vitaly F., and Anna N. Starzhinskaya. 2024. “Ob operativno-rozysknykh i sledstvennykh merakh protivodeystviya legalizatsii prestupnykh dokhodov s ispol'zovaniyem kriptovalyut” [“On operational-search and investigative measures to counter money laundering using cryptocurrencies”] (In Russ.). *Rossijskoe pravo: obrazovanie, praktika, nauka [Russian law: education, practice, science]*, no. 4: 68–78. https://doi.org/10.34076/2410-2709-2024-142-4-68-78.

Лапшин В. Ф. Финансовые преступления в структуре экономических уголовно наказуемых посягательств // *Пенитенциарная наука*. 2011. № 16. С. 9–13.

Lapshin, Valeriy F. 2011. “Finansovyye prestupleniya v strukture ekonomicheskikh ugolovno nakazuyemykh posyagatel'stv” [“Financial crimes in the structure of economic criminal offenses”] (In Russ.). *Penitenciarnaya nauka [Penitentiary science]*, no. 16: 9–13.

Решетов К. Ю., Фунтикова К. В., Дьячкова Д. К. Влияние искусственного интеллекта на трансформацию мировой финансовой системы // *Экономика и предпринимательство*. 2024. № 1 (162). С. 452–458. https://doi.org/10.34925/EIP.2024.162.1.084.

Reshetov, Konstantin Y., K. V. Funtikova, D. K. Dyachkova. 2024. “Vliyaniye iskusstvennogo intellekta na transformatsiyu mirovoy finansovoy sistemy” [“The influence of artificial intelligence on the transformation of the global financial system”] (In Russ.). *E`konomika i predprinimatel`stvo [Economics and entrepreneurship]* 162, no. 1: 452–8. https://doi.org/10.34925/EIP.2024.162.1.084.

Савин С. В., Мурзин А. Д. Системы поддержки принятия решений на базе искусственного интеллекта: интеграция, адаптация и оценка эффективности // *Экономика и управление*. 2024. Т. 30, № 12. С. 1521–1534. https://doi.org/10.35854/1998-1627-2024-12-1521-1534.

Savin, Sergei V., and Anton D. Murzin. 2024. “Sistemy podderzhki prinyatiya resheniy na baze iskusstvennogo intellekta: integratsiya, adaptatsiya i otsenka effektivnosti” [“Decision support systems based on artificial intelligence: integration, adaptation and effectiveness assessment”] (In Russ.). *Ekonomika i upravlenie [Economics and management]* 30, no. 12: 1521–34. https://doi.org/10.35854/1998-1627-2024-12-1521-1534.

Свиридов О. Ю., Некрасова И. В. Тенденции развития финтех-экосистемы в российской экономике // *Вестник Волгоградского государственного университета. Экономика*. 2019. Т. 21, №. 4. С. 197–206.

Sviridov, Oleg Yu., and Inna V. Nekrasova. 2019. “Tendentsii razvitiya fintekh-ekosistemy v rossiyskoy ekonomike” [“Trends in the development of the fintech ecosystem in the Russian economy”] (In Russ.). *Vestnik volgogradskogo gosudarstvennogo universiteta. Ekonomika [Bulletin of the Volgograd State University. Economy]* 21, no. 4: 197–206.

Хабибулин А. Г. Актуальные проблемы формирования знаний для подготовки специалистов-юристов в сфере обеспечения экономической и финансовой безопасности, защиты финансового суверенитета Российской Федерации в условиях трансформации миропорядка / Хабибулин А. Г., Анищенко В. Н., Молчанов А. В., Костюк М. Ф. [и др.] // *Вестник Московского университета. Серия 26: Государственный аудит*. 2024. № 4. С. 27–52. https://doi.org/10.55959/MSU2413-631X-27-15-4-03.

Khabibulin, Alik G. et al. 2024. “Aktual'nyye problemy formirovaniya znaniy dlya podgotovki spetsialistov-yuristov v sfere obespecheniya ekonomicheskoy i finansovoy bezopasnosti, zashchity finansovogo suvereniteta Rossiyskoy Federatsii v usloviyakh transformatsii miroporyadka” [“Actual problems of knowledge formation for the training of legal specialists in the field of ensuring economic and financial security, protecting the financial sovereignty of the Russian Federation in the context of the transformation of the world order”] (In Russ.). *Vestnik Moskovskogo universiteta. Seriya 26: Gosudarstvenny`j audit [Bulletin of the Moscow University]*, 4: 27–52. https://doi.org/10.55959/MSU2413-631X-27-15-4-03.

Эскиндаров М. А. Направления развития финтеха в России: экспертное мнение Финансового университета / Эскиндаров М. А., Абрамова М. А., Масленников В. В., Амосова Н. А. [и др.] // *Мир новой экономики*. 2018. № 12 (2). С. 6–23. https://doi.org/10.26794/2220-6469-2018-12-2-6-23.

Eskindarov, Mikhail A. et al. 2018. "Napravleniya razvitiya fintekha v Rossii: ekspertnoye mneniye Finansovogo universiteta" ["The direction of business development in Russia: the analyst's expert opinion"] (In Russ.). *Mir novoj ekonomiki [The world of new information]* 12, no. 2: 6–23. https://doi.org/10.26794/2220-6469-2018-12-2-6-23.

AL-Dosari K., Fetais N., Kucukvar M. Artificial intelligence and cyber defense system for banking industry: A qualitative study of AI applications and challenges // *Cybernetics and systems*. 2022. № 2 (55). P. 1–29. . https://doi.org/10.1080/01969722.2022.2112539.

AL-Dosari, Khalifa, Noora Fetais, and Murat Kucukvar. 2022. "Artificial intelligence and cyber defense system for the banking industry: qualitative research of AI applications and challenges." *Cybernetics and Systems* 55, no. 2 (August): 1–29. https://doi.org/10.1080/01969722.2022.2112539.

Bodker A. et al. Card-not-present fraud: using crime scripts to inform crime prevention initiatives // *Security Journal*. 2022. Vol. 36, № 4. P. 1–19. https://doi.org/10.1057/s41284-022-00359-w.

Bodker, Amanda et al. 2022. "Card-not-present fraud: using crime scripts to inform crime prevention initiatives." *Security Journal* 36, no. 4 (November): 1–19. https://doi.org/10.1057/s41284-022-00359-w.

Gargano M., Pauwels E. Demography in the next institutional cycle: Preparing the landing space // *Egmont Policy Brief 349*. 2024. 1–6. URL: https://www.jstor.org/stable/resrep67775.

Gargano, Maria, and Emilia Pauwels. 2024. "Demography in the next institutional cycle: Preparing the landing space." *Egmont Policy Brief 349*, (July): 1–6. URL: https://www.jstor.org/stable/resrep67775.

Kovács L., David S. Fraud risk in electronic payment transactions // *Journal of Money Laundering Control*. 2016. Vol. 19, №. 2. P. 148–157. https://doi.org/10.1108/JMLC-09-2015-0039.

Kovács, Levente, and Sandor David. 2016. "The risk of fraud in the implementation of electronic payment transactions." *Journal of Money Laundering Control* 19, no. 2 (May): 148–57. https://doi.org/10.1108/JMLC-09-2015-0039.

Marasi S., Ferretti S. Anti-money laundering in cryptocurrencies through graph neural networks: A comparative study / *2024 IEEE 21st Consumer Communications & Networking Conference (CCNC)*. P. 272–277. https://doi.org/10.1109/CCNC51664.2024.10454631.

Marasi, Simone, and Stefano Ferretti. 2024. "Combating money laundering in cryptocurrencies using graph neural networks: a comparative study." In: *2024 IEEE 21st Consumer Communications & Networking Conference (CCNC)* 272–7 (January). https://doi.org/10.1109/CCNC51664.2024.10454631.

Martinčević I., Črnjević S., Klopotan I. Fintech Revolution in the Financial Industry / *Proceedings of the ENTRENOVA – ENTerprise REsearch InNOVAtion Conference*, Virtual Conference, 10–12 September 2020. Zagreb : IRENET – Society for Advancing Innovation and Research in Economy, 2020. P. 563–571. URL: https://proceedings.entrenova.org/entrenova/article/view/357.

Martincevich, Ivana, Sandra Črnjević, and Igor Klopotan. 2020. "Fintech Revolution in the Financial Industry." In: *Proceedings of the ENTRENOVA – ENTerprise REsearch InNOVAtion Conference* 563–71. Zagreb : IRENET – Society for Advancing Innovation and Research in Economy. https://proceedings.entrenova.org/entrenova/article/view/357.

Richardson B., Waldron D. Fighting back against synthetic identity fraud // *McKinsey on RISK*. 2019. № 7. С. 1–6.

Richardson, Bryan, and Derek Waldron. 2019. "Combating artificial identity fraud." *McKinsey on Risks*, no. 7 (January): 1–6.

Sabharwal M. The use of Artificial Intelligence (AI) based technological applications by Indian Banks // I*nternational Journal of Artificial Intelligence and Agent Technology*. 2014. Vol. 2, № 1. P. 1–5. URL: https://www.researchgate.net/publication/299430567.

Sabharwal, Munish. 2014. "The use of technological applications based on artificial intelligence (AI) by Indian banks." *International Journal of Artificial Intelligence and Agency Technologies* 2, no. 1 (February): 1–5. https://www.researchgate.net/publication/299430567.

Santoso P. A. The Role of Threat Intelligence Sharing in Strengthening Collective Cyber Defense Across Organizations // *Global Research Perspectives on Cybersecurity Governance, Policy, and Management*. 2024. Vol. 8, № 12. P. 24–33. https://hammingate.com/index.php/GRPCGPM/article/view/3/3.

Santoso, Putri A. 2024. "The role of threat information exchange in strengthening collective cyber defense of organizations." *Perspectives of global research in the field of management, policy and rational use of resources in the field of cybersecurity* 8, no. 12 (December): 24–33. https://hammingate.com/index.php/GRPCGPM/article/view/3/3.

Авторами внесен равный вклад в написание статьи.
Авторы заявляют об отсутствии конфликта интересов.

The authors have made an equal contribution to the writing of the article.
The authors declare no conflicts of interests.