БИЗНЕС-ИНФОРМАТИКА

BUSINESS INFORMATICS

Вестник НГУЭУ. 2024. № 4. С. 79–96
Vestnik NSUEM. 2024. No. 4. P. 79–96

Научная статья
УДК 658.511
DOI: 10.34020/2073-6495-2024-4-079-096

ПОСТРОЕНИЕ СИСТЕМ ФРОД-МОНИТОРИНГА: ПОДХОДЫ, МЕТОДИКИ, МОДЕЛИ И ИХ ПРАКТИЧЕСКАЯ РЕАЛИЗАЦИЯ

Крайнов Никита Михайлович[1], Бобров Леонид Куприянович[2]

[1, 2] *Новосибирский государственный университет экономики и управления «НИНХ»*

[1] nikitivich@bk.ru
[2] l.k.bobrov@edu.nsuem.ru

Аннотация. Банки и финансовые организации используют различные программно-технологические решения, направленные на противодействие мошенническим транзакциям, и спектр таких решений достаточно широк. Поскольку ни одно из решений не гарантирует полного исключения разнообразных мошеннических действий, антифрод-системы постоянно развиваются и совершенствуются. В настоящей работе предпринята попытка систематизировать информацию, касающуюся построения систем фрод-мониторинга, выделить основные подходы к созданию таких систем, кратко описать используемые методики и модели, а также представить результаты сравнительного анализа наиболее известных отечественных и зарубежных систем фрод-мониторинга.

Ключевые слова: информационные системы, фрод-мониторинг, проектирование, классификация подходов, методики и модели, примеры антифрод-систем, сравнительный анализ

Для цитирования: Крайнов Н.М., Бобров Л.К. Построение систем фрод-мониторинга: подходы, методики, модели и их практическая реализация // Вестник НГУЭУ. 2024. № 4. С. 79–96. DOI: 10.34020/2073-6495-2024-4-079-096.

Original article

BUILDING FRAUD MONITORING SYSTEMS: APPROACHES, METHODS, MODELS AND THEIR PRACTICAL IMPLEMENTATION

Krainov Nikita M.[1], Bobrov Leonid K.[2]

[1, 2] *Novosibirsk State University of Economics and Management*

[1] nikitivich@bk.ru
[2] l.k.bobrov@edu.nsuem.ru

Abstract. Banks and financial organizations use various software and technology solutions aimed at combating fraudulent transactions, and the range of such solutions is quite wide. But none of the solutions guarantees the complete elimination of various fraudulent activities. Therefore, anti-fraud systems are constantly developing and improving. In this paper, an attempt is made to systematize information regarding the construction of fraud monitoring systems, highlight the main approaches to creating such systems, briefly describe the methods and models used, and also present the results of a comparative analysis of the most well-known domestic and foreign fraud monitoring systems.

Keywords: information systems, fraud monitoring, design, classification of approaches, methods and models, examples of anti-fraud systems, comparative analysis

For citation: Krainov N.M., Bobrov L.K. Building fraud monitoring systems: approaches, methods, models and their practical implementation. *Vestnik NSUEM.* 2024; (4): 79–96. (In Russ.). DOI: 10.34020/2073-6495-2024-4-079-096.

1. Введение

В научной литературе можно встретить множество различных определений термина «фрод-мониторинг» (fraud monitoring), из которых следует, что под фрод-мониторингом принято понимать процесс постоянного автоматического отслеживании финансовых транзакций клиента банка на предмет выявления аномальных или подозрительных операций с целью предотвращения мошеннических действий третьих лиц. Работы по данному направлению ведутся во многих странах мира, о чем свидетельствует поток публикаций, представленных в базе данных Lens[1] (рис. 1).

Тематическое распределение публикаций иллюстрирует рис. 2.

Банки и финансовые организации используют разнообразные программно-технологические решения, направленные на противодействие мошенническим транзакциям, и спектр таких решений достаточно широк. Поскольку ни одно из решений не гарантирует полного исключения разнообразных мошеннических действий, антифрод-системы постоянно развиваются и совершенствуются. В настоящей работе предпринята попытка систематизировать информацию, касающуюся построения систем фрод-мониторинга, выделить подходы к созданию таких систем, кратко описать используемые методики и модели, а также дать обзор наиболее известных отечественных и зарубежных систем фрод-мониторинга.

[1] Lens – крупнейшая в мире общедоступная база данных научных публикаций (более 270 млн работ).

Рис. 1. Публикационная активность стран и регионов (цветовая насыщенность отражает степень публикационной активности)

Publication activity of countries and regions (color saturation reflects the degree of publication activity)

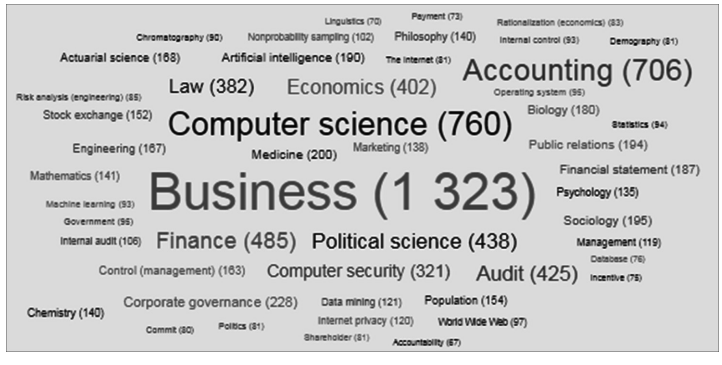

Рис. 2. Тематическое распределение публикаций[2]

Thematic distribution of publications

2. Построение систем фрод-мониторинга: подходы, методики, модели

Можно выделить следующие подходы к построению систем фрод-мониторинга:

– традиционный: исторически первый появившийся подход к реализации мероприятий по предотвращению мошеннических операций, основанный на построении и использовании системы логических ограничений на проведение операций с учетом целей, задач и особенностей мониторинга;

– алертно-традиционный: последующий этап развития традиционных систем, когда в дополнение к логическим ограничениям предусматривается учет информации об инцидентах и новых рисках, поступающей в систему фрод-мониторинга по различным каналам;

[2] Рис. 1 и 2: поиск в БД Lens проводился по запросу (title:(fraud AND monitoring) OR abstract:(fraud AND monitoring) OR keyword:(fraud AND monitoring) OR field_of_study:(fraud AND monitoring)).

– онлайн-скоринг пользователей систем дистанционного банковского обслуживания: предусматривается сбор и анализ общих онлайн-метрик, характеризующих действия клиента в личном кабинете, а также построение правил и условий, свидетельствующих о несоответствии или аномалии в поведении клиента;

– системы с машинным обучением: построение правил мониторинга и идентификация операции, отвечающей тому или иному правилу, происходит на основе алгоритмов машинного обучения;

– смешанные системы: осуществляют комплексные мероприятия скоринга и составления правил мониторинга операций с одновременным применением нескольких подходов, зачастую являются кросс-канальными инструментами мониторинга как онлайн-транзакций, так и оффлайн-операций по банковским картам.

К числу наиболее популярных методик выполнения мероприятий по противодействию мошенничеству можно отнести: профайлинг и безликий профайлинг; методики, основанные на машинном обучении; классификаторы транзакций; методики, предполагающие использование нейронных сетей.

Профайлинг и безликий профайлинг. Профайлинг (англ. «profile» – профиль) – это совокупность психологических методов оценки и прогнозирования поведения человека на основе анализа наиболее информативных частных признаков. Данный инструмент родом из криминалистики, где получил широчайшее развитие и популярность [1]. Можно сказать, что предотвращение финансового мошенничества пролегает рядом с криминалистикой, поэтому не удивительно, что такой популярный инструмент стали применять в современных системах фрод-мониторинга. Однако в отличие от криминалистики, где цель составить профиль конкретных людей, в банковском секторе сохранение персональных данных является важной задачей и использование подобных данных должно производиться с явного разрешения клиента. По этой причине в некоторых системах для анализа операций осуществляется только безликий профайлинг клиентов.

Примером методики создания безликого профиля пользователя (клиента) может служить User and Entity Behavioral Analytics [2, 3]. Данная методика предусматривает сбор сведений о поведении пользователя, а также устройств, приложений и иных объектов в информационной системе (называемых сущностями), для последующего составления профиля нормального поведения клиента (группы клиентов) и сущностей с помощью машинного обучения и статистического анализа. Методики такого рода уже применены в некоторых успешных решениях фрод-мониторинга – Kaspersky Fraud Prevention [4] и IBM Safer Payments [5].

Явный профайлинг реализуется на основе использования симбиоза безликого профайлинга и анализа биометрии клиентов в рамках двухфакторной аутентификации при выполнении каких-либо весомых операций (досрочное закрытие вклада, перевод всего баланса после закрытия вклада и т.п.) для общего анализа или анализа всех операций со счетом по востребованности в индивидуальном порядке. При анализе используется, как правило, голос и лицо, которые проверяются на соответствие и на ориги-

нальность, чтобы исключить применение DeepFake технологий – нейросетей для подмены внешности и/или голоса.

Методики и модели машинного обучения. Фрод-мониториг предполагает обработку больших по объему массивов данных с целью установления имеющихся закономерностей в поведении клиента и своевременного выявления возникающих отклонений от стереотипов его поведения. Для решения этих задач все более активно применяется машинное обучение. На практике различные модели машинного обучения используются в системах фрод-мониторинга как для генерации правил, так и для анализа операций. Некоторые системы ориентированы на симбиозный вариант, когда обе эти задачи решаются одновременно.

В системах, использующих машинное обучение для генерации правил, происходит сбор, обработка и анализ исторических данных для выявления некоего шаблона, который с большой долей вероятности поможет разделить легитимную операцию и мошенническую. Основные методы при генерации правил – кластеризация и регрессионный анализ для выявления соответствия примеров и кластеров данных, а также составления шаблонов «нормализованных» показателей [6, 7].

Системы, использующие машинное обучение для анализа операций, строятся с применением широкого спектра алгоритмов разной направленности и специфики для создания среды анализа операций по четко построенной логике. При этом применяются методы обучения с учителем, без учителя и обучение с подкреплением. В методы обучения с учителем входят алгоритмы: Байеса; опорных векторов; древо решений; k-means; логистическая, линейная и полиноминальные регрессии. В методах обучения без учителя чаще всего применяют алгоритмы: k-средний; DBSCAN; сингулярное разложение; анализ главных компонентов и латентное размещение Дирихле. В обучении с подкреплением применяются Q-обучение, генеративный алгоритм и алгоритм глубоко детерминированного градиента политики. При этом в приложении к задачам фрод-мониторинга может использоваться какой-то один алгоритм, к примеру, описанный в [8], или комплекс алгоритмов машинного обучения, как показано в работах отечественных авторов Т.А. Осиповой [9], Г.С. Ивановой [10], В.К. Вертухова [11], А.В. Власенко [12] и в публикациях зарубежных специалистов [13–15].

Симбиозный вариант предполагает комплексное использование машинного обучения для генерации системы правил и для анализа операций клиента, при этом модели правил и модели анализа взаимодополняют друг друга, что положительно сказывается на дальнейшем обучении и переобучении системы фрод-мониторинга.

Классификаторы транзакций. Классификаторы транзакций имеет смысл рассматривать как отдельную категорию методик (хотя и могут использоваться алгоритмы машинного обучения), потому что здесь прослеживается некая невидимая связующая нить между традиционными системами проверки легитимности банковских транзакций и современными системами фрод-мониторинга. При классификации транзакций (фрод – не фрод) используются статистические модели распознавания образов, где

решающее правило генерируется в результате использования размеченной обучающей выборки исходя из желания минимизировать ошибки первого и второго рода. Несмотря на относительную простоту метода классификации, удается найти настройки системы фрод-мониторинга, когда вероятность отнесения мошеннической транзакции к легальной на всех ступенях проверки будет относительно небольшой, а общее количество оставшихся подозрительных транзакций, подлежащих операторской проверке, будет приемлемым по трудозатратам [16].

Нейронные сети. Применение нейронных сетей в решении задач фрод-мониторинга вызывает большой интерес специалистов и, судя по значительному числу публикаций, сулит многообещающие результаты. В связи с этим активно исследуются различные модели и методы обучения нейронных сетей, позволяющие повысить надежность обнаружения мошеннических действий. Приведем несколько примеров. В работе [17] представлен сравнительный анализ обнаружения мошенничества с кредитными картами с помощью искусственной нейронной сети и иерархической временной памяти, обученной методом имитации отжига. В [18] констатируется значительное повышение идентификации мошенничества в онлайн-платежах при применении глубокой нейронной сети на основе конкурентной роевой оптимизации. В то же время специалисты обращают внимание на необходимость дальнейших углубленных исследований по вопросам использования возможностей нейронных сетей для обнаружения аномалий и прогнозного моделирования в раскрытии скрытых мошеннических действий [19, 20].

3. Примеры реализации систем фрод-мониторинга

Различия в системах фрод-мониторинга (часто называемых антифрод-системами) могут быть следствием не только расхождений в используемых подходах, но вытекать из специфики предмета мониторинга. Пример тому – разные типы транзакций, различные транзакционные схемы, специфические схемы идентификации и подтверждения платежей. Поэтому система, разработанная в одной стране, может не вполне корректно работать в других странах. С учетом этого представляется целесообразным рассмотреть наиболее успешные решения в области фрод-мониторинга, четко разграничив зарубежные и отечественные системы.

Зарубежные системы фрод-мониторинга. *Nice Actimize.* Предложение Nice Actimize, реализованное израильской корпорацией NICE Systems Ltd (рис. 3), является ярким представителем общеаналитического класса платформ и предлагает инструменты по обнаружению и предотвращению мошеннических транзакций в реальном времени. Дополнительно реализован механизм детального расследования случаев отмывания денег, базирующийся на встроенном контроле жизненного цикла отмывания денег. Система предлагает защиту транзакций, проходящих через SWIFT или Wire, быстрых платежей, снятие наличных или оплаты по картам, платежей по счетам, P2P транзакций, а также различных форм переводов внутри доступных на рынках систем [21].

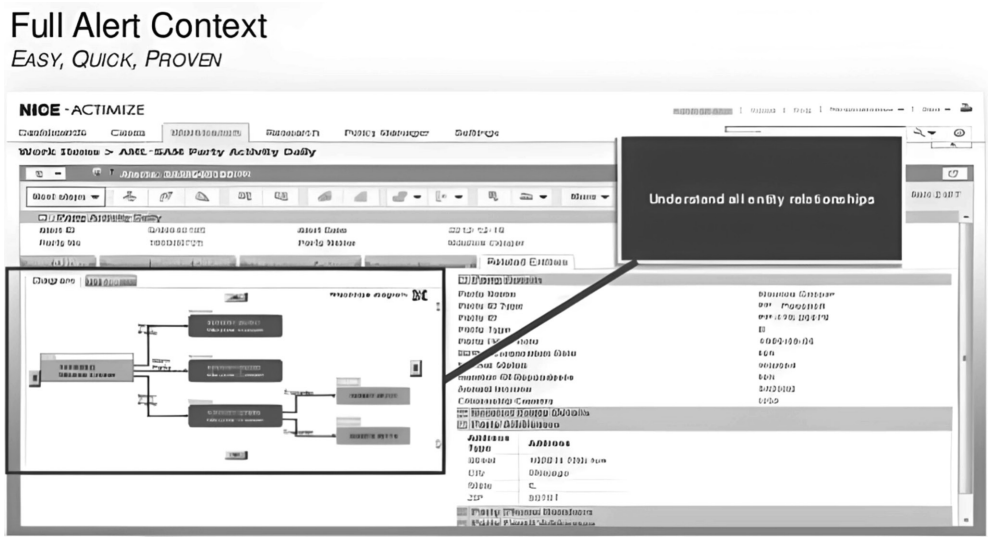

Рис. 3. Интерфейс системы Nice Actimize
Nice Actimize System Interface

Особенности Nice Actimize:

поддержка нескольких аутентификационных каналов для пользователей;

кросс-канальный мониторинг;

защита транзакций на мобильных устройствах, интерактивное голосовое меню в контакт-центрах;

возможность интегрирования в другие системы в качестве облачного сервиса;

применение машинного обучения в создании унифицированных шаблонов.

FICO Application Fraud Manager. Данный продукт компании FICO (рис. 4) представляет собой общеаналитическую платформу, нацеленную на анализ больших массивов данных для выявления скрытых зависимостей

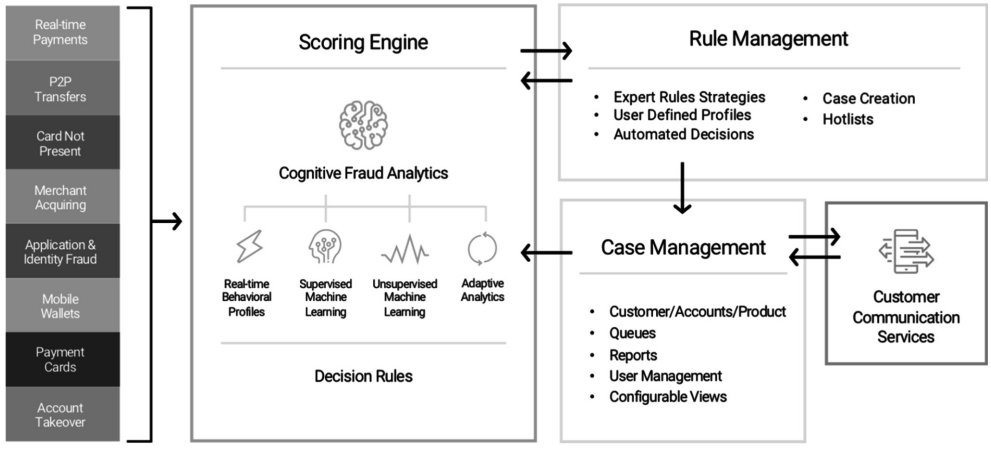

Рис. 4. Система FICO
FICO System

и закономерностей. В рамках этой системы с применением моделей машинного обучения в режиме реального времени реализуется кросс-канальная идентификация операций с целью обнаружения возможных мошеннических действий. Использование этой системы дает возможность пресекать несанкционированные действия третьих лиц, нацеленные на мошенничество со всеми видами эмиссии банковских карт, электронными платежами, депозитными счетами, а также попытки получения мошеннического доступа к платежеспособным учетным записям [22].

К особенностям системы FICO Application Fraud Manager можно отнести, помимо ориентации на технологии машинного обучения, следующее:

применение NLP (Natural Language Processing) алгоритмов распознавания и обработки устной и письменной речи для анализа ссылок и социальных сетей;

возможность расследования инцидентов в отношении ролей пользователей и автоматическое формирование соответствующих отчетов;

возможность использования этой системы как встраиваемого облачного сервиса.

SAS Fraud and Security Intelligence (*SAS FSI*). Кросс-канальная система SAS FSI (рис. 5) ориентирована на работу практически со всеми источниками данных и предотвращение многих видов мошенничества (транзакционного, кредитного, внутреннего и др.) на основе использования технологий машинного обучения. В этой системе, исходя из различных бизнес-ситуаций, пользователь через простой и интуитивно понятный интерфейс может легко осуществлять соответствующую настройку правил. При этом пользователю предоставляется возможность выбора наиболее подходящей на его взгляд обучающей модели и ее тестирования на реальных данных [23].

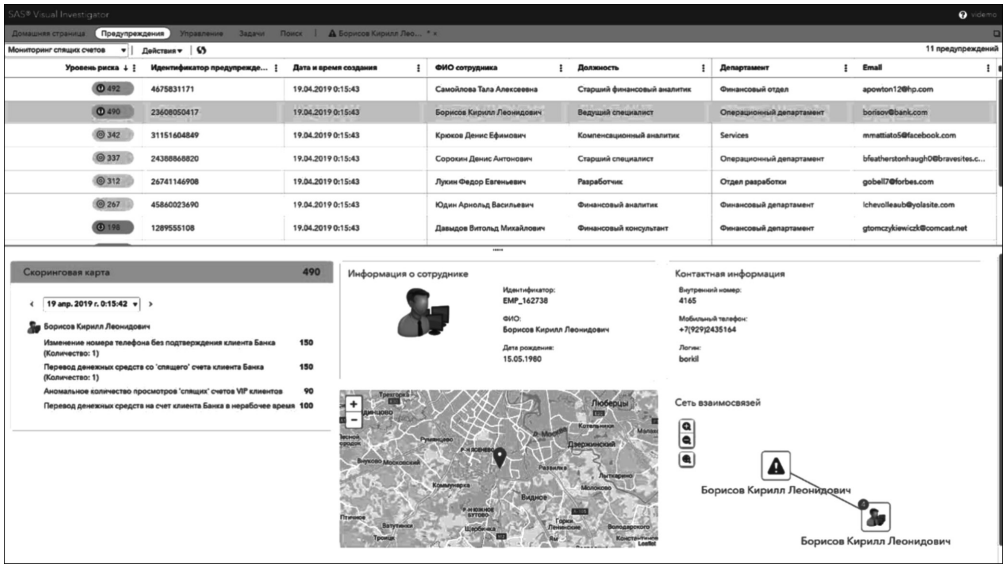

Рис. 5. Интерфейс SAS FSI
SAS FSI Interface

Особенности SAS FSI:

принятие решений за доли секунды;

упрощенная интеграция в бизнес-процессы, сервисы аутентификации и базы данных;

применение самообучающихся нейронных сетей;

многофункциональный конструктор правил;

инструменты по глубокой настройке интерфейса модуля принятия решений под все запросы пользователей и реализации бизнес-процессов по расследованию инцидентов.

IBM Safer Payments. Система IBM Safer Payments (рис. 6) позволяет реализовать многофункциональную защиту клиентов в режиме реального времени не только касательно безналичных платежей через различные системы (банки-эквайеры, «единая европейская зона платежей», чип-пин авторизаций и др.), но и в отношении платежей через торговые терминалы, терминалы снятия наличных и онлайн-банкинг. Поскольку система представляет собой открытую платформу, это позволяет заказчику использовать и собственные модели обнаружения мошеннических действий [5].

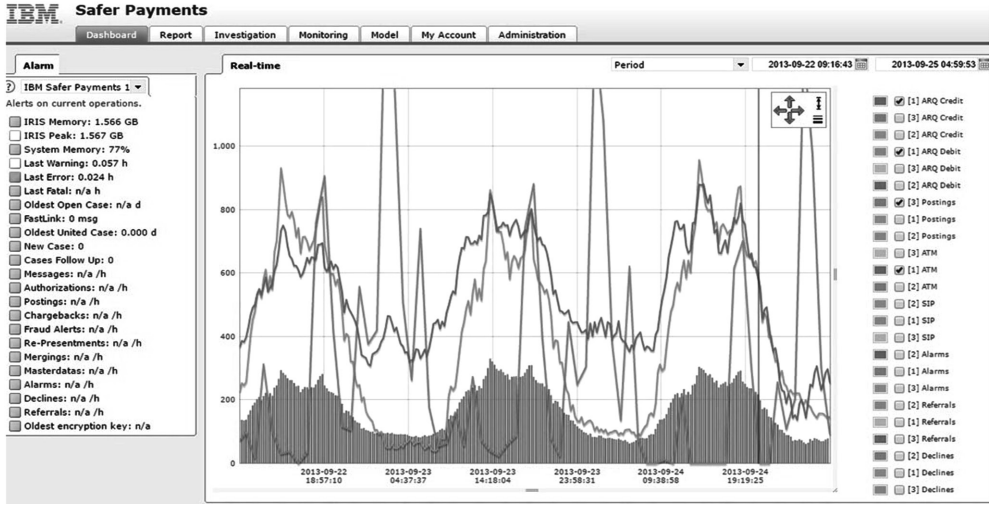

Рис. 6. Интерфейс IBM Safer Payments
IBM Safer Payments Interface

Особенности IBM Safer Payments:

реализация подходов машинного обучения и когнитивных вычислений для фрод-мониторинга;

использование технологий параллельных вычислений для ускорения обработки запросов;

применение профайлинга для создания взаимосвязей и вычисления аномалий.

Российские системы фрод-мониторинга. *OmniReact.* OmniReact [24] – система, созданная компанией Cybertonica (рис. 7) и ориентированная на решение задач скоринга пользователей систем дистанционного банковского обслуживания, мониторинга на базе подходов машинного обучения и

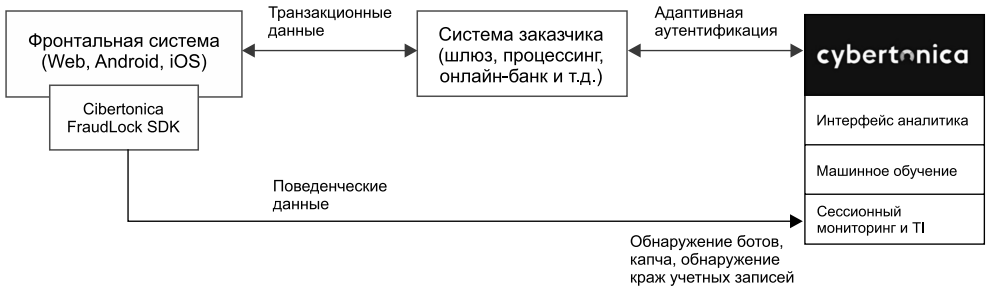

Рис. 7. Система OmniReact
OmniReact System

гибкую генерацию правил. Предусматривается несколько вариантов выработки правил, включая их комбинацию:

задание в явной форме;

выработка правил на основе использования системы балльных оценок;

выбор из готовой библиотеки правил, учитывающих наиболее распространенные угрозы для каждой конкретной отрасли;

генерация правил по результатам машинного обучения на массивах ретроспективной информации.

Kaspersky Fraud Prevention. Лаборатория Касперского в 2014 г. представила новый продукт Kaspersky Fraud Prevention (рис. 8) для борьбы с финансовым онлайн-мошенничеством. Данная система использует поведенческий анализ для выявления отклонений от привычной модели действий пользователя. В ходе сбора и обработки данных формируются шаблоны стандартных и подозрительных действий, которые служат основой для анализа поступающих транзакций в Kaspersky Fraud Prevention. Отличительной чертой стала так называемая поведенческая биометрия, позволяющая фиксировать и устранять угрозы хищения учетных записей или мошеннического доступа к ним, а также действия фишинговых ботов. Используемые технологии подходят для защиты операций как онлайн, так и в различных сервисах мобильного канала, в том числе гейминг [4].

Рис. 8. Система Kaspersky Fraud Prevention
Kaspersky Fraud Prevention System

Особенности Kaspersky Fraud Prevention:

непрерывный поиск и анализ новых, продвинутых схем мошенничества до момента их практической реализации и исполнения соответствующей транзакции в режиме реального времени;

кросс-канальное обнаружение мошенничества;

анализ поведения и биометрии;

использование технологий машинного обучения и поведенческого анализа применяется для идентификации и классификации вредоносных программ, фишинга, атак ботов и т.п.;

глубокий анализ учетных записей пользователей и их устройств.

BI. ZONE Fraud Prevention. Система BI. ZONE Fraud Prevention (рис. 9) состоит из двух модулей:

1) защиты платежных операций;

2) сессионной аналитики и глобального профилирования.

В первом модуле реализована защита практически всех каналов выполнения операций. Она в большинстве своем основана на моделях анализа отклонений в привычном поведении клиента. Для обнаружения и пресечения ложных срабатываний по операциям используются модели машинного обучения. Второй модуль, он же модуль сессионной аналитики, вбирает в себя порядка трехсот индикаторов определения отклонений и явных/неявных аномалий, которые в реальном времени служат основой для анализа транзакций. Вдобавок вторым модулем производится глобальный профайлинг устройства, с которого совершается транзакция. При составлении профиля используется глобальная репутационная база, которая также автоматически обогащается результатами самой системы [25].

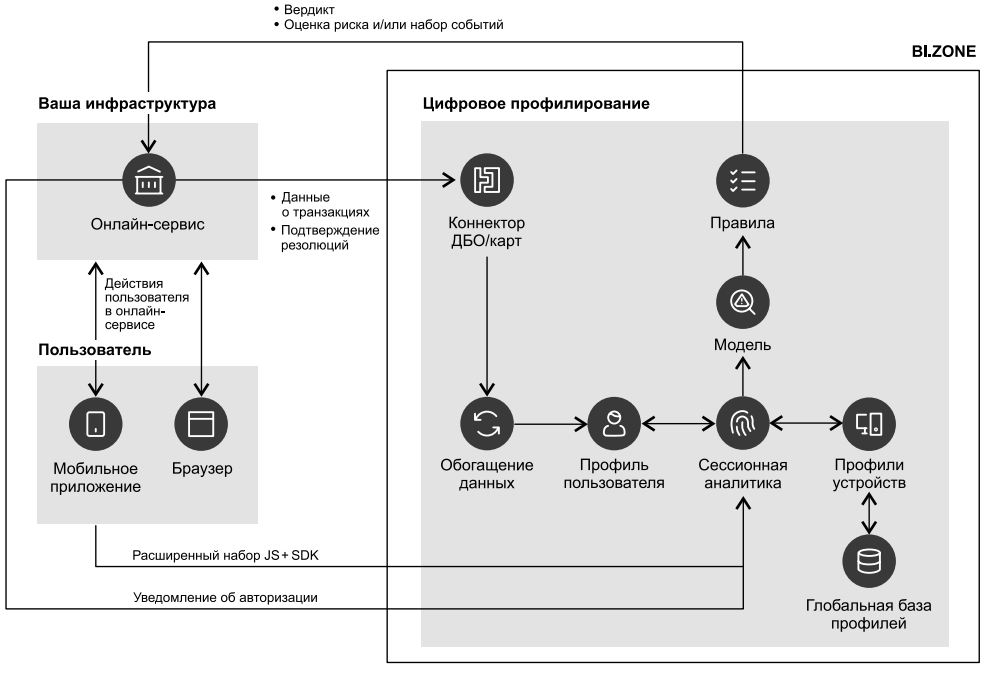

Рис. 9. Система BI.ZONE Fraud Prevention
BI.ZONE Fraud Prevention System

Основные особенности системы:

кросс-канальный мониторинг и анализ транзакций в различных каналах платежей;

анализ транзакций с использованием системы правил и с использованием моделей машинного обучения;

использование алгоритмов машинного обучения и самообучения для автоматической оценки риска по каждой транзакции с учетом настроенных правил, профиля клиента, цифрового «отпечатка» устройства;

использование технологии Risk-Based Authentication (RBA) для интернет-банкинга и мобильного банка;

наличие инструментов разработки мобильных приложений для построения цифровых «отпечатков» устройств.

Сбербанк anti-fraud. Система Sber anti-fraud (рис. 10) предусматривает применение трех классов моделей:

модели классификации поступающих в банк жалоб клиентов на мошеннические действия;

модели обработки больших данных (графовый анализ, эмбеддинг, кластеризация и др.);

модели скоринга транзакций клиентов в реальном времени.

В данной системе осуществляется обработка и анализ всех входящих данных, в том числе оффлайн-оплаты с карт, интернет-покупок, транзакций через мобильный банк, отделения банка и банкоматы: по всем каналам обслуживания проходит более 12 000 операций в секунду [26].

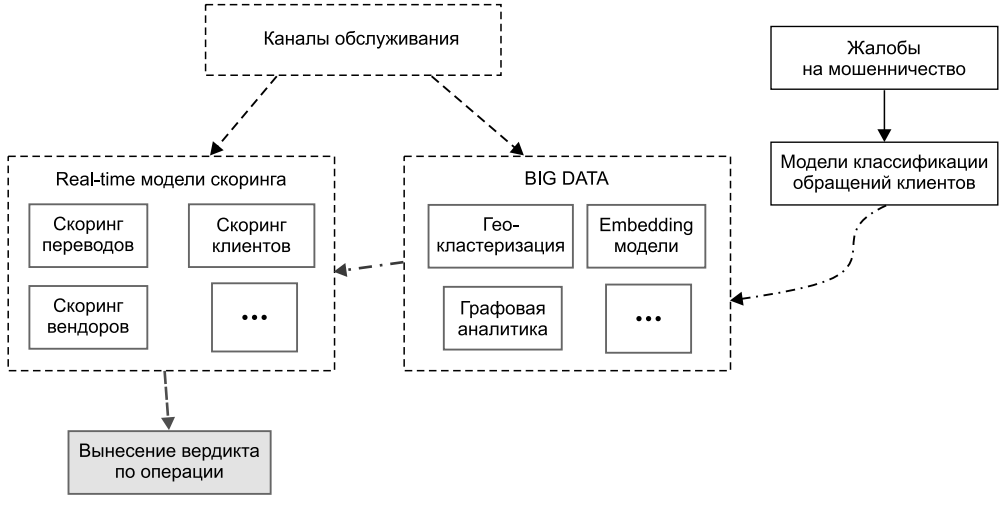

Рис. 10. Система Sber anti-fraud
Sber anti-fraud system

Основные особенности системы Sber anti-fraud:

автоматизация обработки сообщений о мошенничестве с помощью элементов искусственного интеллекта;

применение моделей машинного обучения для составления правил и кросс-канального мониторинга входящих операций;

осуществление безликого профайлинга (составление психологического портрета человека и определения искренности его намерений) на основе результатов анализа больших массивов данных (гео-кластеризация, эмбеддинг, кластеризация);

возможность использовать комбинацию нескольких моделей скоринга для любых транзакций;

непрерывное «самообучение» системы за счет автоматического обогащения новыми данными.

4. Сравнительный анализ систем фрод-мониторинга

Основные характеристики рассмотренных отечественных и зарубежных систем фрод-мониторинга в сравнении с пока еще широко распространенными системами, основанными на построении и использовании системы логических ограничений на проведение операций, приведены в таблице.

Несмотря на то, что цель у всех систем одна – предотвратить мошеннические действия, подходы и методы, присущие каждой системе, могут отличаться. Каждая система по сути своей индивидуальна и не может считаться универсальной для абсолютно каждой финансовой компании. Также немаловажную роль играет и страновая специфика осуществления финансовых операций, которую учитывают антифрод-системы. Поэтому зарубежные системы далеко не всегда применимы в нашей стране, не говоря уже об обратном варианте. Например, при всей схожести характеристик, системы SAS Fraud and Security Intelligence и OmniReact никак нельзя считать полностью тождественными.

Основные характеристики систем фрод-мониторинга
Main characteristics of fraud monitoring systems

Система фрод-мониторинга	Характеристики								
	Применение методов машинного обучения для составления правил	Применение методов машинного обучения для мониторинга	Real-time скоринг при дистанционном банковском обслуживании	Кросс-канальный мониторинг	Real-time фрод-мониторинг	Возможность интеграции в другие системы в виде облачного сервиса	Использование профайлинга в мониторинге и биометрии для идентификации	Мониторинг оффлайн-операций	Наличие конструктора правил
Nice Actimize	✓	×	×	✓	✓	✓	✓	✓	×
FICO Fraud Manager	✓	✓	×	✓	✓	✓	×	✓	×
IBM Safer Payments	✓	×	✓	✓	✓	×	×	✓	×
SAS FSI	✓	✓	✓	✓	✓	✓	✓	✓	✓
OmniReact	✓	✓	✓	✓	✓	✓	✓	✓	✓
Kaspersky Fraud Prevention	×	✓	✓	✓	✓	✓	✓	×	×
BI. ZONE Fraud Prevention	✓	✓	✓	✓	✓	✓	✓	✓	×
Sber anti-fraud	✓	✓	✓	✓	✓	×	✓	✓	×
Традиционная система	×	×	×	×	✓	×	×	✓	✓

5. Заключение

За последнее десятилетие функциональность и гибкость систем фрод-мониторинга значительно усовершенствовались в сравнении с традиционным мониторингом, основанным на системе пополняемых логических правил и ограничений. Это связано как с положительной динамикой случаев мошенничества [27, 28], так и с модернизацией схем и видов мошенничества [29, 30].

На решение масштабных проблем противодействия ущербу от мошеннических действий нацелены кросс-канальные системы фрод-мониторинга, которые работают в режиме 24/7 и выносят вердикты легитимности по транзакциям в режиме реального времени. Методы машинного обучения рассматриваются как перспективный инструмент и все шире внедряются в системы фрод-мониторинга. Они уже не только используются для анализа данных при создании правил, но и привлекаются для непосредственного анализа операций в «real-time» моделях.

Защищенность приходит во все виды операций – от оффлайн-оплаты с банковских карт до дистанционного банковского обслуживания. Одновременно ведутся работы, связанные с повышением гибкости и клиентоориентированности антифрод-систем. Некоторые компании уже предлагают возможность интеграции своих антифрод архитектур в другие системы в виде облачного сервиса, дающего возможность самостоятельно конструировать правила мониторинга даже пользователям, не имеющим опыта разработки автоматизированных систем противодействия мошенничеству.

Можно предположить, что в этих условиях организации, использующие традиционные антифрод-системы, будут предпочитать не полный отказ от своих привычных систем, а комплексные решения, направленные на их расширение и дополнение.

Список источников

1. *Абрамовский А.А*. Профайлинг. Понятие и основные направления в криминалистике // Известия Тульского государственного университета. 2020. № 2. С. 44–56.
2. User Entity and Behavioral Analytics. Энциклопедия Касперского [сайт]. URL: https://encyclopedia.kaspersky.ru/glossary/ueba/ (дата обращения: 11.04.2024).
3. *Ranjan R., Kumar S.S*. User behavior analysis using data analytics and machine learning to predict malicious user versus legitimate user // Decision Analytics Journal. 2022. No. 2 (1). P. 1–10.
4. Kaspersky Fraud Prevention [сайт]. Россия, 2014. URL: https://kfp.kaspersky.com/ru/ (дата обращения: 11.04.2024).
5. IBM Corp. [сайт]. США, 1911. URL: https://www.ibm.com/products/safer-payments (дата обращения: 11.04.2024).
6. *Sardar T.H., Ansari Z*. Partition based clustering of large datasets using MapReduce framework: An analysis of recent themes and directions // Future Computing and Informatics Journal. 2018. No. 3 (2). P. 247–261.
7. *Bhattacharya R., Nagwani N.K., Tripathi S*. A community detection model using node ambedding approach and graph convolutional network with clustering technique // Decision Analytics Journal. 2023. No. 9. P 1–11.

8. *Miguel Ângelo Lellis Moreira, Claudio de Souza Rocha Junior, Diogo Ferreira de Lima Silva, Marcos Alexandre Pinto de Castro Junior, Igor Pinheiro de Araújo Costa, Carlos Francisco Simões Gomes*. Exploratory analysis and implementation of machine learning techniques for predictive assessment of fraud in banking systems // Procedia Computer Science. 2022. No. 1 (214). P. 117–124.
9. *Осипова Т.А., Зайцев К.С., Биферт В.О*. Применение алгоритмов машинного обучения к задаче выявления мошенничества при использовании пластиковых карт // International Journal of Open Information Technologies. 2021. № 1. С. 23–29.
10. *Иванова Г.С., Фокина Ю.О*. Анализ использования алгоритмов машинного обучения в системах фрод-мониторинга // Технологии инженерных и информационных систем. 2022. № 2. С. 121–132.
11. *Вертухов В.К., Ткаченко С.Н*. Использование машинного обучения в системах фрод-мониторинга // Наука, технологии и инновации: тенденции и направление развития: сб. науч. тр. по мат-лам XVI Международного междисциплинарного форума молодых ученых. М.: Профессиональная наука, 2019. С. 24–31.
12. *Власенко А.В., Дзьобан П.И., Жук Р.В*. Обзор инструментов машинного обучения и их применения в области кибербезопасности // Прикаспийский журнал: управление и высокие технологии. 2020. № 1 (49). С. 144–155.
13. *Dornadula V.N., Geetha S*. Credit Card Fraud Detection using Machine Learning Algorithms // Procedia Computer Science. 2019. No. 1 (165). P. 631–641.
14. *Domashova J., Kripak E*. Identification of non-typical international transactions on bank cards of individuals using machine learning methods // Procedia Computer. 2021. No. 1 (190). P. 178–183.
15. *Sadgali I., Sael N., Benabbou F*. Performance of machine learning techniques in the detection of financial frauds // Procedia Computer Science. 2019. No. 1 (148). P. 45–54.
16. *Левашов М.В., Овчинников П.В*. Эффективность классификаторов для выявления фрода в финансовых транзакциях // Вопросы кибербезопасности. 2019. № 5 (33). С. 63–69.
17. Osegi E.N., Jumbo E.F. Comparative analysis of credit card fraud detection in Simulated Annealing trained Artificial Neural Network and Hierarchical Temporal Memory // Machine Learning with Applications. 2021. No. 6. P. 1–10.
18. *Kathikeyan T., Govidarajan M., Vijayakumar V*. An effective fraud detection using competitive swarm optimization based deep neural network // Measurement: Sensors. 2023. No. 27. P. 1–13.
19. *Intissar Grissa, Ezzeddine Abaoub*. Enhancing Fraud Detection in Financial Statements with Deep Learning: An Audit Perspective // International Journal For Multidisciplinary Research. January-February 2024. Vol. 6, issue 1. URL: https://www.ijfmr.com/papers/2024/1/13451.pdf (дата обращения: 23.06.2024).
20. *Patricia Craja, Alisa Kim, Stefan Lessmann*. Deep learning for detecting financial statement fraud // Decision Support Systems. December 2020. Vol. 139. 113421. URL: https://doi.org/10.1016/j.dss.2020.113421 (дата обращения: 23.06.2024).
21. Nice company [сайт]. 1986. URL: https://www.niceactimize.com/ (дата обращения: 02.04.2024).
22. FICO company [сайт]. 1956. URL: https://www.fico.com/ (дата обращения: 03.04.2024).
23. SAS company [сайт]. 1976. URL: https://www.sas.com (дата обращения: 08.04.2024).
24. Cybertonica OmniReact [сайт]. 2015. URL: https://cybertonica.ru/products/omnireact/ (дата обращения: 02.04.2024).
25. BI. ZONE Fraud Prevention [сайт]. 2016. URL: https://bi.zone/catalog/products/antifraud/ (дата обращения: 03.04.2024).
26. Фрод-мониторинг: противодействие мошенничеству. Новостной портал AI RUSSIA [сайт]. 2021. URL: https://ai-russia.ru/library/sber-transaction (дата обращения: 03.04.2024).

27. Мошенники стали чаще атаковать россиян. Аналитический центр НАФИ [сайт]. 2023. URL: https://nafi.ru/analytics/moshenniki-stali-chashche-atakovat-rossiyan/ (дата обращения: 12.04.2024).
28. Потери банков от киберпреступности. TADVISER [сайт]. 2024. URL: https://www.tadviser.ru/ (дата обращения: 12.04.2024).
29. Мошенничество с банковскими картами и платежами. TADVISER [сайт]. 2024. URL: https://www.tadviser.ru/ (дата обращения: 12.04.2024).
30. *Данилова Е.П., Портняга Е.М*. Финансовое мошенничество в современном мире // Siberian Socium. 2023. Т. 7, № 2 (24). С. 67–97.

References

1. Abramovskij A.A. Profajling. Ponyatie i osnovnye napravleniya v kriminalistike [The concept and main directions in forensics], *Izvestiya Tul'skogo gosudarstvennogo universiteta* [*News of the Tula State University*], 2020, no. 2, pp. 44–56.
2. User Entity and Behavioral Analytics [User Entity and Behavioral Analytics]. Enciklopediya Kasperskogo [website]. Available at: https://encyclopedia.kaspersky.ru/glossary/ueba/ (accessed: 11.04.2024).
3. *Ranjan R., Kumar S.S*. User behavior analysis using data analytics and machine learning to predict malicious user versus legitimate user, *Decision Analytics Journal*, 2022, no. 2 (1), pp. 1–10.
4. Kaspersky Fraud Prevention [website]. Rossiya, 2014. Available at: https://kfp.kaspersky.com/ru/ (accessed: 11.04.2024).
5. IBM Corp. [website]. SSHA, 1911. Available at: https://www.ibm.com/products/safer-payments (accessed: 11.04.2024).
6. Sardar T.H., Ansari Z. Partition based clustering of large datasets using MapReduce framework: An analysis of recent themes and directions, *Future Computing and Informatics Journal*, 2018, no. 3 (2), pp. 247–261.
7. Bhattacharya R., Nagwani N.K., Tripathi S. A community detection model using node ambedding approach and graph convolutional network with clustering technique, *Decision Analytics Journal*, 2023, no. 9, pp. 1–11.
8. Miguel Ângelo Lellis Moreira, Claudio de Souza Rocha Junior, Diogo Ferreira de Lima Silva, Marcos Alexandre Pinto de Castro Junior, Igor Pinheiro de Araújo Costa, Carlos Francisco Simões Gomes. Exploratory analysis and implementation of machine learning techniques for predictive assessment of fraud in banking systems, *Procedia Computer Science*, 2022, no. 1 (214), pp. 117–124.
9. Osipova T.A., Zajcev K.S., Bifert V.O. Primenenie algoritmov mashinnogo obucheniya k zadache vyyavleniya moshennichestva pri ispol'zovanii plastikovyh kart [The use of machine learning algorithms for the problem of identifying fraud using plastic cards], *International Journal of Open Information Technologies* [*International Journal of Open Information Technologies*], 2021, no. 1, pp. 23–29.
10. Ivanova G.S., Fokina Yu.O. Analiz ispol'zovaniya algoritmov mashinnogo obucheniya v sistemah frod-monitoringa [Analysis of the use of machine learning algorithms in fraud monitoring systems], *Tekhnologii inzhenernyh i informacionnyh system* [*Technologies of Engineering and Information Systems*], 2022, no. 2, pp. 121–132.
11. Vertuhov V.K. Tkachenko S.N. Ispol'zovanie mashinnogo obucheniya v sistemah frod-monitoringa [The use of machine learning in fraud monitoring systems]. Nauka, tekhnologii i innovacii: tendencii i napravlenie razvitiya: sb. nauch. tr. po mat-lam XVI Mezhdunarodnogo mezhdisciplinarnogo foruma molodyh uchenyh. Moscow: Professional'naya nauka, 2019. Pp. 24–31.
12. Vlasenko A.V., Dz'oban P.I., Zhuk R.V. Obzor instrumentov mashinnogo obucheniya i ih primeneniya v oblasti kiberbezopasnosti [Review of machine learning tools and their

application in the field of cybersecurity], *Prikaspijskij zhurnal: upravlenie i vysokie tekhnologii* [*Caspian Journal: Management and High Technologies*], 2020, no. 1 (49), pp. 144–155.
13. Dornadula V.N., Geetha S. Credit Card Fraud Detection using Machine Learning Algorithms, *Procedia Computer Science*, 2019, no. 1 (165), pp. 631–641.
14. Domashova J., Kripak E. Identification of non-typical international transactions on bank cards of individuals using machine learning methods, *Procedia Computer*, 2021, no. 1 (190), pp. 178–183.
15. Sadgali I., Sael N., Benabbou F. Performance of machine learning techniques in the detection of financial frauds, *Procedia Computer Science*, 2019, no. 1 (148), pp. 45–54.
16. Levashov M.V., Ovchinnikov P.V. Effektivnost' klassifikatorov dlya vyyavleniya froda v finansovyh tranzakciyah [The effectiveness of classifiers for the identification of Frod in financial transactions], *Voprosy kiberbezopasnosti* [*Issues of cybersecurity*], 2019, no. 5 (33), pp. 63–69.
17. Osegi E.N., Jumbo E.F. Comparative analysis of credit card fraud detection in Simulated Annealing trained Artificial Neural Network and Hierarchical Temporal Memory, *Machine Learning with Applications*, 2021, no. 6, pp. 1–10.
18. Kathikeyan T., Govidarajan M., Vijayakumar V. An effective fraud detection using competitive swarm optimization based deep neural network, *Measurement: Sensors.* 2023, no. 27, pp. 1–13.
19. Intissar Grissa, Ezzeddine Abaoub. Enhancing Fraud Detection in Financial Statements with Deep Learning: An Audit Perspective, *International Journal For Multidisciplinary Research*, January-February 2024, vol. 6, iss. 1. Available at: https://www.ijfmr.com/papers/2024/1/13451.pdf (accessed: 23.06.2024).
20. Patricia Craja, Alisa Kim, Stefan Lessmann. Deep learning for detecting financial statement fraud, *Decision Support Systems*, December 2020, vol. 139, 113421. Available at: https://doi.org/10.1016/j.dss.2020.113421 (accessed: 23.06.2024).
21. Nice company [website]. 1986. Available at: https://www.niceactimize.com/ (accessed: 02.04.2024).
22. FICO company [website]. 1956. Available at: https://www.fico.com/ (accessed: 03.04. 2024).
23. SAS company [website]. 1976. Available at: https://www.sas.com (accessed: 08.04. 2024).
24. Cybertonica OmniReact [website]. 2015. Available at: https://cybertonica.ru/products/omnireact/ (accessed: 02.04.2024).
25. BI. ZONE Fraud Prevention [website]. 2016. Available at: https://bi.zone/catalog/products/antifraud/ (accessed: 03.04.2024).
26. Frod-monitoring: protivodejstvie moshennichestvu. Novostnoj portal AI RUSSIA [website]. 2021. Available at: https://ai-russia.ru/library/sber-transaction (accessed: 03.04.2024).
27. Moshenniki stali chashche atakovat' rossiyan [Fraudsters began to attack Russians more often]. Analiticheskij centr NAFI [website]. 2023. Available at: https://nafi.ru/analytics/moshenniki-stali-chashche-atakovat-rossiyan/ (accessed: 12.04.2024).
28. Poteri bankov ot kiberprestupnosti [Bank losses from cybercrime]. TADVISER [website]. 2024. Available at: https://www.tadviser.ru/ (accessed: 12.04.2024).
29. Moshennichestvo s bankovskimi kartami i platezhami [Fraud with bank cards and payments]. TADVISER [website]. 2024. Available at: https://www.tadviser.ru/ (accessed: 12.04.2024).
30. Danilova E.P., Portnyaga E.M. Finansovoe moshennichestvo v sovremennom mire [Financial fraud in the modern world], *Siberian Socium* [*Siberian Socium*], 2023, vol. 7, no. 2 (24), pp. 67–97.

Сведения об авторах:

Н.М. Крайнов – аспирант, Новосибирский государственный университет экономики и управления «НИНХ», Новосибирск, Российская Федерация.

Л.К. Бобров – доктор технических наук, профессор кафедры прикладной информатики, Новосибирский государственный университет экономики и управления «НИНХ», Новосибирск, Российская Федерация.

Information about the authors:

N.M. Krainov – Graduate Student, Novosibirsk State University of Economics and Management, Novosibirsk, Russian Federation.

L.K. Bobrov – Doctor of Technical Sciences, Professor of the Department of Applied Informatics, Novosibirsk State University of Economics and Management, Novosibirsk, Russian Federation.

Вклад авторов: все авторы сделали эквивалентный вклад в подготовку публикации.
Авторы заявляют об отсутствии конфликта интересов.

Contribution of the authors: the authors contributed equally to this article.
The authors declare no conflicts of interest.

Статья поступила в редакцию	*05.09.2024*	*The article was submitted*	*05.09.2024*
Одобрена после рецензирования	*28.09.2024*	*Approved after reviewing*	*28.09.2024*
Принята к публикации	*10.10.2024*	*Accepted for publication*	*10.10.2024*