Петров Александр Васильевич
студент
ФГБОУ ВО «Чувашский государственный
университет им. И.Н. Ульянова»
г. Чебоксары, Чувашская Республика

ИННОВАЦИОННЫЕ МЕТОДЫ ОБНАРУЖЕНИЯ МОШЕННИЧЕСТВА В БАНКОВСКОЙ СФЕРЕ

Аннотация*: рассматриваются методы мониторинга финансовых операций, верификации клиентов, аудита и внутреннего контроля, автоматизации процессов и применения передовых технологий. Подчёркивается значимость комплексного подхода и своевременного внедрения инноваций для обеспечения безопасности банковской системы и противодействия мошенничеству.*

Ключевые слова*: мошенничество, банковская система, верификация клиентов, биометрические технологии, мониторинг подозрительной активности.*

В наше время мошенничество в банковской сфере приобретает всё более сложные и изощрённые формы. Финансовые институты сталкиваются с разнообразными видами мошенничества, такими как кража персональных данных, фиктивные транзакции, легализация доходов, полученных преступным путём, и киберпреступления. Для успешной борьбы с этими проблемами банкам необходимо применять инновационные методы выявления мошеннических действий [2].

Мошенничество в банковской сфере представляет собой противозаконные действия, нацеленные на обман или злоупотребление доверием сотрудников и клиентов банка ради получения нелегальной прибыли. К видам мошенничества в банковской сфере относятся:

– компьютерное мошенничество: использование компьютерных технологий для обмана и кражи средств;

– мошенничество с платёжными картами: подделка, кража или использование чужих платёжных карт;

– мошенничество с банковскими счетами: незаконное получение доступа к чужим банковским счетам;

– мошенничество с кредитами: предоставление ложной информации о себе для получения кредита;

– мошенничество с инвестициями: обман инвесторов с целью получения инвестиций.

Существует множество факторов, которые способствуют мошенничеству в банковской сфере. Среди них можно выделить следующие:

– развитие цифровых технологий и онлайн-банкинга приводит к возникновению новых видов мошенничества, связанных с несанкционированным доступом к информации, средствам и активам банков и их клиентов с использованием разнообразных технологий;

– внутреннее мошенничество представляет собой действия сотрудников банка, нацеленные на незаконное извлечение выгоды за счёт самого банка или его клиентов;

– недостаточная информированность и подготовка персонала, отсутствие знаний о методах мошенничества и способах его предотвращения могут привести к серьёзным последствиям;

– слабая система безопасности, устаревшие или недостаточно защищённые технологии, которые легко взломать, повышают риск мошенничества;

– низкая культура безопасности, когда руководство и сотрудники банка не уделяют должного внимания вопросам безопасности, также способствует мошенничеству;

– недостаточный контроль над операциями, отсутствие мониторинга и анализа операций клиентов и сотрудников банка может привести к утечке конфиденциальной информации и финансовым потерям.

Современные подходы к обнаружению мошенничества основаны на наблюдении за подозрительными действиями, проверке клиентов, аудите и внутреннем контроле, автоматизации процессов, использовании специализиро-

ванного программного обеспечения, методов машинного обучения и искусственного интеллекта, а также биометрических систем.

Мониторинг подозрительной активности включает в себя анализ и отслеживание действий пользователей, клиентов или сотрудников, которые могут свидетельствовать о возможных мошеннических действиях. Этот метод основан на использовании специализированных программных решений и аналитических инструментов.

Программные средства для отслеживания необычных действий используют системы определения отклонений, методы машинного обучения и искусственного интеллекта, а также инструменты для изучения больших объёмов информации. Эти инструменты автоматически распознают сомнительные операции, поведение пользователей или работников и оценивают вероятность мошенничества.

Машинное обучение и искусственный интеллект применяют для разработки моделей поведения пользователей, способных определять аномалии и подозрительные действия. Эти модели обучаются на основе исторических данных о поведении пользователей и могут адаптироваться к изменениям условий и обстоятельств.

Инструменты анализа больших данных помогают находить скрытые закономерности, указывающие на мошенничество. Мониторинг подозрительной активности помогает компаниям вовремя замечать и предотвращать мошенничество, уменьшать финансовые потери и укреплять репутацию.

Верификация клиентов – это проверка личности и платёжеспособности клиентов. Банки должны строго контролировать этот процесс, чтобы не допустить открытия счетов на вымышленные имена и использования банка для отмывания незаконных доходов.

Для проведения верификации клиентов банки используют системы проверки личности, анализируют финансовые документы и справки о доходах. Это позволяет им идентифицировать реальных клиентов и убедиться в их надёжности.

Проверка клиентов нужна, чтобы не допустить отмывания денег и финансирования терроризма. Банки должны следовать законам и правилам международ-

ных организаций, таких как FATF и EAG. Но процесс проверки клиентов может быть сложным и долгим. Банкам нужно тщательно изучать информацию о клиентах и сотрудничать с другими финансовыми учреждениями и госорганами.

Аудит и внутренний контроль способствуют выявлению мошенничества на ранних стадиях, прежде чем оно приведёт к серьёзным убыткам. Они обнаруживают слабые места в системе безопасности, проблемы в процедурах и операциях, а также возможные ошибки в управлении рисками. Во время аудита и внутреннего контроля аудиторы и инспекторы изучают финансовые документы, процессы и системы управления рисками. Они выявляют несоответствия в финансовых операциях и действиях клиентов.

Автоматизация процессов происходит благодаря программному обеспечению, машинному обучению и искусственному интеллекту, которые анализируют большие объёмы данных и находят несоответствия. Это позволяет банкам и другим финансовым организациям обнаруживать подозрительную деятельность и предотвращать мошенничество.

Один из ключевых аспектов автоматизации процессов – отслеживание финансовых операций на предмет необычной активности. Банкам нужно установить системы контроля над транзакциями, изучать частоту и размер операций, а также проверять, соответствуют ли действия профилю клиента и его предполагаемым действиям. Применение программного обеспечения и машинного обучения для обнаружения мошенничества в банковской сфере снижает вероятность ошибочного определения мошенничества и пропуска реальных случаев мошенничества [1].

Основные задачи программного обеспечения для обнаружения мошенничества включают анализ и обработку потоков финансовых и нефинансовых операций, применение бизнес-правил и алгоритмов для обнаружения подозрительной активности, выявление нехарактерных моделей поведения клиентов и сотрудников, а также последовательности событий, обладающих признаками мошенничества.

Машинное обучение значительно снижает процент ложных срабатываний и улучшает обнаружение мошеннических операций. Благодаря использованию алгоритмов машинного обучения можно выявлять сложные взаимосвязи и оперативно обрабатывать значительные объёмы данных [3].

Искусственный интеллект (далее – ИИ) имеет огромное значение в сфере противодействия финансовым преступлениям. Он предоставляет финансовым учреждениям эффективные инструменты для обработки данных, отслеживания операций в режиме реального времени, анализа поведения пользователей и прогнозирования возможных рисков. Благодаря своей способности обрабатывать большие объёмы данных и выявлять закономерности, ИИ помогает предотвращать финансовые преступления.

Основные способы использования искусственного интеллекта:

– анализ данных и распознавание образов: искусственный интеллект анализирует информацию и обнаруживает аномалии, связанные с незаконной деятельностью;

– мониторинг в реальном времени: ИИ отслеживает транзакции в режиме реального времени и генерирует оповещения для проведения расследований;

– поведенческий анализ: искусственный интеллект анализирует поведение пользователей и выявляет нестандартные действия, которые могут свидетельствовать о мошенничестве;

– обработка естественного языка (НЛП): ИИ мониторит и анализирует неструктурированные текстовые данные, выявляя признаки правонарушений;

– машинное обучение для прогнозного анализа: алгоритмы машинного обучения прогнозируют потенциальные финансовые преступления и рекомендуют стратегии снижения рисков.

Список литературы

1. Аркадьева О.Г. Формирование модели государственного регулирования развития технологий искусственного интеллекта в финансовом секторе / О.Г. Аркадьева, Н.В. Березина // Oeconomia et Jus. – 2023. – №4. – С. 12–21. DOI 10.47026/2499-9636-2023-4-12-21. EDN RXEYSM

2. Аркадьева О.Г. Влияние парадигмы безопасности на функции управления финансами / О.Г. Аркадьева // Проблемы обеспечения безопасности: Материалы III Междунар. науч.-практ. конф. – Т. 1. – Уфа: Уфимский гос. авиац. техн. ун-т, 2021. – С. 239–242. EDN LULXZW

3. Белов А.С. Модернизация системы информационной безопасности / А.С. Белов, М.М. Добрышин, Д.Е. Шугуров // Защита информации. Инсайд. – 2022. – №4. – С. 76–80. EDN ZXRAIZ