

ИССЛЕДОВАНИЕ ВОЗМОЖНОСТЕЙ ИНТЕГРАЦИИ ИСКУССТВЕННОГО ИНТЕЛЕКТА И ТЕХНОЛОГИИ БЛОКЧЕЙН В БАНКОВСКИЕ СИСТЕМЫ ВЫЯВЛЕНИЯ МОШЕННИЧЕСКИХ ТРАНЗАКЦИЙ

Федосенко М.Ю. (Федеральное государственное автономное образовательное учреждение высшего образования "Национальный исследовательский университет ИТМО")

Научный руководитель – к.т.н., доцент (квалификационная категория "ординарный доцент") Менщиков А.А. (Федеральное государственное автономное образовательное учреждение высшего образования "Национальный исследовательский университет ИТМО")

В докладе рассматривается проблематика оптимизации процесса идентификации мошеннических действий в системах банковского дистанционного обслуживания. Описывается значимость интеграции в банковские системы моделей злоумышленников и жертв мошенничества, возможности осуществления качественной апробации платёжной информации вычислительными средствами. В работе рассматриваются действия по интеграции систем обнаружения банковского мошенничества с такими перспективными направлениями компьютерных технологий как машинное обучение, большие данные, блокчейн.

Введение. Мошенничество в финансовой сфере имеет место быть с самого начала развития товарно-денежных отношений и развивалось совместно с историческим развитием технологий. Один из наиболее значимых этапов развития финансового мошенничества приходится на становление возможности осуществления электронных платежей. Это связано с упрощением процесса аутентификации и идентификации плательщика, наличием уязвимостей в используемых электронных платёжных системах, слабой осведомлённостью пользователей в вопросах кибербезопасности и действий мошенников. Банковские организации уже внедряют различные программные компоненты противодействия мошенничеству в банковские системы дистанционного обслуживания. Данные компоненты называются антифрод системами и представляют собой совокупность решений по обработке информации, мониторингу и аналитике событий. Актуальность исследования, осуществлённого в рамках доклада, заключается в выявлении направлений по оптимизации работы систем идентификации мошеннических транзакций при использовании современных научно-технических решений.

Основная часть. В последние годы увеличение числа мошеннических действий в электронных платежах тесно связано с пандемией и стремительным развитием на её фоне онлайн торговли. В результате чего происходит увеличение объёма обрабатываемой платёжной информации, что в свою очередь приводит к увеличению нагрузки на вычислительные ресурсы системы. При всём при этом, банковская система выявления и предотвращения мошенничества должна обеспечивать высокую точность идентификации мошеннических транзакций в допустимые временные промежутки, при наличии должного уровня отказоустойчивости и защищённости системы. Вопрос увеличения точности верной идентификации типа транзакции способна решить интеграция методов машинного обучения в процессы работы банковских систем. Однако имеется необходимость в проработке вопроса возможности работы систем с большими объёмами данных пользовательских транзакций. Обработка больших данных позволяет строить более точные поведенческие модели мошенников и их действий, которые способны увеличить точность работы всей системы. Однако следствием интеграции машинного обучения и больших данных в работу системы противодействия мошенничеству является увеличение нагрузки на вычислительные ресурсы, в связи с чем увеличиваются риски отказоустойчивости и защищённости системы. Данную

проблему способна решить грамотно разработанная методика тестирования, включающая в себя модульное, интеграционное, функциональное, системное тестирования, а также методика безопасной разработки и защиты системы от актуальных угроз, основанная на методологии уязвимостей OWASP Top-10.

Постепенное усложнение внутреннего устройства рассматриваемых систем и наличие угроз обеспечения доступности и конфиденциальности приводит к задаче исследования возможности реализации системы на распределённой технологии блокчейн. Данная технология представляет собой децентрализованную систему, отличную от классической клиент-серверной архитектуры, позволяющая распределить обрабатываемую информацию между всеми участниками, обеспечив им при этом равный доступ к процессам. Ключевым преимуществом технологии является защищённость обрабатываемых данных при помощи криптографических алгоритмов и смарт-контрактов. Современный опыт работы научно-исследовательских институтов и крупных компаний демонстрирует, что блокчейн активно применяется не только в криптовалюте, но и в производственной и финансовой сфере. Российскими учёными уже разработаны собственные блокчейн-платформы Мастерчейн, Waves Enterprise, которые являются сертифицированными ФСБ РФ для работы с персональными данными, платежами, юридически важной информацией. Данные платформы постепенно внедряются для работы с документооборотом в Сбербанке, Альфа банке, банке Тинькофф и т.д., для обеспечения логистики в Норильском никеле, Газпроме, Авиакомпаниях Сибирь. Также, данные компании ведут собственные разработки платформ и их использования для реализации единых информационных систем.

Вывод. Таким образом, основными направлениями в исследовании возможностей улучшения работы банковских систем выявления мошенничества являются работы по оптимизации используемых вычислительных ресурсов, уменьшению временных показателей работы системы, увеличению вероятности верной идентификации, уменьшению числа ошибочно идентифицированных или упущенных случаев мошенничества, обеспечению целостности обрабатываемых данных и отказоустойчивости систем. Все эти задачи позволяет решить применение таких современных технологий, как машинное обучение, большие данные, блокчейн. Однако процесс их внедрения является сложным, многоэтапным, требует тщательного исследования и проработки, поскольку улучшение точности приводит к увеличению нагрузки на систему.

Также, немаловажной задачей является качественное выявление мошеннических действий при постинцидентных расследованиях, среди юридических лиц и государственных служащих, поскольку данные варианты наносят значительный ущерб для финансовых организаций и государства в целом.

Федосенко М.Ю. (автор)

Подпись

Менщиков А.А. (научный руководитель)

Подпись