Секция «Современные вызовы и угрозы международной безопасности»

Роль бизнеса в противодействии финансированию терроризма: методы, инструменты и успешные практики

Научный руководитель – Бажуков Владимир Иванович

Тымченко Оксана Витальевна
Студент (магистр)
Московский государственный университет имени М.В.Ломоносова, Факультет глобальных процессов, Москва, Россия
E-mail: ksyusha.tymchenko@mail.ru

Механизмы, применяемые бизнесом, опираются на современные технологии, возможности искусственного интеллекта и машинного обучения, блокчейн-системы.

Программы мониторинга транзакций фильтруют операции на признаки, которые свойственны нелегальным транзакциям — переводы крупных сумм, частые транзакции в зоны и страны «высокого финансового риска», а также переводы лицам и организациям, находящимся под международными санкциями. Примером подобной программы может служить платформа «NICE Actimize». [1]

Блокчейн-аналитика вошла в инструментарий бизнес-структур из-за активного использования криптовалют террористическими организациями и радикальными группировками. К примеру, на базе платформы Chainalysis работает система «Alternia», которая использует искусственный интеллект для выявления мошеннических операций на криптовалютных биржах, отслеживания денежных средств в токенах, а также выявляя вовлеченных контрагентов. [2] Сервис Elliptic предлагает клиентам услугу проверки криптокошельков с помощью механизма Elliptic Lens. [3]

Китайская компания Alibaba является одной из крупнейших технологических платформ электронной коммерции в мире. Для предотвращения финансовых преступлений корпорация использует искусственный интеллект, анализ больших данных в рамках мониторинга транзакций через свою платежную систему Alipay, входящую в компанию «Ant Group».

ПАО «Сбербанк» реализует несколько программ по минимизации рисков: в 2024 году Сбер ввел новую антифрод систему, направленную на усиление безопасности операций и оперативное выявление подозрительных транзакций. Система Plarform V DataGrid хранит информацию обо всех финансовых операциях, использует искусственный интеллект для проверки транзакций. [4] Платформа X Threat Intelligence от Сбера представляет собой передовой механизм управления киберугрозами, который осуществляет мониторинг уязвимостей и предоставляет бизнесу доступ к аналитике о подозрительных операциях с использованием ИИ. [5]

Современные технологии являются фундаментальной частью противодействия финансированию терроризма, поскольку они позволяют автоматизировать ручные процессы мониторинга и анализа транзакций, более оперативно и точно выявлять подозрительные операции и минимизировать риски, связанные с человеческим фактором.

Источники и литература

1) Complete Financial Crime and Compliance Coverage // Nice Actimize URL: https://www.niceactimize.com/xceed/aml/ (дата обращения: 07.02.2025 г.)
2) Chainalysis Acquires Alterya // Chainalysis URL: https://www.chainalysis.com (дата обращения: 07.02.2025 г.)

3) Crypto Wallet Screening with Elliptic Lens // Elliptic URL: https://www.elliptic.co/platform/lens (дата обращения: 07.02.2025 г.)
4) Как российское ПО позволяет осуществлять фрод-мониторинг в режиме реального времени // Platform V URL: https://platformv.sbertech.ru/blog/kak-rossijskoe-po-pozvolyaet-osushhestvlyat-frod-monitoring-v-rezhime-realnogo-vremeni (дата обращения: 13.02.2025 г.)
5) ИНТЕЛЛЕКТУАЛЬНАЯ ПЛАТФОРМА УПРАВЛЕНИЯ КИБЕРУГРОЗАМИ // ПАО Сбербанк URL: https://www.sberbank.ru/promo/xti (дата обращения: 26.02.2025 г.)