Научная статья
Original article
УДК 33

АВТОМАТИЗАЦИЯ ПРОЦЕССОВ ФРОД-МОНИТОРИНГА ТРАНЗАКЦИЙ КОММЕРЧЕСКОГО БАНКА

AUTOMATIZATION OF FRAUD-MONITORING PROCESS IN COMMERCIAL BANK

Киселев Илья Игоревич, студент 2 курс, кафедра «Прикладная информатика», МИРЭА – Российский технологический университет, Россия, г. Москва
Одинцова Мария Александровна, кандидат экономических наук, доцент Доцент кафедры «Практической и прикладной информатики», МИРЭА – Российский технологический университет, Россия, г. Москва

Kiselev Ilya Igorevich, 2nd year student, Department of Applied Informatics, MIREA - Russian Technological University, Russia, Moscow
Odintsova Maria Alexandrovna, Candidate of Economic Sciences, Associate Professor, Associate Professor of the Department of Practical and Applied Informatics, MIREA - Russian Technological University, Russia, Moscow

Аннотация: В статье рассматриваются процессы фрод-мониторинга банковских транзакций на примере коммерческого банка. Рассмотрено понятие фрод-мониторинга. Проанализирована законодательная база Российской Федерации в части регулирования процессов противодействия мошенничеству. Представлены современные информационные системы и

сервисы отечественного и зарубежного рынка, позволяющие осуществлять мониторинг банковский операций. Рассмотрен вариант использования одного из ИТ-решений — IBM Safer Payments. Приведен пример ИТ-инфраструктуры для реализации процесса фрод-мониторинга. Сделаны выводы о необходимости непрерывного совершенствования процессов и систем фрод-мониторинга.

Summary: The article deals with the processes of fraud monitoring of banking transactions using the example of a commercial bank. The concept of fraud monitoring is considered. The legislative base of the Russian Federation has been analyzed in terms of regulating the processes of combating fraud. Modern information systems and services of the domestic and foreign markets are presented, which allow monitoring banking operations. Considered the option of using one of the IT solutions - IBM Safer Payments. An example of an IT infrastructure for the implementation of the fraud monitoring process is given. Conclusions are drawn about the need for continuous improvement of fraud monitoring processes and systems.

Ключевые слова. Антифрод, фрод-мониторинг, ИТ-инфраструктура, противодействие мошенничеству.

Key words. Antifraud, fraud-monitoring, IT-infrastructure, fraud defense.

Введение

Банковскими услугами ежедневно пользуются миллионы людей. При этом наиболее остро стоит проблема защищенности банковских транзакций и разработка мер, направленных на обеспечение их максимальной защиты от мошенничества. Для достижения этих целей коммерческие банки создают специальные подразделения — отделы по противодействию мошенничества — отделы антифрода. В задачи таких отделов входит мониторинг банковских транзакций, разработка мер, направленных на выявление, анализ мошеннических операций и их возможное предотвращение. Для поддержки этих задач в отделах антифрода разрабатываются и используется специальные

информационные системы (ИС) — системы антифрода или системы фрод-мониторинга.

Противодействие мошенничеству как необходимая часть работы коммерческого банка

Необходимость коммерческих банков противостоять мошенникам зафиксирована на законодательном уровне, в таких законах как 115-ФЗ «Федеральный закон о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» от 7 августа 2001 года [https://static.qiwi.com/ru/doc/fz-115.pdf] и 161-ФЗ «О национальной платежной системе», от 27 июня 2011 года [https://static.qiwi.com/ru/doc/fz-161.pdf] статья 27 которого направлена на совершенствование информационного взаимодействия Банка России и МВД России по вопросам, связанным с возбуждением и расследованием уголовных дел по фактам мошенничества при осуществлении переводов денежных средств. 115-ФЗ предполагает ответственность банков перед законом за игнорирование или несоблюдение требований ЦБ в части предотвращения мошеннических действий. Требования законодательства, а также необходимость защиты своей деятельности обязывает все банки к созданию отделов по противодействию мошенничеству.

В состав отделов по противодействию мошенничеству коммерческого банка могут входить аналитики, специалисты, разработчики программного обеспечения. Деятельность сотрудников направлена на тщательный мониторинг банковских транзакций, а также на создание и поддержку функционирования информационных систем, осуществляющих такой мониторинг. Потребности в новых системах и сервисах возникают постоянно, так как мошенники используют все более изощренные схемы мошенничества, что требует не менее изощренной логики на стороне антифрода для предотвращения мошенничества с их использованием.

Понятие фрод-мониторинга

Фрод (с англ. fraud «обман») — это операции, связанные с мошенническими действиями.

Антифрод (от англ. anti-fraud «борьба с мошенничеством»), или фрод-мониторинг — система, предназначенная для оценки финансовых и не финансовых событий (карточных транзакций, действий пользователя в дистанционном банковском обслуживании, операций с баллами лояльности др.) на предмет подозрительности с точки зрения мошенничества и предлагающая рекомендации по их дальнейшей обработке. Как правило, система антифрода состоит из стандартных и уникальных правил, фильтров и списков, по которым и проверяется каждая транзакция.

В общем случае, процесс фрод-мониторинга представляет собой проверку банковской транзакции на признаки мошенничества, с блокировкой или приостановкой с последующим расследованием в случае обнаружения таковых признаков в конкретной транзакции.

Системы фрод-монитроинга

На сегодняшний день на отечественном рынке наиболее известны следующие системы фрод-мониторинга:

- Safer Payments от IBM – Наиболее популярное решение для реализации фрод-мониторинга банковских транзакций. Используется концепция работы, основанная на загружаемых правилах, в которых описаны в формализованном виде условия блокировок получаемого трафика. Система давно представлена на рынке и хорошо себя зарекомендовала, хоть она и является самой дорогой по стоимости обслуживания системой фрод-мониторинга.
- TranzWare Fraud Analyser от Compass Plus Technologies – система была представлена на рынке с 2003 года и продолжает свою работу до настоящего момента. Архитектура системы также построена на основе Rule-based подхода, но не получила такого широкого распространения как решение от IBM.

- Smart Fraud Detection от Российской компании Fuzzy Logic Labs – Отечественная система фрод-мониторинга появившаяся на рынке с 2016 года. Система работает в автономном режиме, используя алгоритмы машинного обучения для противодействия мошенническим операциям.

Автоматизация процессов фрод-мониторинга банковских транзакций на базе решения Safer Payments

Для автоматизации процессов фрод-мониторинга транзакций коммерческие банки не редко используют распространенное коробочное решение от IBM — Safer Payments. Пример ИТ-инфраструктура коммерческого банка с его использованием представлен на Рисунке 1. Модель ИТ-инфраструктуры банка выполнена в нотации ArchiMate 3.0 с использованием облачного программного средства Visual Paradigm Online.

Нотация ArchiMate 3.0 позволяет представить ИТ-архитектуры компании в виде слоев, как с точки зрения бизнес-логики, так и с точки зрения используемых ИТ решений. В данном случае, на диаграмме представлена архитектура в трех разрезах: бизнес-слой, слой приложений и технический слой. Если рассматривать архитектуру в общем виде, можно выделить три блока инфраструктуры — это платформа онлайн-банка, отвечающая за работу сервисов банка и взаимодействие с клиентами, процессинг, отвечающий за обработку платежей, и система фрод-мониторинга, направленная на противодействие мошенничеству на платформе банка.

В процессе мониторинга банковских транзакций IBM Safer Payments ИС получает от процессинга транзакцию для проверки, исполняет проверочные алгоритмы — правила, заложенные аналитиками банка с использованием внутреннего хранилища информационной системы. В результате этого ИС получает вердикт по транзакции, это может быть BLOCK — блокировка транзакции, HOLD — приостановка транзакции, OK — проведение транзакции. При получении вердикта приостановки транзакции создается инцидент, который в дальнейшем обрабатывается специалистом. ИС уведомляет процессинг о приостановке проведения транзакции. Специалист

собирает дополнительные сведения, и, при необходимости, связывается с клиентом для уточнения информации или разъяснения происходящего. В конечном счете, специалист принимает решение: провести транзакцию или заблокировать проведение. Решение указывается в инциденте, после чего последний закрывается. В результате чего у ИС появляется информация об одном из финальных решений — BLOCK или OK, который отправляется в процессинг в качестве ответа.

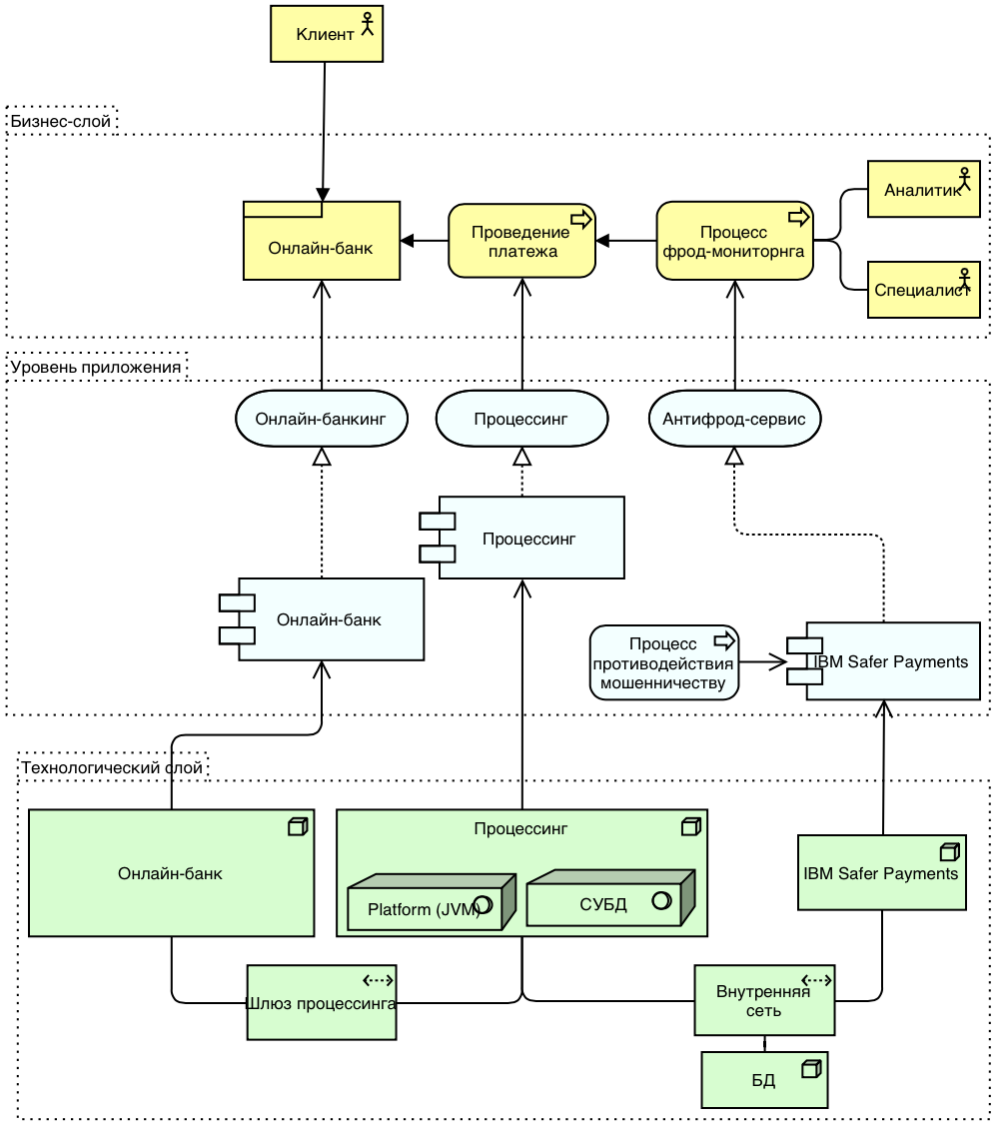


Рисунок 1 — ИТ-архитектура коммерческого банка

Использование рассмотренного программного средства позволяет добиться поставленных целей, а именно осуществить мониторинг банковских транзакций. Однако, данная система не лишена недостатков. Среди таковых следует отметить довольно низкое быстродействие, являющееся причиной

возможной невысокой скорости расследования инцидентов. К тому же мошенники всегда совершенствуют свою работу и находят новые способы обхода препятствий. Таким образом, задача качественной автоматизации процессов фрод-мониторинга является актуальной и весьма важной в деятельности коммерческого банка.

Заключение

Защита банковских транзакций является важной задачей в работе любого коммерческого банка. Для ее выполнения банки создают специальные подразделения — отделы антифрода или фрод-мониторига, которые в свою очередь разрабатывают, внедряют информационные системы противодействия мошенничеству — системы антифрода. Для стабильного и безопасного функционирования любого коммерческого банка такие системы должны постоянно обновляться и совершенствоваться, чтобы максимально обезопасить свою работу и не подвергать рискам средства своих клиентов.

Список использованных источников

1. ГОСТ Р 7.0.97-2016 — «Система стандартов по информации, библиотечному и издательскому делу. Организационно-распорядительная документация. Требования к оформлению документов» (ред. от 14.05.2018) [Интернет-ресурс] // URL: https://www.internet-law.ru/gosts/gost/63653. (дата обращения: 09.03.2022).
2. Давид Марка, КлементМакГоуэн, Методология структурного анализа и проектирования. Пер. с англ. М.:1993, 240 с., ISBN 5-7395-0007-9.
3. 115-ФЗ «Федеральный закон о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» от 7 августа 2001 года // https://static.qiwi.com/ru/doc/fz-115.pdf (Дата обращения: 13.03.2022).
4. 161-ФЗ «О национальной платежной системе», от 27 июня 2011 года // https://static.qiwi.com/ru/doc/fz-161.pdf (Дата обращения: 15.03.2022)

5. Нотация ArchiMate 3.0 [Интернет-ресурс] // https://pubs.opengroup.org/architecture/archimate3-doc/ (Дата обращения: 15.03.2022).
6. Простейшие методы прогнозирования [Интернет-ресурс] // URL: http://www.econstep.ru/apsteps-528-1.html. (дата обращения: 14.03.2022).
7. Software compare [Интернет-ресурс] // URL: https://www.capterra.com/ (дата обращения: 08.10.2021)
8. Fuzzy Logic Labs – Официальный сайт [Интернет-ресурс] // https://www.fzlabs.ru (Дата обращения: 16.03.2022)
9. Журнал ПЛАС №2(122) 2007 г – Системы фрод-мониторинга транзакций TranzWare Fraud Analyzer [Интернет-ресурс] // https://plusworld.ru/journal/2007/02-122/art140117/ (Дата обращения: 12.03.2022)
10. Anti Maleware – Обзор Smart Fraud Detection, системы противодействия мошенническим транзакциям – Екатерина Быстрова [Интернет-ресурс] // https://www.anti-malware.ru/reviews/Smart-Fraud-Detection (Дата обращения 12.03.2022)

Literature

1. GOST R 7.0.97-2016 - “System of standards for information, librarianship and publishing. Organizational and administrative documentation. Requirements for paperwork” (as amended on May 14, 2018) [Internet resource] // URL: https://www.internet-law.ru/gosts/gost/63653. (date of access: 03/09/2022).
2. David Mark, Clement McGowan, Methodology of Structural Analysis and Design. Per. from English. M.: 1993, 240 pp., ISBN 5-7395-0007-9.
3. 115-FZ "Federal law on combating the legalization (laundering) of proceeds from crime and the financing of terrorism" dated August 7, 2001 // https://static.qiwi.com/ru/doc/fz-115.pdf (Accessed: 03/13/2022).
4. 161-FZ "On the National Payment System", dated June 27, 2011 // https://static.qiwi.com/ru/doc/fz-161.pdf (Date of access: 03/15/2022)

5. ArchiMate 3.0 notation [Internet resource] // https://pubs.opengroup.org/architecture/archimate3-doc/ (Date of access: 03/15/2022).
6. The simplest forecasting methods [Internet resource] // URL: http://www.econstep.ru/apsteps-528-1.html. (date of access: 03/14/2022).
7. Software compare [Internet resource] // URL: https://www.capterra.com/ (Date of access: 10/08/2021)
8. Fuzzy Logic Labs - Official website [Internet resource] // https://www.fzlabs.ru (Date of access: 03/16/2022)
9. Journal PLUS No. 2 (122) 2007 - Transaction fraud monitoring systems TranzWare Fraud Analyzer [Internet resource] // https://plusworld.ru/journal/2007/02-122/art140117/ (Date of access: 03/12/ /2022)
10. Anti Maleware - Review of Smart Fraud Detection, a system for countering fraudulent transactions - Ekaterina Bystrova [Internet resource] // https://www.anti-malware.ru/reviews/Smart-Fraud-Detection (Date of access: 03/12/2022)

© Киселев И.И., Одинцова М.А.,2022 Научно-образовательный журнал для студентов и преподавателей «StudNet» №5/2022.

Для цитирования: Киселев И.И., Одинцова М.А. АВТОМАТИЗАЦИЯ ПРОЦЕССОВ ФРОД-МОНИТОРИНГА ТРАНЗАКЦИЙ КОММЕРЧЕСКОГО БАНКА// Научно-образовательный журнал для студентов и преподавателей «StudNet» №5/2022.