УДК 336.71

# *СОВЕРШЕНСТВОВАНИЕ СИСТЕМЫ ПРОТИВОДЕЙСТВИЯ КОРПОРАТИВНОМУ МОШЕННИЧЕСТВУ В КОММЕРЧЕСКОМ БАНКЕ: ОРГАНИЗАЦИОННЫЕ, ТЕХНОЛОГИЧЕСКИЕ И ЭКОНОМИЧЕСКИЕ АСПЕКТЫ*

***Евстигнеев А.А.***

*магистрант,*

*ФГОБУ ВО «Финансовый университет при Правительстве Российской Федерации»,*

*Москва, Россия*

***Боташева Л.Х.***

*доцент кафедры экономической безопасности и управления рисками факультета экономики и бизнеса,*

*ФГОБУ ВО «Финансовый университет при Правительстве Российской Федерации»,*

*Москва, Россия*

**Аннотация**

Статья посвящена разработке комплекса мер по совершенствованию системы противодействия корпоративному мошенничеству в коммерческом банке. На материалах трех российских банков - ПАО «Сбербанк», АО «Альфа-Банк» и АО КБ «Модульбанк» - предложены организационные, нормативно-методические и технологические решения, дифференцированные с учетом масштаба и специфики каждой кредитной организации. Ключевые предложения включают создание Anti-Fraud Center of Excellence, реформирование системы KPI с включением антифрод-метрик, внедрение единой аналитической платформы Anti-Fraud Data Lake, алгоритмов машинного обучения, графовых нейронных сетей, поведенческой биометрии и платформы SOAR. Проведена оценка социально-экономической эффективности: ROI за трехлетний горизонт

составляет от 139,6% до 736,2%, период окупаемости - от 2,7 до 7,5 месяца, NPV по всем банкам положительна.

**Ключевые слова:** корпоративное мошенничество, противодействие мошенничеству, коммерческий банк, машинное обучение, Anti-Fraud Center of Excellence, экономическая безопасность, цифровые технологии, KPI, поведенческая биометрия, ROI.

## *IMPROVING THE CORPORATE FRAUD PREVENTION SYSTEM IN A COMMERCIAL BANK: ORGANIZATIONAL, TECHNOLOGICAL AND ECONOMIC ASPECTS*

***Evstigneev A.A.***
*Master's student,*
*Financial University under the Government of the Russian Federation,*
*Moscow, Russia*
***Botasheva L.Kh.***
*Associate Professor, Department of Economic Security and Risk Management,*
*Faculty of Economics and Business,*
*Financial University under the Government of the Russian Federation,*
*Moscow, Russia*

**Abstract**

The article is devoted to the development of a set of measures to improve the corporate fraud prevention system in a commercial bank. Based on the analysis of three Russian banks - Sberbank PJSC, Alfa-Bank JSC and Modulbank JSC - organizational, regulatory, methodological and technological solutions are proposed, differentiated according to the scale and specifics of each credit institution. Key proposals include the establishment of an Anti-Fraud Center of Excellence, the reform of the KPI system incorporating anti-fraud metrics, the implementation of a unified Anti-Fraud Data Lake analytics platform, machine learning algorithms, graph neural networks, behavioral

biometrics, and a SOAR platform. A socio-economic efficiency assessment has been conducted: the 3-year ROI ranges from 139.6% to 736.2%, the payback period ranges from 2.7 to 7.5 months, and the NPV is positive for all three banks.
**Keywords:** corporate fraud, fraud prevention, commercial bank, machine learning, Anti-Fraud Center of Excellence, economic security, digital technologies, KPI, behavioral biometrics, ROI.

Корпоративное мошенничество представляет собой одну из наиболее острых угроз устойчивости коммерческих банков в условиях продолжающейся цифровой трансформации финансового сектора. По данным Ассоциации сертифицированных специалистов по расследованию хищений (ACFE), организации ежегодно теряют в среднем 5% выручки вследствие мошеннических действий, а банковский сектор традиционно входит в число наиболее уязвимых отраслей. Для российских кредитных организаций данная проблема усугубляется стремительным ростом экосистемных бизнес-моделей, расширением дистанционных каналов обслуживания и появлением принципиально новых угроз, связанных с применением генеративного искусственного интеллекта для создания синтетических биометрических данных и дипфейков.

Вместе с тем существующие системы противодействия мошенничеству в большинстве российских банков страдают рядом устойчивых недостатков: разрозненностью функций между службой безопасности, комплаенсом и риск-менеджментом, фрагментацией информационных систем, конфликтом интересов между ростом бизнес-показателей и соблюдением контрольных процедур, дефицитом прозрачности антифрод-решений для клиентов. Данные обстоятельства определяют актуальность разработки комплексной системы совершенствования антифрод-функции, охватывающей как организационно-нормативное, так и технологическое измерения.

Цель настоящей статьи состоит в представлении авторских рекомендаций

по совершенствованию системы противодействия корпоративному мошенничеству на примере трех российских банков различного масштаба.

Первым и концептуально наиболее значимым предложением является создание в каждом из исследуемых банков организационной структуры, консолидирующей функции выявления, расследования и предотвращения мошенничества в единый центр компетенций - Anti-Fraud Center of Excellence (AF CoE). Данная рекомендация адресует сразу несколько системных недостатков: разрозненность функций между службой безопасности, комплаенсом и риск-менеджментом, диффузию ответственности в распределенных сетях и дефицит экспертного суждения при принятии антифрод-решений.

AF CoE предлагается выстроить как матричную структуру, включающую четыре ключевых блока: блок превенции и обучения, блок детекции и мониторинга, блок расследований и реагирования, а также блок аналитики данных и технологий (рис. 1). Принципиально важным является непосредственное подчинение руководителя AF CoE Наблюдательному совету или его комитету по аудиту, что обеспечивает независимость антифрод-функции от исполнительного руководства.

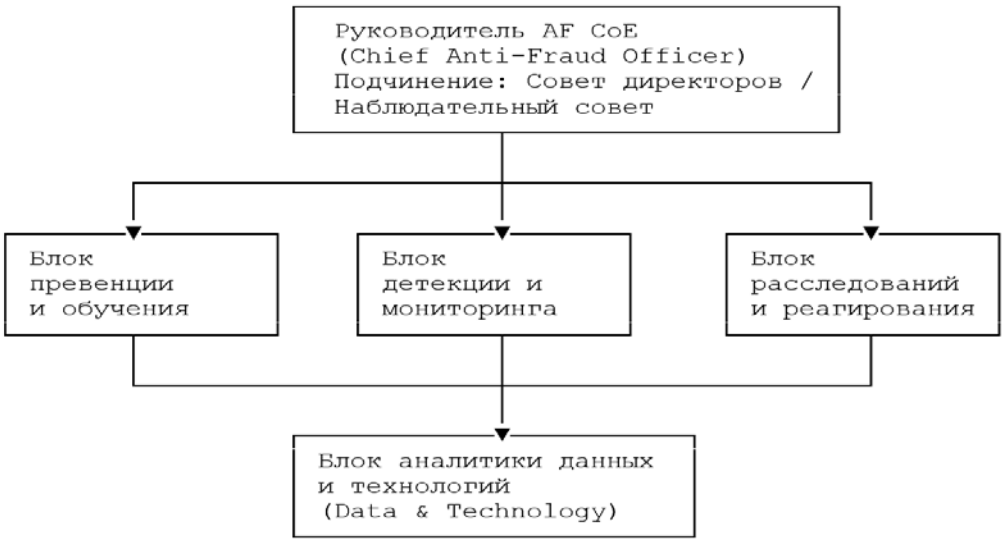


Рис. 1 - Предлагаемая организационная структура Anti-Fraud Center of Excellence

Поскольку банки исследуемой выборки существенно различаются по масштабу, для каждого из них предлагается дифференцированная модель реализации AF CoE (таблица 1).

Таблица 1 - Дифференцированная модель AF CoE для исследуемых банков

| Параметр | ПАО «Сбербанк» | АО «Альфа-Банк» | АО КБ «Модульбанк» |
|---|---|---|---|
| Формат AF CoE | Самостоятельное департаментское подразделение с региональными представителями | Самостоятельное управление в составе блока рисков и безопасности | Выделенный отдел с матричным взаимодействием с IT и комплаенсом |
| Численность персонала | 150–200 специалистов + региональная сеть | 50–80 специалистов | 10–15 специалистов |
| Приоритетный блок | Детекция и мониторинг | Превенция и обучение | Аналитика данных и технологии |

Вторым организационным предложением является включение антифрод-метрик в систему ключевых показателей эффективности сотрудников бизнес-подразделений. Данная мера адресует конфликт интересов между ростом бизнес-показателей и требованиями контрольных процедур.

Предлагается ввести в систему KPI кредитных и клиентских менеджеров дополнительный показатель - «индекс качества антифрод-процедур», рассчитываемый по формуле:

$$I_{AFP} = \alpha \cdot \frac{N_{compl}}{N_{total}} - \beta \cdot \frac{L_{fraud}}{V_{portfolio}} - \gamma \cdot \frac{N_{FP}}{N_{alerts}} \quad (1)$$

где $I_{AFP}$ - индекс качества антифрод-процедур сотрудника за период;

$N_{compl}$ - число операций, проведенных с полным соблюдением контрольных процедур;

$N_{total}$ - общее число операций сотрудника за период;

$L_{fraud}$ - фактические потери от мошенничества по портфелю сотрудника;

$V_{portfolio}$ - объем портфеля;

$N_{FP}$ - число ложноположительных сигналов, инициированных сотрудником без дальнейшего подтверждения;

$N_{alerts}$ - общее число сигналов, переданных сотрудником в антифрод-службу;

α,β,γ - весовые коэффициенты, устанавливаемые банком с учетом приоритетов управления рисками.

Вес $I_{AFP}$ в итоговом KPI должен составлять не менее 15–20%, что создает реальный экономический стимул к соблюдению антифрод-процедур без подавления коммерческой инициативы.

Третьим организационным предложением является введение программы обязательной ротации сотрудников на позициях с повышенным риском внутреннего мошенничества. Устанавливаются три группы должностей:

- группа А (высокий риск) - ротация не реже чем каждые 24 месяца;

- группа Б (средний риск) - не реже чем каждые 36 месяцев;

- группа В (низкий риск) - в соответствии с плановыми кадровыми перемещениями.

Параллельно вводится практика обязательного использования не менее 14 последовательных календарных дней отпуска ежегодно для сотрудников групп А и Б, в течение которых их функции выполняются замещающим специалистом.

Нормативная компонента предлагаемых преобразований охватывает разработку и актуализацию пяти ключевых документов:

1. Политика защиты информаторов (Whistleblower Protection Policy), формализующая гарантии защиты сотрудников, сообщающих о подозрительных действиях, от любых форм репрессивных мер;

2. Обновленный Кодекс корпоративной этики со специализированным антифрод-разделом, содержащим перечень типичных мошеннических схем и поведенческих индикаторов;

3. Регламент управления доступом к информационным системам, реализующий принцип минимально необходимых привилегий (Principle of Least Privilege);

4. Политика противодействия мошенничеству в партнерских каналах,

адресующая специфическую уязвимость банков с разветвленными экосистемами;

5. Стандарт прозрачности антифрод-решений для клиентов, устанавливающий форму уведомления клиента, сроки рассмотрения апелляций и перечень документов для снятия ограничений [1].

Взаимосвязь предложенных мер с выявленными недостатками систематизирована в таблице 2.

Таблица 2 - Матрица соответствия предложенных мер выявленным недостаткам

| Предложенная мера | Адресуемые недостатки | Приоритет реализации |
|---|---|---|
| Создание AF CoE | Диффузия ответственности, разрозненность функций | Высокий (1-й этап) |
| Антифрод-метрики в KPI | Конфликт интересов бизнеса и контроля | Высокий (1-й этап) |
| Программа ротации | Риски внутреннего мошенничества | Средний (2-й этап) |
| Политика защиты информаторов | Барьеры к сообщению об инцидентах | Высокий (1-й этап) |
| Регламент управления доступом | Инсайдерское мошенничество | Высокий (1-й этап) |
| Политика партнёрских каналов | Риски в экосистемных структурах | Средний (2-й этап) |
| Стандарт прозрачности для клиентов | Непрозрачность решений, правовые риски | Средний (2-й этап) |

Фундаментальным технологическим предложением является создание единой аналитической платформы - Anti-Fraud Data Lake, - консолидирующей информацию из разрозненных источников в единое хранилище. Архитектура платформы включает три функциональных слоя: слой сбора и хранения данных (Data Ingestion Layer), охватывающий транзакционные системы, HRMS, CRM, внешние базы данных ФНС, Росреестра, ФССП, СПАРК и данные ФинЦЕРТ; слой обработки и аналитики (Processing & Analytics Layer), реализующий алгоритмы обнаружения аномалий в потоковом и пакетном режимах; слой управления и визуализации (Management & Visualization Layer), предоставляющий аналитикам AF CoE интерактивные инструменты работы с

результатами [2].

Для АО КБ «Модульбанк» рекомендуется использование облачной платформы Data Lake as a Service на базе отечественных провайдеров (Яндекс Облако, VK Cloud), что позволит минимизировать капитальные затраты и обеспечить необходимую масштабируемость.

На основе консолидированных данных Anti-Fraud Data Lake предлагается развернуть обновленную аналитическую экосистему, включающую несколько взаимодополняющих классов моделей машинного обучения.

В целях выявления мошеннических транзакций в режиме реального времени предлагается применение ансамблей алгоритмов, сочетающих градиентный бустинг (XGBoost, LightGBM) и рекуррентные нейронные сети (LSTM). Точность классификации P для ансамблевой модели может быть описана следующим образом:

$$P_{ensemble} = 1 - \prod_{i=1}^{n} (1 - P_i \cdot w_i) \quad (2)$$

$P_i$ - точность i-й модели в ансамбле;

$w_i$ - ее весовой коэффициент;

n - число моделей в ансамбле.

Графовые нейронные сети (GNN). Для выявления мошеннических схем, реализуемых через сети связанных лиц и компаний, предлагается внедрение графовых нейронных сетей, позволяющих моделировать отношения между клиентами, счетами, устройствами и адресами как граф. Открытые исследования демонстрируют повышение точности выявления синтетической идентификации при применении GNN в среднем на 23–31% по сравнению с традиционными методами скоринга [3].

Алгоритмы обнаружения аномалий без учителя. Для выявления ранее неизвестных типов мошенничества рекомендуется применение Isolation Forest, автоэнкодеров и моделей на основе Gaussian Mixture Models. Ожидаемая доля

дополнительно выявляемых аномалий при внедрении данного класса моделей составляет 8–15% от общего числа инцидентов.

Для преодоления уязвимости систем идентификации к атакам с использованием дипфейков предлагается внедрение технологий поведенческой биометрии, анализирующих уникальные паттерны взаимодействия пользователя с устройством: динамику набора текста, характеристики движения мыши, углы наклона мобильного устройства. В отличие от статической биометрии, поведенческие паттерны крайне сложно воспроизвести мошеннику. Непрерывная аутентификация применяет данные поведенческой биометрии на протяжении всей сессии, а не только в момент входа. Оценочное снижение числа успешных случаев несанкционированного доступа при внедрении данной технологии составляет 40–60% [4].

Технология Process Mining позволяет анализировать последовательности действий в рамках бизнес-процессов (кредитный андеррайтинг, операционное обслуживание клиентов, закупки, подготовка отчетности) и выявлять отклонения от эталонных регламентов - индикаторы потенциального внутреннего мошенничества [5].

Для повышения оперативности реагирования предлагается внедрение платформы Security Orchestration, Automation and Response (SOAR), автоматизирующей стандартные процедуры реагирования на типовые инциденты. Согласно данным Gartner, внедрение SOAR сокращает среднее время реагирования (MTTR) в финансовых организациях в среднем на 70–80% [6].

Дорожная карта технологического внедрения рассчитана на 36-месячный горизонт реализации и структурирована в три этапа (таблица 3).

Таблица 3 - Дорожная карта технологического внедрения

| Этап | Период | Мероприятия | Целевые показатели |
|---|---|---|---|
| 1. Фундамент | Месяцы 1–12 | Anti-Fraud Data Lake; базовые DLP и IAM | Консолидация 80% источников данных; снижение несогласованных прав |

| | | | |
|---|---|---|---|
| | | | доступа на 60% |
| 2. Аналитика | Месяцы 13–24 | Ансамблевые ML-модели; GNN; Process Mining | Снижение ложноположительных срабатываний на 30%; рост выявляемости на 25% |
| 3. Автоматизация | Месяцы 25–36 | Поведенческая биометрия; SOAR; детекторы дипфейков | Сокращение MTTR на 70%; снижение потерь на 35–40% |

Экономический эффект от внедрения предложенных мероприятий формируется из трех составляющих.

- сокращение прямых потерь от мошенничества;
- снижение операционных расходов на расследования;
- снижение стоимости регуляторных штрафов.

Наряду с прямым экономическим эффектом реализация предложенных мероприятий генерирует существенные нефинансовые выгоды. Повышение клиентского доверия формирует устойчивый потребительский доверительный капитал: каждый дополнительный балл в рейтинге клиентской удовлетворенности коррелирует с ростом числа рекомендаций банка на 8–12%. Укрепление корпоративной культуры нетерпимости к мошенничеству снижает число инцидентов внутреннего мошенничества более чем на 52% - таков результат, зафиксированный в исследовании PwC Global Economic Crime Survey для организаций с сильной антифрод-культурой [7]. Для банков с активными программами привлечения капитала совершенствование системы корпоративного управления способно снизить стоимость фондирования на 15–40 базисных пунктов [8]. Наконец, добровольное опережающее совершенствование системы противодействия мошенничеству формирует позитивный регуляторный капитал и снижает вероятность внеплановых проверок со стороны Банка России.

Проведенное исследование позволяет сформулировать следующие основные выводы.

Устойчивое противодействие корпоративному мошенничеству требует

комплексного подхода, сочетающего организационно-нормативные и технологические меры. Они находятся в тесной взаимосвязи: организационные решения создают институциональный фундамент, без которого технологические инновации не способны обеспечить устойчивого эффекта.

Создание AF CoE как единого центра компетенций является концептуально приоритетной мерой, обеспечивающей консолидацию антифрод-функции и устранение диффузии ответственности.

Технологическое совершенствование должно реализовываться поэтапно, с приоритетом создания единой аналитической платформы данных как инфраструктурной основы для последующего развертывания аналитических моделей.

**Библиографический список:**

1. Association of Certified Fraud Examiners. Report to the Nations: 2024 Global Study on Occupational Fraud and Abuse. - Austin: ACFE, 2024. - 112 p.
2. Bailey K. Behavioral Biometrics: A New Approach to Authentication / K. Bailey, K. Okolica, G. Peterson // Computers & Security. - 2014. - Vol. 43. - P. 109–116.
3. Gartner. Market Guide for Security Orchestration, Automation and Response Solutions. - Stamford: Gartner Research, 2023. - 28 p.
4. Hamilton W.L. Graph Representation Learning / W.L. Hamilton. - San Rafael: Morgan & Claypool Publishers, 2020. - 159 p.
5. Inmon W.H. Building the Data Warehouse / W.H. Inmon. - 4th ed. - Indianapolis: Wiley Publishing, 2005. - 576 p.
6. PricewaterhouseCoopers. Global Economic Crime and Fraud Survey 2022 [Электронный ресурс]. - URL: https://www.pwc.com/gx/en/services/forensics/economic-crime-survey.html (Дата обращения: 05.05.2026).
7. Van der Aalst W.M.P. Process Mining: Data Science in Action / W.M.P. Van der Aalst. - 2nd ed. - Berlin: Springer, 2016. - 467 p.

8. Банк России. Положение об организации внутреннего контроля в кредитных организациях и банковских группах: Положение от 16.12.2003 № 242-П (ред. от 2021) [Электронный ресурс]. - URL: https://www.cbr.ru (Дата обращения: 15.04.2026).

9. Городецкий А.Е. Экономическая безопасность: теория и практика / А.Е. Городецкий. - М.: Проспект, 2022. - 544 с.

10. Лобанова Е.Н. Финансовый менеджмент: учебник / Е.Н. Лобанова. - М.: Юрайт, 2023. - 482 с.

11. Тавасиев А.М. Банковское дело: управление и технологии / А.М. Тавасиев. - М.: ЮНИТИ-ДАНА, 2021. - 671 с.