

КОМПЛАЕНС, ВНУТРЕННИЙ КОНТРОЛЬ И АУДИТ
В ФИНАНСОВЫХ ИНСТИТУТАХ

Особенности внутреннего контроля в условиях применения технологий электронного банкинга

Рустам Мухаметшин

Блок комплаенс и нефинансовых рисков

Трансформация среды контроля

Ключевые вызовы цифрового банкинга для внутреннего контроля

- Переход от «кейс-менеджмента» к управлению в реальном времени
- Отсутствие физического контакта с клиентом → рост рисков дистанционного мошенничества
- Скорость транзакций превышает скорость традиционных проверок
- Новые объекты контроля: мобильные приложения, каналы переводов

Вывод: Внутренний контроль должен стать прогнозным и автоматизированным

Архитектура внутреннего контроля в цифровом банке

Три линии защиты в среде электронного банкинга

Схема / маркеры:

- Первая линия (Бизнес): Лимиты операций, скоринг сессий, антифрод-модули.
- Вторая линия (Риски и ПОД/ФТ): Мониторинг транзакций, блокировка подозрительных операций.
- Третья линия (Аудит): Пост-анализ логов, оценка эффективности алгоритмов.

Ключевое: Автоматизированный контроль вместо ручного.

Функция финансового мониторинга (ПОД/ФТ)

Специфика выявления сомнительных операций

Особенности:

- Операции дробления сумм через разные устройства (сниффинг устройств)
- Использование технологий «дропперства» и массового открытия дистанционно
- Транзакции в криптовалютах через P2P-платформы (обменники)
- Рост числа «спящих» счетов с резкой активизацией через веб-банк

Инструмент: Поведенческий скоринг (фиксация привычных паттернов)

Алгоритмы выявления нетипичного поведения

Примеры правил и метрик ПОД/ФТ

Список технологических признаков:

- Смена девайса и геолокации за < 1 мин до крупного платежа
- Использование анонимайзеров или компрометированных IP-адресов
- Операции в нерабочее время, например, 02:00 – 05:00
- Скорость ввода данных (бот копирует, человек печатает медленнее)

Результат: Автоматическая блокировка до подтверждения личности

Инструменты и технологии контроля

Что внедрять цифровому банку?

- Отпечаток устройства – уникальные признаки гаджета. Выявляет подмену IP и новые/подозрительные устройства
- Поведенческий анализ – скорость нажатий, движение мыши. Отличает живого человека от бота
- Антифрод на правилах – готовые сценарии: «сумма > X → запросить СМС». Мгновенная реакция на типовые схемы
- Машинное обучение – ищет аномалии, которые не прописаны в правилах. Учится на истории клиента
- Динамические лимиты – лимиты падают при подозрениях. Мошенник не выведет крупную сумму

Внутренний контроль как источник рисков для аудита

Типичные зоны сбоев в E-Banking

Что проверять внутреннему аудиту:

- Доступы сотрудников к ключам подписи и API клиентов
- Журналы событий (log management) – их полноту и защиту от модификации
- Сценарии принудительного выхода из системы при подозрении
- Политики повторного подтверждения при смене номера телефона/устройства

Рекомендация: Ежеквартальная пентест-атака на систему ДБО

Инструменты и технологии контроля

Что внедрять цифровому банку?

- Отпечаток устройства – уникальные признаки гаджета. Выявляет подмену IP и новые/подозрительные устройства
- Поведенческий анализ – скорость нажатий, движение мыши. Отличает живого человека от бота
- Антифрод на правилах – готовые сценарии: «сумма > X → запросить СМС». Мгновенная реакция на типовые схемы
- Машинное обучение – ищет аномалии, которые не прописаны в правилах. Учится на истории клиента
- Динамические лимиты – лимиты падают при подозрениях. Мошенник не выведет крупную сумму

Кейс: управление лимитами и контроль транзакций

Пример настройки риск-профилей

Тип клиента	Лимит в сутки	Доп. контроль ПОД/ФТ
Новый (менее 7 дней)	100 тыс. руб.	Только исходящие на счета той же страны
Подтвержденный (с биометрией)	5 млн руб.	Контроль по географии и времени
Корпоративный	50 млн руб.	Проверка бенефициаров по каждой

Вывод: Гибкие динамические лимиты снижают «шум» для фин. мониторинга

Организационные аспекты

Кто управляет рисками E-Banking

- Подразделения: Подразделение ПОД/ФТ + Антифрод
- Регламенты:
 - Алгоритм рассмотрения кейсов и разблокировки клиента
 - Проработанный клиентский путь, отвечающий требованиям законодательства
- Обучение: Скрипты для сотрудников call-центра

Заключение и рекомендации

Как построить эффективную систему контроля

Итоги:

- Внутренний контроль в цифровом банке – это код, а не бумага
- Финансовый мониторинг становится неотделим от антифрода и ИБ
- Ручные проверки должны оставаться только для сложных кейсов (правовая экспертиза)

Рекомендации:

- Внедрить единую платформу логов для всех каналов E-Banking
- Создать комитет по управлению канальными рисками

Спасибо за внимание!