

XXXXXXXXXX

По какой схеме может быть выстроен процесс выявления внутреннего мошенничества в банке? Как работает антифрод-скоринг? Возможно ли идеальное мошенничество? Как математически определить вероятность успеха мошеннических действий в зависимости от эффективности антифрод-процедур? Как минимизировать человеческий фактор при расследовании случаев мошенничества и улучшить качество работы сотрудников?

## Выявление внутреннего мошенничества в розничном кредитовании

— Почему вы грабите банки?  
— Потому что там деньги.

Вилли Саттон, грабитель банков



**С.В. АФАНАСЬЕВ,**  
*риск-менеджер<sup>1</sup>*

Как показывает практика работы по пресечению фактов кредитного мошенничества, наибольший ущерб банку наносит организованное внутреннее мошенничество со стороны недобросовестных сотрудников и организаций-партнеров. Каждый факт внутреннего мошенничества приносит ущерб, практически не сопоставимый по размерам с ущербом, который приносят отдельные мошенники или даже мошеннические группы, действующие «извне». Возврат денежных средств, похищенных таким образом у банка, представляет собой весьма трудный и длительный процесс, не всегда приводящий к успеху.

Для борьбы с внутренним мошенничеством банкам доступен обширный комплекс инструментов, в который входят процедуры проверки персонала и партнеров, мотивационные схемы, фрод-мониторинг, специализированное программное обеспечение и многое другое.

В этой статье мы разберемся с ключевыми принципами работы автоматизированной системы по выявлению внутреннего мошенничества.

<sup>1</sup> Автор имеет 8-летний руководящий опыт в банках ХКФБ и «ТРАСТ».

---

## Выявление внутреннего мошенничества в розничном кредитовании

---

### Проблематика внутреннего мошенничества

Несколько лет назад в одном крупном розничном банке запустили новый продукт под названием «Виртуальная карта». По технологии продукта клиенту на мобильный телефон приходило SMS с паролем и реквизитами счета по одобренному кредиту. Чтобы получить наличные, клиенту необходимо было ввести пароль и реквизиты в банкомате, то есть никаких пластиковых карт или походов в кассу не требовалось — только данные SMS.

Продукт набирал свою популярность, и с каждым днем все больше кредитных заявок оформлялось по технологии «Виртуальная карта». Одна из таких заявок попала на проверку в подразделение андеррайтинга. Сотрудник, проверяющий заявку, выявил, что на прикрепленной к заявке фотографии изображен не клиент, а какой-то графический персонаж. Этим персонажем оказался герой компьютерной игры Tom Clancy's Splinter Cell — Сэм Фишер.

Информация об этом была направлена на расследование в подразделение безопасности банка. Выяснилось, что заявка была оформлена на клиента, который уже брал кредит в банке. Сам клиент утверждал, что новую заявку не оформлял. Также выяснилось, что мобильный телефон, указанный в мошеннической заявке, был предварительно изменен в системе банка и клиенту не принадлежал. В процессе расследования было выявлено еще несколько десятков заявок, по которым были изменены номера мобильных телефонов в банковской базе данных. Сотрудникам, проводившим расследования, стало понятно, что банк имеет дело с организованным внутренним мошенничеством. Первой под подозрение попала сотрудница, под логином которой были оформлены мошеннические кредитные заявки. По результатам проверки сотрудники подразделения безопасности выяснили, что подозреваемая сотрудница не причастна к оформлению мошеннических кредитов, а ее логином и паролем мог воспользоваться кто-то из недобросовестных коллег, поскольку среди сотрудников офисов негласно практиковалась передача логинов и паролей друг другу.

Круг подозреваемых сотрудников расширился, были проверены и допрошены несколько действующих сотрудников офиса, включая их руководителя. По результатам проведенных проверок была установлена личность первого мошенника. Им оказался действующий сотрудник банка Шарапов. В день оформления мошеннических кредитов он брал незапланированный отгул. Анализ лог-файлов показал, что IP-адрес, с которого оформлялись мошеннические кредиты, не принадлежал банку и использовался ранее Шараповым.

XXXXXXXXXX

На допросе Шарапов раскрыл все детали мошеннической схемы и двух своих соучастников. Одним из соучастников оказался друг Шарапова, бывший сотрудник банка Першин. Вторым соучастником Шарапова был студент московского технического вуза Ефремов. Схема мошенничества заключалась в том, что Шарапов и его соучастники меняли в базе данных банка номера мобильных телефонов клиентов на свои. Потом они оформляли заявки на этих клиентов по технологии «Виртуальная карта», получая на свои мобильные телефоны SMS со всеми необходимыми данными. Затем вся мошенническая компания ехала по банкоматам снимать наличные. За три дня своей деятельности они успели снять порядка 3 млн руб., после чего их выдал Сэм Фишер — главный герой любимой компьютерной игры Першина. Для всех операций в системе банка мошенники использовали логины и пароли, украденные ранее у своих коллег.

На этом история с «виртуальными картами» не закончилась. Сотрудниками подразделений рисков и безопасности были выявлены еще два эпизода мошенничества со стороны сотрудников банка, которые действовали по такой же схеме, но в одиночку. Технологию «виртуальной карты» временно закрыли, банк вернул украденные деньги, а мошенники, к их счастью, остались на свободе, возместив весь ущерб, причиненный банку в результате их действий.

Разобранный пример является одним из эпизодов внутреннего мошенничества, с которыми банки сталкиваются каждый день. При этом он наглядно демонстрирует ключевые проблемы банков, связанные с внутренним мошенничеством (табл. 1):

1. Большие потери за короткие сроки.

В приведенном примере мошенники за три дня вывели 3 млн руб. Если бы мошенничество не было выявлено на ранних этапах, то при

Контроль и воспитание сотрудников помогут донести до штатного персонала, что мошеннические действия не остаются безнаказанными.

Таблица 1

### Проблематика внутреннего мошенничества в банках

Проблема	Решение
Большие потери за короткие сроки	Выявление мошенничества на ранних этапах
Уязвимости в банковских процессах и ПО	Выявление уязвимостей и доработка процессов
Сотрудники чувствуют безнаказанность	Контроль и воспитание сотрудников

---

## Выявление внутреннего мошенничества в розничном кредитовании

---

таких темпах через месяц потери составили бы 30 млн руб., через два месяца — 60 млн руб. и т.д.

2. Уязвимости в банковских процессах и программном обеспечении.

Мошенники воспользовались слабыми местами в технологии нового продукта. Кроме того, они без особого труда узнали логины и пароли своих коллег, а также бесконтрольно меняли в банковской базе данных мобильные телефоны клиентов, на которые приходили SMS с паролями и реквизитами для снятия наличных.

3. Чувство безнаказанности у сотрудников.

Чувство вседозволенности и безнаказанности подталкивает некоторых сотрудников на противоправные действия. В рассмотренном примере мошенники продемонстрировали это, прикрепив фотографию компьютерного героя Сэма Фишера и зная при этом, что в банке работает биометрическая система, выявляющая подозрительные фотографии.

Для устранения перечисленных ключевых проблем банку необходимо выстроить процессы противодействия внутреннему мошенничеству таким образом, чтобы были решены следующие задачи:

1) выявление мошенничества на ранних этапах (позволит минимизировать потери банка от мошенничества, а также снизить влияние мошеннической составляющей на финансовые показатели портфеля);

2) выявление уязвимостей и доработка процессов (закроют возможности для подобного мошенничества в будущем);

3) контроль и воспитание сотрудников (помогут донести до штатного персонала, что мошеннические действия не остаются безнаказанными).

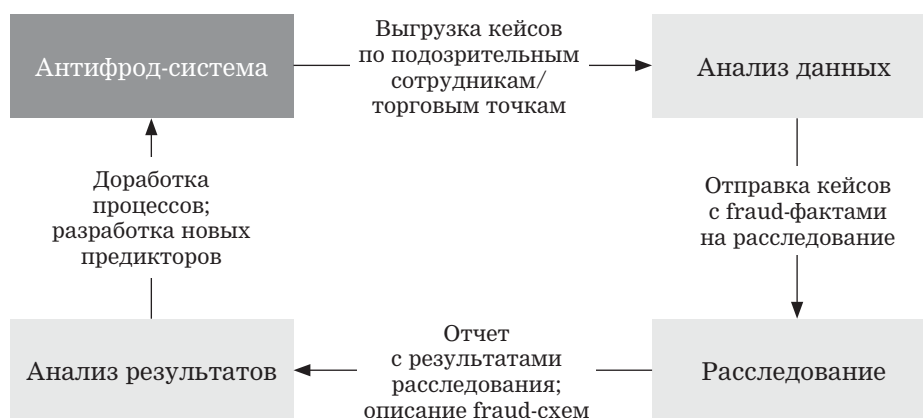
### Схема процесса

Процесс выявления внутреннего мошенничества в банке должен быть выстроен таким образом, чтобы с его помощью решались все ключевые проблемы, рассмотренные выше. Одна из возможных схем такого процесса изображена на рис. 1.

Выявление внутреннего мошенничества начинается с работы антифрод-системы. Эта система в автоматическом режиме выявляет подозрительных сотрудников и партнеров (например, торговые точки в POS-сегменте) и формирует список кейсов. После обработки данных кейсы направляются на ручной анализ к сотруднику аналитического подразделения. На втором этапе аналитик проверяет кейсы, анализирует выгруженные факты, убирает «мусорные» данные и, если

XXXXXXXXXX

Рисунок 1

**Схема процесса выявления внутреннего мошенничества в банке**

необходимо, проводит дополнительные проверки и сбор данных. После проведенного анализа сотрудник принимает решение, отправлять данные на расследование сотруднику подразделения безопасности или нет. Этот этап важен, так как при ручном анализе отсеивается порядка 50–80% кейсов, ошибочно выгруженных антифрод-системой.

На третьем этапе сотрудник подразделения безопасности проводит расследование, используя различные методы криминалистики: осмотр, изучение документов, беседа с подозреваемыми и свидетелями, ревизии, оперативно-разыскные мероприятия и др. Результаты расследования сотрудник подразделения безопасности направляет аналитику.

На четвертом, завершающем, этапе аналитик обрабатывает результаты расследования: смотрит, какие уязвимости в банковских процессах и ПО были обнаружены, принимает меры по устранению этих уязвимостей, строит новые алгоритмы и правила выявления внутреннего мошенничества и добавляет их в антифрод-систему.

Приведенная схема имеет следующие плюсы:

1. Ручной анализ позволяет обрабатывать большое число кейсов. Количество кейсов регулируется с помощью порога отсеечения в антифрод-системе. Чем больше кейсов будет проверено, тем больше случаев мошенничества будет раскрыто. С другой стороны, издержки на дорогостоящие расследования растут пропорционально количеству кейсов, отправленных в подразделение безопасности. Ручной

## Выявление внутреннего мошенничества в розничном кредитовании

анализ позволяет оптимально подойти к вопросу издержек и эффективности расследований.

Для ручного анализа иногда привлекается ресурс call-центра: заявки, оформленные подозрительными сотрудниками, отправляются на обзвон. Ресурс call-центра недорогой и позволяет обзвонить по специальным скриптам большое количество лиц. Результаты обзвона прикрепляются к данным, направляемым на расследование, и у сотрудников безопасности уже нет необходимости обзванивать всех лиц, заявки которых признаны подозрительными.

2. Квалифицированное расследование силами сотрудников подразделения безопасности позволяет выявить новые схемы мошенничества и выработать эффективные меры защиты.

3. Схема процесса является замкнутой (аналог «колеса науки»). Это позволяет развивать антифрод-систему путем внедрения новых алгоритмов, которые выявляют мошенничество в автоматическом режиме.

4. Наличие скоринговой карты в антифрод-системе позволяет выделять сотрудников с высоким уровнем дефолта, то есть прогнозировать банковские потери. При таком подходе не возникает проблемы, когда выявление мошенничества становится самоцелью. То есть основной целью антифрод-процесса является снижение финансовых потерь банка.

### Антифрод-система

После печально известных террористических атак в Лондоне перед аналитиками британских банков поставили задачу: найти в клиентской базе людей, которые с высокой вероятностью могут быть террористами. В распоряжение аналитиков были предоставлены данные по всем уже известным террористам-смертникам. Основная проблема заключалась в том, что аналитикам надо было выделить небольшую группу подозрительных лиц из 500-миллионной клиентской базы. При такой постановке задачи (когда искомая группа в сотни тысяч раз меньше общей выборки) стандартные эконометрические методы не работают. Аналитикам пришлось проявить изобретательность, чтобы выделить не слишком большую группу лиц (порядка 500 человек, которых спецслужбы смогли бы поставить на слежение), при этом чтобы выделенная группа охватывала как можно больше потенциальных террористов. В результате кропотливой работы британским аналитикам удалось выяснить, что террористы, как и обычные люди, могут быть холостыми, а могут иметь семью. Террористы, как и обычные люди, могут жить рядом с мечетью, а могут и далеко от нее.

Для ручного анализа иногда привлекается ресурс call-центра: заявки, оформленные подозрительными сотрудниками, отправляются на обзвон.



XXXXXXXXXX

Однако среди террористов больше мужчин, чем женщин. А еще террористы, в отличие от обычных людей, редко страхуют свою жизнь. Аналитикам также удалось выявить несколько финансово-поведенческих характеристик, по которым можно было выделить ту самую небольшую группу потенциальных террористов из многомиллионной клиентской базы. Эта информация была передана в спецслужбы и по понятным причинам остается засекреченной.

Выявление внутреннего мошенничества в банках строится по такому же принципу: необходимо выделить небольшую группу мошенников среди нескольких тысяч сотрудников. Такую задачу в банках решает антифрод-система (Fraud Investigation System), которая состоит из трех основных модулей (рис. 2):

1) хранилище данных — систематизированная, регулярно обновляемая база данных с информацией о кредитах, клиентах и партнерах;

2) математическая модель — скоринговая карта, прогнозирующая высокий уровень просрочки по сотрудникам и партнерам в зависимости от их поведенческих характеристик;

3) пользовательский интерфейс — модуль для пользователей системы, в котором ведется работа с кейсами.

## Хранилище данных

Хранилище данных наполняется информацией из внутренних и внешних источников.

Рисунок 2

## Антифрод-система для выявления внутреннего мошенничества

Хранилище данных	Антифрод-скоринг	Интерфейс (кейсы)
<b>Внутренние источники</b> Данные по заявкам. Данные по сотрудникам. Данные по партнерам. Биометрика. Транзакции и платежи <b>Внешние источники</b> Государственные сервисы (ФМС, ФССП и др.). Данные БКИ. Данные FPS. Социальные сети. GPS-координаты	<b>Предикторы</b> Аналитики разрабатывают предикторы на основе результатов расследований <b>Правила</b> С помощью ассоциативного анализа из предикторов строятся правила <b>Модель</b> На правилах строится скоринговая модель, выявляющая внутреннее мошенничество	<b>Удобный формат</b> Данные в удобном формате для аналитиков и сотрудников безопасности <b>Автоматизация</b> Автоматизация обработки данных (SQL-процедуры, макросы на VBA, ПО) <b>Понятные факты</b> 30–50 типов понятных фактов, с которыми легко работать в процессе расследования

---

## Выявление внутреннего мошенничества в розничном кредитовании

---

При выявлении внутреннего мошенничества используется следующая «внутренняя» информация:

- 1) данные по клиентам: персональные данные, данные по заявкам, биометрические данные, данные по платежам и транзакциям, результаты работы службы взыскания и др.;
- 2) данные по сотрудникам и партнерам: карточка сотрудника/партнера, график работы, данные по оформленным заявкам, лог-файлы и т.д.;
- 3) данные по состоянию договоров: результаты проверок верификации и андеррайтинга, скоринговые оценки, данные по просрочкам, взысканию и др.

К «внешней» информации относятся:

- 1) данные государственных сервисов (ФМС (недействительные паспорта), ФССП, ФНС, Росреестр и др.);
- 2) данные кредитных бюро (НБКИ, «Эквифакс», ОКБ и др.);
- 3) данные антифрод-сервисов (FPS, National Hunter);
- 4) данные интернет-ресурсов (социальные сети, сервисы интернет-статистики (счетчики), картографические сервисы (GPS-координаты) и др.);
- 5) данные сторонних компаний (СПАРК, мобильные операторы, страховые компании и др.).

Хранилище антифрод-системы строится, как правило, в виде плоской таблицы, данные в которую импортируются из внутренних и внешних источников с помощью регулярной ETL-процедуры. Единая плоская таблица необходима для «разгрузки» основного аналитического хранилища, поскольку многие антифрод-правила вычисляются алгоритмами сложностью  $O(N^2)$ .

### Скоринговая модель

Антифрод-скоринг — это скоринговая модель, прогнозирующая вероятность высокого уровня просрочки по сотруднику или партнеру. Высокий уровень просрочки по сотруднику или партнеру может быть связан с различными причинами, но чаще всего такой причиной является мошенничество со стороны сотрудника или партнера. Модель состоит из набора правил, которые формируются в три этапа (рис. 3):

- 1) разработка поведенческих предикторов;
- 2) формирование правил методами Data Mining;
- 3) отбор правил в скоринговую модель.

На первом этапе аналитики разрабатывают поведенческие предикторы — алгоритмы, характеризующие нетипичное поведение заемщиков, сотрудников или партнеров. При разработке предикто-



XXXXXXXXXX

Рисунок 3

### Схема разработки скоринговой модели для выявления внутреннего мошенничества



ров используются результаты раскрытых мошеннических схем, а также широкий математический инструментарий, разнообразие которого ограничено только фантазией и компетенциями аналитиков. К поведенческим предикторам относятся как простые, так и сложные алгоритмы.

К простым предикторам можно отнести следующие алгоритмы:

- сотрудник завел заявки на разных заемщиков, а в заявках указал одинаковый номер мобильного телефона;
- сотрудник завел несколько заявок на одного заемщика, в которых указал разные адреса проживания.

К сложным предикторам можно отнести, например, такие алгоритмы:

- за короткий срок сильно выросло количество оформленных сотрудником кредитных карт, с которых в течение одного дня сняты максимальные денежные суммы;
- в партнерских заявках распределение зарплат не соответствует распределению Бенфорда.

Описание предикторов является конфиденциальным и не разглашается банками, поэтому в разных банках набор предикторов может различаться.

На втором этапе разработки модели аналитики строят правила. Правило представляет собой комбинацию предикторов, связанных друг с другом с помощью математических и логических операторов. При разработке правил применяются методы Data Mining, которые

---

## Выявление внутреннего мошенничества в розничном кредитовании

---

позволяют выделить небольшой сегмент из общей выборки данных. Для такой задачи не подходят классические методы скоринга, такие как логистическая регрессия и деревья решений, поскольку эти алгоритмы хорошо разделяют выборку на сопоставимые по размеру сегменты.

Одним из наиболее подходящих методов моделирования в задачах антифрода является ассоциативный анализ. Суть метода ассоциативного анализа заключается в построении правил из предикторов методом полного перебора и выделения набора эффективных правил из полученного множества. В качестве показателя эффективности выбираются показатели просрочки на первом платеже (fpd) и частоты срабатывания правила (hit-rate).

На третьем этапе разработки скоринговой модели аналитики отбирают самые эффективные правила для скоринговой карты. Правила и коэффициенты скоркарты пересчитываются 1–2 раза в год. Новые правила и предикторы можно добавлять в скоринговую карту, не пересчитывая всю модель.

Рассмотренный подход к моделированию антифрод-скоринга используется в нескольких розничных банках, аналитики которых разработали порядка 300 поведенческих предикторов, с помощью ассоциативного анализа построили около 3000 правил, из них 100 вошли в скоринговую модель.

### Интерфейс

Пользовательский интерфейс является важной и неотъемлемой частью антифрод-системы, поскольку в пользовательской среде антифрод-системы ведется основная часть работы по расследованию внутреннего мошенничества. Есть три принципа построения хорошего интерфейса антифрод-системы:

- 1) данные должны отображаться в удобном для пользователя формате;
- 2) обработка данных должна быть максимально автоматизирована;
- 3) в кейсах должны отображаться понятные для расследования факты.

Первые два принципа достаточно просты и очевидны. Удобный формат подразумевает наличие необходимых функций для каждого типа пользователя: аналитикам для работы необходимы функции сортировки, фильтрации, построения сводных таблиц и диаграмм — таким набором инструментов обладает, к примеру, Excel. Сотрудникам безопасности необходима возможность распечатки досье с фактами, требуемыми для проведения расследования, поэтому

XXXXXXXXXX

для этих целей наиболее подходят форматы doc, pdf. Автоматизация обработки данных может в несколько раз увеличить производительность. Так, например, в одном крупном розничном банке у аналитика на ручную обработку одного кейса уходило в среднем 60 минут, а после автоматизации — 15 минут. Таким образом, с помощью автоматизации удалось увеличить производительность работы аналитиков в четыре раза.

Третий принцип требует пояснения. Под фактами понимается подозрительная информация, которая отображается в кейсах и которую аналитики и сотрудники подразделения безопасности могут проверить в процессе расследования (через обзвоны или выездные проверки). Часто факты дублируют антифрод-правила, входящие в модель, однако в пользовательской среде факты отображаются не в виде алгоритма, а в виде описания (поэтому факты относятся к интерфейсной части). Например, антифрод-модель может содержать следующее правило: у одного заемщика в двух или более заявках, заведенных за последние 30 дней, указано два или более различных номеров мобильного телефона. Факт, соответствующий этому правилу, будет представлен в следующем виде: у одного заемщика указаны разные номера мобильных телефонов. Не все правила из антифрод-модели могут иметь соответствующих «двойников» среди списка фактов, и наоборот: не все факты могут иметь «двойников» среди правил. Антифрод-системы, внедренные в нескольких розничных банках, включают в себя около 50 различных фактов, описание которых по понятным причинам конфиденциально и не разглашается. Примеры некоторых фактов представлены в табл. 2.

Таблица 2

### Примеры фактов, указывающих на подозрительные действия сотрудников

Дата обращения	Фамилия	Имя	Рабочий телефон	Работодатель (место работы)	Улица работодателя	Должность	Срок работы
1	2	3	4	5	6	7	8
За короткий период времени один кредитный консультант меняет личные данные							
08.08.2014 21:54	Шидов	Дмитрий	8123715152	ООО «АРТ»	Приморская ул.	Менеджер по продажам	С 01.2010
08.08.2014 22:14	Шидов	Дмитрий	8123524806	ООО НСК «Энерго»	Морская наб.	Электрик	С 01.2010

антифрод-система \ скоринговая модель \ бизнес-процессы

## Выявление внутреннего мошенничества в розничном кредитовании

Окончание табл. 2

1	2	3	4	5	6	7	8
19.04.2014 16:30	Маркин	Олег	4862410157	ЗАО «Орлэкс»	Ул. Ломоносова	Инженер	С 09.2008
19.04.2014 16:41	Маркин	Олег	4862720053	ОАО «Автобаза»	Пищевой пер.	Экспедитор	С 09.2010
<b>За короткий период времени разные кредитные консультанты меняют личные данные</b>							
08.07.2010 13:26	Дмитриева	Ольга	8125673212	ОАО Трест 3	Просп. Науки	Товаровед	С 05.2003
08.07.2010 13:44	Дмитриева	Ольга	8122243824	ООО «Ладо- пром»	Партизанская ул.	Швея	С 08.2009
Дата обращения	Фамилия	Имя	Мобиль- ный телефон	Индекс	Город	Улица	Номер дома
<b>Одинаковый номер телефона у заемщиков, проживающих по разным адресам</b>							
27.06.2013 17:34	Белов	Валерий	9260565653	141070	Королев	Ленина	9
01.07.2013 17:30	Менщиков	Игорь	9260565653	101000	Москва	Зеленоград	612
02.07.2013 09:52	Флексер	Алексей	9260565653	101000	Москва	Волгоград- ский просп.	4
07.07.2013 17:43	Мисилина	Ирина	9260565653	143517	Пос. Глебовский	Микро- район	37
07.07.2013 19:54	Кальметов	Алексей	9260565653	111399	Москва	Новогиреев- ская	9
07.07.2013 20:13	Воробьев	Марат	9260565653	143910	Балашиха	Текстиль- щиков	11
07.07.2013 20:46	Кожин	Иван	9260565653	119049	Москва	Ленинский просп.	3

Хорошим подспорьем для аналитиков и сотрудников подразделения безопасности является инструкция с описанием фактов и рекомендациями, как проверять тот или иной факт.

### Идеальное мошенничество

Каждый, кто изучал криминологию, знает, что гениальные преступники и мошенники-интеллектуалы встречаются по большей части в сериалах (увы, там же обитают и гениальные следователи). В реаль-

XXXXXXXXXX

ной жизни все прозаичней: большинство мошеннических схем банальны, а сами мошенники оставляют за собой много улик.

В процессе расследования банковского мошенничества факты в кейсах являются своего рода уликами: чем больше обнаружено фактов в действиях сотрудника, тем выше вероятность мошеннических действий со стороны этого сотрудника. С помощью антифрод-системы можно довольно просто и быстро выявлять случаи внутреннего мошенничества. Причем основной причиной простоты выявления внутреннего мошенничества является не столько глупость мошенников (некоторые из них, напротив, настоящие виртуозы), сколько сложность реализации идеальной мошеннической схемы — мошенничества без улик.

Сложность реализации идеального мошенничества можно продемонстрировать на примере карточной аферы Шарапова и его соучастников, которая разбиралась в начале статьи. Напомним, что сотрудник банка Шарапов и двое его подельников оформляли мошеннические кредиты на клиентов банка, меняя в базе данных банка номера мобильных телефонов. В банке, в котором работал Шарапов, внедрен комплекс мероприятий по противодействию мошенничеству. На разных этапах кредитного цикла работают следующие антифрод-процедуры:

- 1) принцип «четыре глаза» на этапе оформления кредита (любой сотрудник может выявить мошенничество и доложить об этом руководству или в подразделение безопасности банка);
- 2) проверки подразделения безопасности;
- 3) верификация и андеррайтинг (антифрод-проверки, биометрика);
- 4) антифрод-сервисы (FPS, ФМС);
- 5) принцип «четыре глаза» на этапе выдачи кредита (кассовые сотрудники, веб-камеры на банкоматах, алерты по транзакциям);
- 6) антифрод-система (выявление внутреннего мошенничества);
- 7) данные службы розыска (неконтактность);
- 8) фрод-репорты (просрочки и риск-концентрации).

Каждая антифрод-процедура имеет определенную эффективность, которую можно охарактеризовать как вероятность обнаружения мошенничества. Для простоты можно считать, что антифрод-процедуры не дублируются, то есть события обнаружения мошенничества независимы. Вероятности независимых событий можно перемножать, а это значит, что по формуле обратной вероятности можно оценить шансы мошенников на успех:

$$Q = (1 - p_1)(1 - p_2)(1 - p_3)(1 - p_4)(1 - p_5)(1 - p_6)(1 - p_7)(1 - p_8), \quad (1)$$

## Выявление внутреннего мошенничества в розничном кредитовании

где  $Q$  — вероятность мошенников пройти все антифрод-процедуры без подозрений;

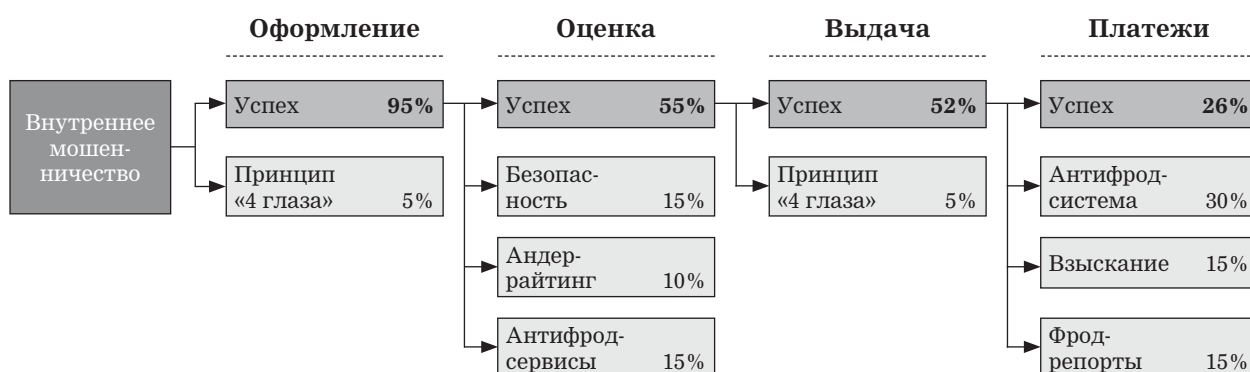
$p_i$  — вероятность обнаружения мошенничества для  $i$ -й антифрод-процедуры.

Подставив в формулу (1) значения  $p_i$ , можно оценить вероятность успешных мошеннических действий на каждом этапе кредитного цикла (рис. 4). Напомним, что мошенничество Шарапова было обнаружено на этапе биометрических проверок андеррайтинга.

Полученная вероятностная оценка показывает, насколько сложно разработать идеальную мошенническую схему. Чтобы обойти все антифрод-процедуры банка, мошенникам необходимо продумать десятки различных сценариев и учесть сотни разных факторов. На практике в подавляющем большинстве случаев мошенники прорабатывают всего один план, в лучшем случае обходящий андеррайтинг, проверки подразделения безопасности и мониторинг риск-показателей. Отклонение от плана заставляет мошенников быстро реагировать и корректировать свои действия. Из нейропсихологии известно, что в состоянии быстрого реагирования к работе подключаются подкорковые образования головного мозга (таламус и гипоталамус), которые отвечают за быстрое эмоциональное мышление (в отличие от коры головного мозга, которая отвечает за медленное рациональное мышление). Быстрое эмоциональное мышление значительно увеличивает количество ошибок, поскольку таламус и гипоталамус запрограммированы информацией, полученной десятки

Рисунок 4

### Вероятность успеха мошеннических действий в зависимости от эффективности антифрод-процедур





XXXXXXXXXX

тысяч поколений назад. Поэтому, попадая в незапланированную ситуацию, мошенник, как обычный человек, действует эмоционально, допуская ошибки в своих действиях и оставляя за собой много улик (фактов). Если предположить, что вероятность ошибки мошенника при оформлении каждой кредитной заявки равна  $p$ , то по формуле обратной вероятности можно вычислить вероятность того, что мошенник ни разу не ошибется, оформив  $N$  заявок:

$$Q = \prod_{i=1}^N (1 - p_i) = (1 - p)^N. \quad (2)$$

Подставив в формулу (2) различные значения  $p$  и  $N$ , можно оценить шансы мошенника оформить  $N$  заявок без ошибок (табл. 3). Отметим, что на практике вероятность обнаружения мошенничества будет

Таблица 3

**Вероятность безошибочных действий мошенника  
в зависимости от количества заведенных заявок**

Кол-во заявок	Вероятность ошибки мошенника при оформлении одной кредитной заявки, %										
	1	5	10	15	20	25	30	35	40	45	50
1	99,0	95,0	90,0	85,0	80,0	75,0	70,0	65,0	60,0	55,0	50,0
2	98,0	90,3	81,0	72,3	64,0	56,3	49,0	42,3	36,0	30,3	25,0
3	97,0	85,7	72,9	61,4	51,2	42,2	34,3	27,5	21,6	16,6	12,5
4	96,1	81,5	65,6	52,2	41,0	31,6	24,0	17,9	13,0	9,2	6,3
5	95,1	77,4	59,0	44,4	32,8	23,7	16,8	11,6	7,8	5,0	3,1
6	94,1	73,5	53,1	37,7	26,2	17,8	11,8	7,5	4,7	2,8	1,6
7	93,2	69,8	47,8	32,1	21,0	13,3	8,2	4,9	2,8	1,5	0,8
8	92,3	66,3	43,0	27,2	16,8	10,0	5,8	3,2	1,7	0,8	0,4
9	91,4	63,0	38,7	23,2	13,4	7,5	4,0	2,1	1,0	0,5	0,2
10	90,4	59,9	34,9	19,7	10,7	5,6	2,8	1,3	0,6	0,3	0,1
11	89,5	56,9	31,4	16,7	8,6	4,2	2,0	0,9	0,4	0,1	0,0
12	88,6	54,0	28,2	14,2	6,9	3,2	1,4	0,6	0,2	0,1	0,0
13	87,8	51,3	25,4	12,1	5,5	2,4	1,0	0,4	0,1	0,0	0,0
14	86,9	48,8	22,9	10,3	4,4	1,8	0,7	0,2	0,1	0,0	0,0
15	86,0	46,3	20,6	8,7	3,5	1,3	0,5	0,2	0,0	0,0	0,0
16	85,1	44,0	18,5	7,4	2,8	1,0	0,3	0,1	0,0	0,0	0,0
17	84,3	41,8	16,7	6,3	2,3	0,8	0,2	0,1	0,0	0,0	0,0
18	83,5	39,7	15,0	5,4	1,8	0,6	0,2	0,0	0,0	0,0	0,0
19	82,6	37,7	13,5	4,6	1,4	0,4	0,1	0,0	0,0	0,0	0,0
20	81,8	35,8	12,2	3,9	1,2	0,3	0,1	0,0	0,0	0,0	0,0

---

## Выявление внутреннего мошенничества в розничном кредитовании

---

монотонно расти при увеличении количества оформленных заявок, так как большинство фактов (улик) построено на несоответствиях данных по нескольким заявкам. Для простоты расчетов мы приняли, что эти вероятности одинаковы, так как характер полученных результатов и общие выводы от этого упрощения не меняются.

Полученные данные демонстрируют, что если мошенник ошибается в более чем 10% случаев, то мошенничество может быть выявлено на ранних этапах (когда оформлено немного мошеннических заявок и потери банка незначительны). Для этого достаточно собирать улики (факты) в автоматизированном режиме, что и позволяет делать антифрод-система.

### Экономический эффект

Одним из наиболее важных вопросов перед внедрением антифрод-системы является оценка ее экономической эффективности. К сожалению, пока не существует единого объективного подхода к оценке экономического эффекта антифрод-системы, так как у правильно выстроенного антифрод-процесса есть превентивный эффект, оценка которого субъективна, поскольку построена на экспертных предположениях.

Если при внедрении антифрод-системы у банка нет собственной статистики по раскрытым случаям мошенничества, то можно обратиться к оценкам сторонних организаций. Так, например, компания «Эквифакс» оценивает уровень внутреннего и внешнего мошенничества по сектору розничного кредитования в 1–2% от общего объема выданных ссуд. Компания Ernst & Young дает оценку соотношения внутреннего и внешнего мошенничества по компаниям финансового сектора как 50 на 50 (по данным за 2014 г.). Перемножая эти цифры, можно получить оценку внутреннего мошенничества, которая составляет от 0,5 до 1% портфеля банка. Соответственно положительный экономический эффект будет достигаться, если стоимость антифрод-системы ниже, чем ее заявленная эффективность, умноженная на оценочные потери.

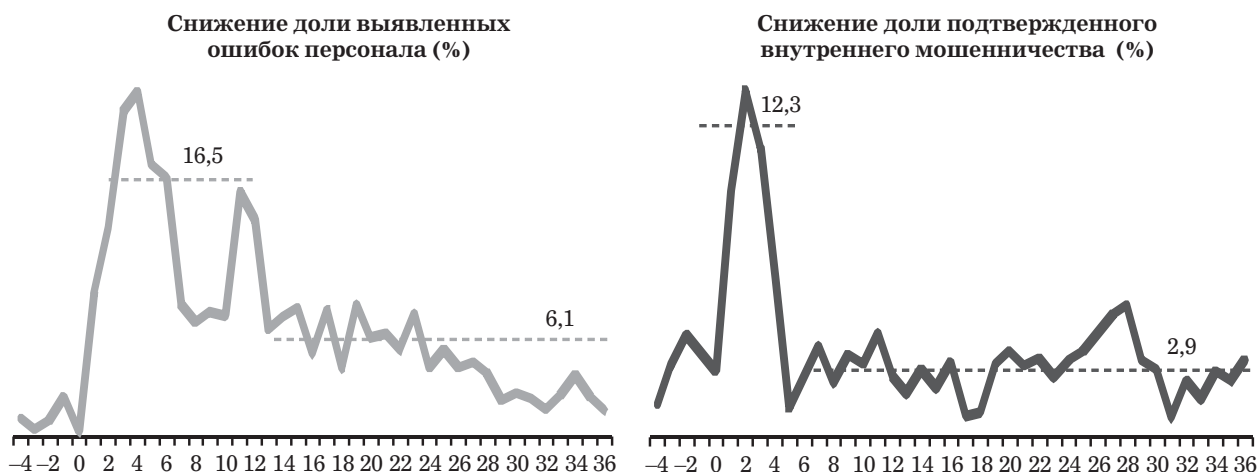
Наличие собственных статистических данных по внутреннему мошенничеству позволяет провести собственную оценку эффективности антифрод-системы. На рис. 5 показаны графики снижения уровня выявленных ошибок персонала и внутреннего мошенничества после внедрения антифрод-системы в крупном розничном банке. По горизонтальной оси отражены месяцы до и после внедрения антифрод-системы.

Из графиков видно, что после внедрения антифрод-системы уровень выявляемых ошибок за первый год работы системы составлял

XXXXXXXXXX

Рисунок 5

### Снижение уровня ошибок персонала и внутреннего мошенничества после внедрения антифрод-системы



16,5%, за последующие два года — 6,1% (средние значения за период). То есть уровень ошибок персонала за один год работы антифрод-системы упал в 2,7 раза.

Уровень подтвержденного внутреннего мошенничества за первые четыре месяца работы антифрод-системы составлял 12,3%, а в последующие месяцы — в среднем 2,9%. То есть уровень внутреннего мошенничества за четыре месяца работы антифрод-системы упал в 4,2 раза.

По этим данным можно сделать и противоположный вывод: эффективность антифрод-системы упала за несколько месяцев работы. На практике, если не внедрять новые правила и предикторы, снижение эффективности антифрод-системы неизбежно, поскольку мошенники быстро адаптируются, придумывая все более изощренные мошеннические схемы. Чтобы избежать снижения эффективности антифрод-системы, необходимо выстраивать антифрод-процесс по принципу «колесо науки», согласно которому аналитики регулярно разрабатывают новые предикторы и правила под новые мошеннические схемы.

В разобранном примере антифрод-процесс был встроен именно таким образом: новые предикторы разрабатывались регулярно, а антифрод-скоркарта пересчитывалась два раза в год. В пользу предположения о снижении уровня мошенничества говорил и факт снижения показателя *fpd90* (90-дневная просрочка на первом пла-

---

## Выявление внутреннего мошенничества в розничном кредитовании

---


теже), который принято считать первичным показателем уровня мошенничества в портфеле. Таким образом, если полученные результаты экстраполировать на весь портфель, используя оценки компаний «Эквифакс» и Ernst & Young, можно оценить превентивный эффект антифрод-системы в денежном эквиваленте.

Предположим, что за год банк выдает потребительских кредитов на 50 млрд руб. Тогда по данным «Эквифакса» и Ernst & Young уровень внутреннего мошенничества составляет 0,5–1% портфеля, то есть 250–500 млн руб. в год. После внедрения антифрод-системы уровень внутреннего мошенничества снизится в четыре раза, то есть на 187,5–375 млн руб. в год.

### Выводы

Считается, что внутреннее мошенничество возможно там, где есть уязвимости в бизнес-процессах. В современном банковском бизнесе с быстро меняющимися технологиями, продуктами и регуляторными требованиями проблема внутреннего мошенничества становится ключевой для бизнеса. Чтобы защититься от мошенничества в условиях быстро меняющегося рынка, банк может придерживаться одной из трех стратегий: (1) ничего не делать, работая по старым проверенным методам; (2) делать все долго, обдумывая каждую деталь внедряемого бизнес-процесса; (3) делать все быстро, вкладываясь в антифрод-технологии.

Выбирая первые две стратегии, банк, скорее всего, будет позади конкурентов. Третья стратегия позволит банку идти в ногу со временем в условиях быстро меняющегося рынка.

В данной статье мы разобрали полный цикл выявления внутреннего мошенничества в розничном банке. Чтобы эффективно противостоять внутреннему мошенничеству, банку необходимы защищенные процессы, качественные антифрод-процедуры и эффективная антифрод-система, которую должны поддерживать и развивать правильно мотивированные сотрудники. 

---

### Литература

1. Паклин Н.Б., Орешков В.И. (2012). Бизнес-аналитика: от данных к знаниям.
2. Чистяков В.П. (2000). Курс теории вероятностей.
3. Levitt S.D., Dubner S.J. (2006). Freakonomics.
4. Goleman D. (1995). Emotional Intelligence: Why It Can Matter More Than IQ.