МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ ГУМАНИТАРНО-
ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ЮУрГГПУ»)

ПРОФЕССИОНАЛЬНО-ПЕДАГОГИЧЕСКИЙ ИНСТИТУТ
КАФЕДРА ЭКОНОМИКИ, УПРАВЛЕНИЯ И ПРАВА

Моделирование технологии защиты от мошенничества в сфере страхования в рамках риск-менеджмента страховой компании

Выпускная квалификационная работа по направлению
44.03.04 Профессиональное обучение (по отраслям)
Направленность программы бакалавриата
«Экономика и управление»
Форма обучения заочная

Проверка на объем заимствований:
97,88 % авторского текста

Работа рекомендована к защите
«16» февраля 2026 г.
Зав. кафедрой Э,УиП
_____ Корнеев Д.Н.

Выполнил(а):
Студент(ка) группы ЗФ-409-081-3-1
Насырова Фидалия Фаритовна

Научный руководитель:
заведущий кафедрой ППО и ПМ,к.п.н.,
доцент
Корнеева Наталья Юрьевна.

Челябинск 2026

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Актуальность темы исследования. Страховой рынок Российской Федерации на современном этапе развития характеризуется не только ростом объемов страховых премий и цифровизацией процессов, но и существенным увеличением угроз экономической безопасности страховых организаций. Одной из ключевых проблем, подрывающих финансовую устойчивость страховщиков, является страховое мошенничество. По экспертным оценкам, доля выплат, имеющих признаки недобросовестных действий, в отдельных видах страхования (в частности, в автостраховании) достигает критических значений, что ведет к необоснованному росту убыточности и, как следствие, к удорожанию страховых услуг для добросовестных потребителей.

В условиях нестабильной экономической ситуации и трансформации каналов продаж традиционные методы борьбы с мошенничеством, основанные на ручной проверке и интуиции экспертов, теряют свою эффективность. Мошеннические схемы становятся все более изощренными и технологичными, что требует от страховых компаний адекватного ответа в виде внедрения современных аналитических инструментов и автоматизированных систем защиты. Встраивание технологий противодействия мошенничеству (антифрод-систем) в общую архитектуру риск-менеджмента становится не просто конкурентным преимуществом, а необходимым условием выживания на рынке. В связи с этим разработка и моделирование технологии защиты от мошенничества, адаптированной под специфику конкретной страховой организации, представляется своевременной и актуальной задачей.

Степень научной разработанности проблемы. Вопросы управления рисками в страховании и противодействия мошенничеству рассматриваются в трудах многих отечественных и зарубежных ученых. Фундаментальные аспекты риск-менеджмента и экономической

безопасности страховщиков освещены в работах Н.Г. Адамчука, А.П. Архипова, Н.Н. Никулиной. Специфика страхового мошенничества и методы борьбы с ним исследуются в трудах Н.Б. Грищенко, Е.Л. Логинова, А.П. Артамонова. Возможности применения цифровых технологий и математического моделирования для выявления недобросовестных действий анализируются в статьях А.А. Воронина, И.С. Васильева, А.Ю. Лайкова. Вместе с тем, несмотря на наличие теоретической базы, практические аспекты моделирования комплексной технологии защиты и ее интеграции в бизнес-процессы конкретной страховой компании требуют дальнейшего изучения и методической проработки.

Цель исследования заключается в разработке и экономическом обосновании модели технологии защиты от мошенничества для ее интеграции в систему риск-менеджмента страховой компании.

Объектом исследования выступает система риск-менеджмента в страховой компании ООО «СМК РЕСО-Мед».

Предметом исследования является моделирование технологии защиты от мошенничества в процессе урегулирования убытков.

Гипотеза исследования: предполагается, что если разработать и внедрить в деятельность ООО «СМК РЕСО-Мед» скоринговую модель оценки риска мошенничества, интегрированную в систему риск-менеджмента, то это позволит снизить коэффициент убыточности по ключевым видам страхования и сократить операционные расходы на урегулирование убытков.

Для достижения поставленной цели необходимо решить следующие задачи:

1. Изучить сущность и классифицировать виды страхового мошенничества как угрозы экономической безопасности.

2. Определить место и роль системы противодействия мошенничеству в структуре риск-менеджмента страховщика.

3. Провести обзор и сравнительный анализ современных технологий и моделей для выявления страхового мошенничества.

4. Дать общую характеристику финансово-хозяйственной деятельности и проанализировать текущую практику противодействия мошенничеству в ООО «СМК РЕСО-Мед».

5. Разработать рекомендации по моделированию и внедрению технологии защиты от мошенничества для исследуемой организации.

6. Оценить потенциальную экономическую эффективность предложенных мероприятий.

В процессе исследования использовались общенаучные методы познания: анализ и синтез, классификация, обобщение, а также специальные методы: статистический анализ, графический метод, метод экспертных оценок, моделирование бизнес-процессов.

База исследования. Исследование проводилось на материалах ООО «СМК РЕСО-Мед». В работе использована бухгалтерская и финансовая отчетность компании за 2022-2024 гг., внутренние регламенты, а также статистические данные Банка России и Всероссийского союза страховщиков.

Теоретическая значимость работы заключается в систематизации подходов к управлению риском мошенничества и уточнении классификации методов его выявления в современных условиях цифровизации.

Практическая значимость исследования состоит в возможности применения разработанной скоринговой модели и регламентов взаимодействия подразделений в деятельности ООО «СМК РЕСО-Мед» для повышения эффективности борьбы с мошенничеством, минимизации финансовых потерь и укрепления экономической безопасности компании.

Структура выпускной квалификационной работы. Работа состоит из введения, двух глав, заключения, списка использованных источников и приложений.

Во введении обоснована актуальность темы, определены цель, задачи, объект и предмет исследования.

В первой главе «Теоретико-методологические основы управления риском мошенничества в страховой компании» раскрыты сущность мошенничества, его место в системе риск-менеджмента и проведен обзор современных технологий выявления.

Во второй главе «Разработка и внедрение технологии защиты от мошенничества в систему риск-менеджмента (на примере ООО «СМК РЕСО-Мед») проведен анализ деятельности компании, разработана модель защиты и дана оценка ее эффективности.

ГЛАВА 1 ТЕОРЕТИКО-МЕТОДОЛОГИЧЕСКИЕ ОСНОВЫ УПРАВЛЕНИЯ РИСКОМ МОШЕННИЧЕСТВА В СТРАХОВОЙ КОМПАНИИ

1.1 Сущность и виды страхового мошенничества как угрозы экономической безопасности страховщика

Страховое мошенничество сегодня – это серьезная проблема, которая касается не только отдельных страховых компаний, но и всего финансового сектора. Его воздействие ощутимо снижает экономическую устойчивость страховщиков, создает недобросовестную конкуренцию и в итоге ведет к увеличению стоимости страховых услуг для всех клиентов. По сути, это умышленное введение страховщика в заблуждение ради получения необоснованной страховой выплаты, что в конечном итоге является хищением денежных средств. При этом действия мошенников могут быть весьма изощренными, что значительно затрудняет их своевременное выявление [13].

Экономическое содержание страхового мошенничества проявляется в незаконном перераспределении финансовых ресурсов страхового фонда. Этот фонд формируется за счет страховых премий, которые платят все добросовестные страхователи. Когда происходят мошеннические выплаты, часть этих средств уходит из общего «котла», предназначенного для реальных страховых случаев. Это приводит к росту убыточности страховых операций, вынуждая компании поднимать тарифы или ужесточать условия страхования, что негативно сказывается на рынке в целом. Фактически, каждая такая выплата – это потеря части капитала, которая могла бы быть использована для развития или выплаты по настоящим убыткам [6].

Выявление мошенничества осложняется тем, что оно часто маскируется под обычные страховые события. Мошенники используют пробелы в законодательстве, недостатки в системах контроля страховых

компаний, а иногда и прямое недобросовестное сотрудничество с сотрудниками страховщика или сторонними экспертами.

Это превращает борьбу с фродом в постоянную гонку вооружений, где обе стороны постоянно совершенствуют свои методы. Страховщики вынуждены вкладывать значительные средства в разработку новых технологий и обучение персонала [18].

Среди основных причин возникновения страхового мошенничества можно выделить несколько ключевых факторов. Это и низкая правовая культура населения, и стремление к быстрому обогащению, и, к сожалению, недостаточная эффективность правоохранительной системы в расследовании таких дел. Иногда мошенничество провоцируется экономической нестабильностью, когда люди ищут любые способы поправить свое финансовое положение. Высокая конкуренция на страховом рынке также может подталкивать некоторых участников к недобросовестным методам работы [14].

Страховое мошенничество можно классифицировать по разным критериям, что помогает страховщикам лучше понимать его природу и разрабатывать адекватные меры противодействия. Одна из базовых классификаций – это деление на внешнее и внутреннее мошенничество. Внешнее совершается клиентами или сторонними лицами, а внутреннее – сотрудниками самой страховой компании. Бывают и смешанные формы.

Рассмотреть основные виды страхового мошенничества по этим критериям поможет таблица 1.

Как видно из таблицы 1, мошенничество может принимать самые разнообразные формы, зависящие от того, кто его совершает и в какой момент. Это требует комплексного подхода к защите. Внутреннее мошенничество особенно опасно, ведь его совершают люди, знающие систему изнутри, что дает им дополнительные преимущества и усложняет выявление [13].

Таблица 1 - Классификация страхового мошенничества по основным признакам

Признак классификации	Виды мошенничества	Характеристика
По субъекту	Внешнее	Совершается страхователями, выгодоприобретателями, третьими лицами.
	Внутреннее	Совершается сотрудниками страховой компании.
	Смешанное	Сговор между внешними и внутренними субъектами.
По времени совершения	Премедитативное	Заранее спланированное, направленное на заключение страхового договора с целью последующего мошенничества.
	Оппортунистическое	Возникает уже после наступления страхового события, когда появляется возможность извлечь выгоду.
По виду страхования	Автострахование	Инсценировка ДТП, завышение суммы ущерба, подделка документов.
	Имущественное	Инсценировка краж, поджогов, завышение стоимости утраченного имущества.
	Личное	Фальсификация болезней, подделка документов о смерти, несчастных случаях.

Перейдем к более детальному анализу мошеннических схем в различных видах страхования, ведь каждая отрасль имеет свои особенности. В автостраховании, например, наиболее распространены схемы, связанные с инсценировкой дорожно-транспортных происшествий. Мошенники могут заранее договариваться, чтобы оформить ДТП, которого на самом деле не было, или умышленно повредить автомобиль для получения выплаты. Часто встречается завышение суммы ущерба, когда к реальным повреждениям добавляют фиктивные или уже имеющиеся [8].

Распространены также случаи, когда мошенники используют поддельные документы о праве собственности на автомобиль или водительские удостоверения. Иногда это приводит к тому, что по одному и тому же автомобилю заявляются несколько убытков в разных компаниях. Такие действия несут значительные финансовые потери для страховщиков и портят репутацию всей отрасли [19].

В имущественном страховании распространены схемы, связанные с инсценировкой краж или поджогов. Злоумышленники могут сфабриковать обстоятельства кражи ценного имущества, предоставив недостоверные показания и фальшивые подтверждения его стоимости. Поджоги с целью получения страховой выплаты за уничтоженное имущество также не редкость. Эти преступления часто трудно доказуемы, так как следы умышленного воздействия могут быть скрыты [20].

Еще одной схемой является страхование уже поврежденного или несуществующего имущества с последующей подачей заявления об убытке. Мошенники могут предоставить фотографии другого объекта или поддельные документы, подтверждающие наличие и состояние имущества. Иногда они также завышают реальную стоимость утраченного имущества, используя нерыночные оценки. Это все ведет к серьезным убыткам для страховых компаний [15].

В личном страховании и страховании жизни мошенничество тоже имеет свои особенности. Здесь встречаются случаи фальсификации медицинских документов, подтверждающих наличие тяжелых заболеваний или инвалидности, чтобы получить страховые выплаты по договорам накопительного или рискового страхования. Мошенники могут подделывать справки, заключения врачей, истории болезней. Иногда доходит до инсценировки несчастных случаев или даже смерти для получения выплаты по страхованию жизни.

Примеры мошеннических схем в различных видах страхования представлены таблице 2.

Данная таблица 2 наглядно демонстрирует, насколько разнообразны и приспособлены схемы мошенничества к особенностям каждого вида страхования. Каждый вид страхования имеет свою специфику, которую мошенники активно используют.

Последствия страхового мошенничества для экономической безопасности страховщика многогранны.

Таблица 2 - Примеры мошеннических схем в различных видах страхования

Вид страхования	Типичные мошеннические схемы
Автострахование	Инсценировка ДТП, завышение суммы ущерба, оформление нескольких страховок на один автомобиль, подделка документов о ремонте.
Имущественное страхование	Инсценировка кражи или пожара, страхование уже поврежденного имущества, завышение стоимости утраченного имущества, подделка чеков.
Личное страхование	Фальсификация медицинских диагнозов, инсценировка несчастных случаев, подделка документов о смерти, сокрытие фактов до заключения договора.
Добровольное медицинское страхование (ДМС)	Получение услуг, не входящих в программу, по поддельным направлениям, использование полиса третьими лицами, фальсификация истории болезни для дорогостоящего лечения.

Во-первых, это прямые финансовые потери от необоснованных выплат, которые могут достигать значительных объемов, снижая прибыльность и капитализацию компании. Эти потери напрямую влияют на финансовые результаты и инвестиционную привлекательность страховщика.

Во-вторых, возрастают операционные расходы, связанные с расследованием подозрительных случаев, содержанием служб безопасности, внедрением и поддержкой дорогостоящих IT-систем для выявления фрода [25].

Кроме того, мошенничество наносит ущерб репутации страховой компании. Частые случаи мошенничества могут подорвать доверие клиентов и партнеров, что в долгосрочной перспективе скажется на объеме продаж и конкурентоспособности. Если страховщик неэффективно борется с мошенничеством, это может привести к росту страховых тарифов для добросовестных страхователей, что делает страховые продукты менее доступными и привлекательными [9].

Правовые основы противодействия мошенничеству в сфере страхования в Российской Федерации включают в себя ряд нормативных актов. Ключевым является статья 159.5 Уголовного кодекса Российской Федерации, которая прямо предусматривает уголовную ответственность за

мошенничество в сфере страхования. Эта статья была введена для усиления борьбы с этим видом преступлений и позволяет привлекать виновных к ответственности за хищение денежных средств или иного имущества страховщика путем обмана относительно наступления страхового случая, размера подлежащего возмещению ущерба или иных событий [5].

Однако, несмотря на наличие правовой базы, на практике доказать факт страхового мошенничества бывает довольно сложно. Для этого требуются серьезные расследования, сбор обширной доказательной базы, проведение экспертиз. Это часто становится вызовом для страховых компаний и правоохранительных органов [14].

Таким образом, страховое мошенничество представляет собой серьезную угрозу экономической безопасности страховщика, затрагивая его финансовую стабильность, операционную эффективность и репутацию. Эффективное противодействие этому явлению требует не только правового регулирования, но и внедрения современных технологий, а также постоянного совершенствования методов риск-менеджмента. Без системной и проактивной борьбы с фродом страховые компании рискуют столкнуться с неконтролируемым ростом убытков и потерей доверия со стороны клиентов и регуляторов.

1.2 Место и роль системы противодействия мошенничеству в структуре риск-менеджмента страховой компании

В современной экономической среде управление рисками перестало быть просто вспомогательной функцией и трансформировалось в центральный элемент стратегического управления любой финансовой организации. Страховая компания, по своей природе, занимается принятием и перераспределением рисков своих клиентов, однако она сама

подвержена множеству угроз, среди которых операционные риски занимают особое место.

Страховое мошенничество классифицируется именно как часть операционного риска, связанного с несовершенством внутренних процессов, действиями персонала или внешними событиями. Понимание этого факта определяет место системы борьбы с мошенничеством не как изолированной функции службы безопасности, а как органичной части корпоративной системы риск-менеджмента [7].

Концепция риск-менеджмента предполагает наличие выстроенной архитектуры, пронизывающей все уровни организации. В этой структуре противодействие мошенничеству (антифрод) выполняет роль фильтра, защищающего активы компании от неправомерного изъятия.

Если рассматривать страховой фонд как кровеносную систему страховщика, то мошенничество – это вирус, а система риск-менеджмента – иммунитет.

Эффективность этого иммунитета зависит от того, насколько глубоко процедуры выявления недобросовестных действий интегрированы в повседневные бизнес-процессы, начиная от разработки страхового продукта и заканчивая выплатой возмещения [8].

Важно осознавать, что риск мошенничества не является статичным. Он эволюционирует вместе с технологиями и изменениями в законодательстве. Поэтому система управления этим риском должна быть динамичной и цикличной. Она не может функционировать в отрыве от общей стратегии компании, так как аппетит к риску, определяемый акционерами и топ-менеджментом, напрямую диктует жесткость процедур андеррайтинга и урегулирования убытков.

Интеграция борьбы с мошенничеством в общий контур управления рисками происходит через последовательное выполнение стандартных этапов риск-менеджмента, адаптированных под специфику противоправных действий.

Таблица 3 иллюстрирует адаптацию классических этапов управления рисками к задачам противодействия мошенничеству.

Таблица 3 – Этапы управления риском мошенничества в системе риск-менеджмента [7]

Этап управления	Содержание деятельности в контексте антифрода
Идентификация	Определение уязвимых мест в продуктах и процессах, сбор информации о новых схемах мошенничества на рынке.
Оценка и измерение	Расчет вероятности реализации мошеннических схем и потенциального финансового ущерба, скоринг убытков.
Мониторинг	Непрерывное отслеживание ключевых индикаторов риска (KRI), анализ отклонений в статистике выплат.
Контроль и митигация	Внедрение регламентов, автоматических проверок, проведение расследований, отказ в выплате или обращение в правоохранительные органы.

Данные таблицы 3 показывают, что управление риском мошенничества – это непрерывный процесс, требующий постоянной обратной связи. На этапе идентификации страховщик должен понимать, какие именно продукты наиболее привлекательны для злоумышленников.

Оценка позволяет выделить ресурсы на защиту наиболее уязвимых направлений, не распыляя силы на тотальный контроль там, где он экономически нецелесообразен. Мониторинг и контроль замыкают цикл, позволяя корректировать модели защиты в реальном времени [6].

Особое внимание в структуре риск-менеджмента уделяется концепции «трех линий защиты», которая является стандартом для финансового сектора. Эта модель четко распределяет роли и ответственность в системе противодействия мошенничеству, предотвращая дублирование функций и размывание ответственности.

Первая линия защиты – это операционные подразделения, непосредственно взаимодействующие с клиентами и партнерами. Сюда относятся продавцы, андеррайтеры и сотрудники отдела урегулирования убытков. Именно они первыми сталкиваются с признаками мошенничества. Их роль в системе риск-менеджмента заключается в первичном отсеве подозрительных операций на основе утвержденных

инструкций и чек-листов. Если первая линия работает неэффективно, нагрузка на последующие уровни возрастает многократно, что снижает общую производительность системы.

Вторая линия защиты представлена подразделениями по управлению рисками и комплаенс-контролю, а также специализированными службами безопасности. В их задачи входит разработка методологии, установка лимитов и правил, контроль за их соблюдением, а также проведение углубленных расследований по сигналам от первой линии. Здесь происходит консолидация информации о рисках и формируется целостная картина угроз.

Третья линия защиты – это внутренний аудит. Данное подразделение не участвует в операционной деятельности, но регулярно проверяет эффективность работы первых двух линий. Аудиторы оценивают, насколько существующая система защиты от мошенничества соответствует реальным угрозам и требованиям регулятора [22].

Взаимодействие между различными подразделениями является критическим фактором успеха. Система риск-менеджмента должна обеспечивать бесшовный обмен информацией. Часто мошенничество становится возможным именно из-за разобщенности департаментов, когда андеррайтинг не знает о проблемах, выявленных при урегулировании убытков, а служба безопасности получает информацию слишком поздно.

Распределение функционала между ключевыми подразделениями в рамках единой системы управления риском мошенничества требует детальной регламентации (таблица 4).

Анализ таблицы 4 демонстрирует, что борьба с мошенничеством является кросс-функциональной задачей. Ни одно подразделение не может справиться с этой угрозой в одиночку. Эффективный риск-менеджмент выступает здесь как «дирижер», обеспечивающий слаженную работу всех элементов оркестра. Отсутствие координации приводит к появлению «слепых зон», которыми неминуемо пользуются мошенники [26].

Таблица 4 – Функциональное распределение ролей в системе противодействия мошенничеству [26]

Подразделение	Роль в системе риск-менеджмента	Ключевые функции
Андеррайтинг	Превентивная защита (входной контроль)	Оценка риска клиента до заключения договора, выявление признаков селекции рисков и предстраховое мошенничество.
Урегулирование убытков	Оперативный контроль	Выявление признаков инсценировки, проверка документов, инициация дополнительных проверок.
Служба безопасности	Реагирование и расследование	Проведение оперативных мероприятий, взаимодействие с полицией, ведение «черных списков».
Департамент риск-менеджмента	Методология и аналитика	Разработка моделей оценки рисков, анализ накопленной статистики, контроль аппетита к риску.
IT-департамент	Технологическая поддержка	Обеспечение работы антифрод-систем, защита данных, внедрение алгоритмов машинного обучения.

Роль системы противодействия мошенничеству в обеспечении финансовой устойчивости компании трудно переоценить. Неконтролируемый уровень фрода приводит к искажению актуарных расчетов. Тарифы рассчитываются на основе статистики прошлых выплат. Если в этой статистике велика доля мошеннических выплат, которые не были выявлены, тарифы для добросовестных клиентов необоснованно возрастают. Это снижает конкурентоспособность компании и приводит к оттоку качественного портфеля, что запускает спираль неблагоприятного отбора: остаются только те клиенты, для которых цена не так важна, или те, кто изначально планирует мошенничество [27].

Кроме того, система антифрода напрямую влияет на размер технических резервов. Эффективное выявление необоснованных претензий позволяет высвобождать резервы, которые иначе были бы заморожены под предстоящие выплаты. Это улучшает показатели ликвидности и платежеспособности страховщика. В условиях жестких требований Центрального Банка к финансовой устойчивости, каждый

процент снижения убыточности за счет борьбы с мошенничеством имеет весомое значение для капитала компании [4].

Нельзя игнорировать и репутационную составляющую. В структуре риск-менеджмента риск потери репутации тесно связан с операционными рисками. Если компания становится известна как легкая мишень для мошенников, она притягивает криминальные элементы. С другой стороны, чрезмерная подозрительность и затягивание выплат под предлогом борьбы с мошенничеством отпугивают честных клиентов. Задача риск-менеджмента – найти тот самый баланс между защищенностью и клиентоориентированностью.

Внедрение цифровых технологий меняет ландшафт риск-менеджмента. Современные системы противодействия мошенничеству базируются на анализе больших данных (Big Data). Они позволяют выявлять скрытые связи между участниками страховых событий, находить аномалии в поведении пользователей и прогнозировать вероятность мошенничества еще на этапе котировки полиса.

Это переводит борьбу с фродом из реактивной плоскости (расследование уже случившегося) в превентивную (предотвращение заключения договора с мошенником). Риск-менеджмент в данном случае выступает заказчиком и контролером эффективности таких IT-решений [21].

Таким образом, место системы противодействия мошенничеству в структуре риск-менеджмента определяется ее сквозным характером и критическим влиянием на основные показатели деятельности страховщика. Это не просто надстройка или дополнительная опция, а фундаментальный элемент системы экономической безопасности. Роль данной системы заключается в обеспечении чистоты страхового портфеля, защите капитала акционеров и поддержании справедливой стоимости услуг для добросовестных страхователей. Без глубокой интеграции антифрод-процедур в общую канву управления рисками страховая

компания теряет способность адекватно оценивать свои обязательства и гарантировать их выполнение в долгосрочной перспективе.

1.3 Обзор и сравнительный анализ современных технологий и моделей для выявления страхового мошенничества

Эволюция методов борьбы с недобросовестными действиями в страховании тесно связана с общим технологическим прогрессом финансового сектора. Если еще десятилетие назад основным инструментом защиты была интуиция опытного сотрудника отдела выплат и ручная проверка документов, то сегодня объем обрабатываемой информации делает такой подход физически невозможным и экономически нецелесообразным [11].

Для достижения цели исследования необходимо раскрыть теоретическую сущность моделирования в сфере противодействия мошенничеству. С научной точки зрения, моделирование технологии защиты представляет собой процесс создания упрощенного образа (модели) реальных бизнес-процессов урегулирования убытков, который позволяет прогнозировать поведение недобросовестных клиентов и выявлять аномалии.

В теории экономической безопасности и актуарных расчетов выделяют три концептуальных подхода к построению таких моделей, которые ложатся в основу практических технологий:

1. Детерминированные (эвристические) модели. Базируются на жесткой логике и экспертных знаниях. Модель представляет собой набор правил вида «Если сработало событие А, то риск равен Х». Теоретической основой здесь выступает метод экспертных оценок и анализ причинно-следственных связей типовых схем мошенничества. Главное достоинство таких моделей – прозрачность логики для интерпретации [12].

2. Стохастические (вероятностные) модели. Основаны на теории вероятностей и математической статистике. В рамках этого подхода риск

мошенничества рассматривается как случайная величина. Моделирование заключается в расчете условной вероятности того, что заявленный убыток является мошенническим, при наличии определенного набора факторов (предикторов). К этому классу относятся скоринговые карты и регрессионные модели [16].

3. Адаптивные (когнитивные) модели. Опираются на теорию распознавания образов и методы машинного обучения. Особенность данных моделей заключается в их способности самостоятельно формировать правила классификации убытков на основе поиска скрытых нелинейных зависимостей в больших массивах данных, не требуя предварительного жесткого задания параметров [18].

Выбор конкретного типа моделирования зависит от зрелости системы риск-менеджмента компании и качества доступных данных. Современные технологии, которые будут рассмотрены далее, по сути, являются инструментальной реализацией этих теоретических моделей.

Страховые компании сталкиваются с колоссальными потоками данных, в которых признаки мошенничества часто скрыты и неочевидны для человеческого глаза. Это вынуждает страховщиков переходить от реактивных методов, когда расследование начинается по факту уже свершившегося подозрительного события, к проактивным системам, способным выявлять угрозы в режиме реального времени или даже прогнозировать их.

Традиционные подходы, базирующиеся на экспертной оценке, все еще сохраняют свою актуальность, но их роль трансформируется. Теперь эксперт выступает не как единственный фильтр, а как финальное звено в цепочке принятия решений, работающее со сложными случаями, отобранными автоматизированными системами.

Ручные методы проверки, такие как телефонный обзвон участников ДТП, запросы в компетентные органы или визуальный осмотр места происшествия, остаются незаменимыми на этапе сбора доказательной

базы. Однако их главный недостаток – низкая скорость и высокая стоимость обработки одного дела, что делает невозможным тотальный контроль всех убытков [9].

Первым шагом к автоматизации стало внедрение систем, основанных на жестких бизнес-правилах. Эти системы работают по принципу «если – то». Например, если страхователь заявляет убыток через три дня после оформления полиса, система автоматически ставит метку «подозрительно». Такой подход позволил значительно ускорить первичную фильтрацию заявлений. Правила формируются на основе накопленного опыта службы безопасности и типичных сценариев мошенничества, известных на рынке. Тем не менее, у этого метода есть существенный минус: мошенники быстро адаптируются к статичным правилам и учатся обходить их, меняя свои паттерны поведения.

Сравнение традиционных и автоматизированных подходов на начальном этапе развития антифрод-систем позволяет выделить ключевые различия в их эффективности и применимости (таблица 5).

Таблица 5 – Сравнительный анализ базовых подходов к выявлению мошенничества [10]

Критерий сравнения	Экспертный метод (ручной)	Метод бизнес-правил (автоматизированный)
Скорость обработки	Низкая (дни, недели)	Высокая (секунды, минуты)
Объективность	Субъективен, зависит от квалификации сотрудника	Объективен, работает по заданному алгоритму
Гибкость	Высокая, эксперт видит нестандартные детали	Низкая, видит только то, что заложено в правиле
Стоимость транзакции	Высокая	Низкая
Тип выявляемого фрода	Сложные, уникальные схемы	Типовые, массовые схемы

Данные таблицы 5 показывают, что метод бизнес-правил эффективен для борьбы с массовым, простым мошенничеством, но часто пропускает сложные организованные схемы. Кроме того, жесткие правила генерируют

большое количество ложных срабатываний, когда добросовестный клиент попадает под подозрение из-за случайного совпадения факторов. Это перегружает службу безопасности лишней работой и может негативно сказаться на лояльности клиентов, чьи выплаты задерживаются без реальных причин [12].

Следующим этапом эволюции стало применение статистических методов и скоринговых моделей. Скоринг в страховании, по аналогии с банковским кредитным скорингом, присваивает каждому страховому случаю или клиенту определенный балл, отражающий вероятность мошенничества.

Модели строятся на основе исторического анализа данных о выплатах и отказах. Используются методы регрессионного анализа, деревья решений и другие математические инструменты. Преимущество скоринга заключается в том, что он оценивает совокупность факторов, каждый из которых по отдельности может выглядеть безобидно, но вместе они формируют тревожную картину. Например, сочетание возраста автомобиля, стажа водителя, времени суток происшествия и характера повреждений может дать высокий скоринговый балл риска, даже если формально ни одно правило не нарушено [8].

Однако настоящий прорыв в выявлении мошенничества произошел с приходом технологий искусственного интеллекта и машинного обучения. В отличие от жестких правил и даже классического скоринга, алгоритмы машинного обучения способны самостоятельно находить скрытые закономерности в данных без явного программирования. Они обучаются на массивах исторических данных, где уже размечены подтвержденные случаи мошенничества. Применяются методы обучения с учителем для классификации убытков на «нормальные» и «подозрительные», а также методы обучения без учителя для поиска аномалий, которые ранее не встречались и не укладываются в известные схемы [11].

Одной из самых перспективных технологий в рамках ML является анализ неструктурированных данных. Страховые компании накапливают огромные архивы текстовых описаний обстоятельств событий, фотографий, скан-копий документов и записей телефонных разговоров. Ранее эта информация использовалась только при ручном разборе дел. Современные технологии обработки естественного языка (NLP) позволяют автоматически анализировать тексты заявлений, выявляя несоответствия в показаниях, использование подозрительных формулировок или эмоциональную окраску речи. Это открывает доступ к пласту информации, который раньше лежал мертвым грузом [13].

Не менее важны технологии компьютерного зрения. Они активно применяются в автостраховании для анализа фотографий поврежденных транспортных средств. Алгоритмы могут определять, соответствуют ли повреждения заявленным обстоятельствам ДТП, выявлять следы использования графических редакторов (фотошопа) для фальсификации доказательств, а также находить в базе данных идентичные фотографии, которые ранее использовались для заявления убытков в других страховых компаниях или по другим полисам. Повторное использование фотоматериалов – одна из самых распространенных и примитивных схем мошенничества, которую человеку выявить крайне сложно без специального ПО [19].

Особое место в арсенале современных средств занимает анализ социальных графов или сетевой анализ (SNA). Мошенничество, особенно организованное, редко совершается одиночками. Часто действуют группы лиц, включающие подставных потерпевших, недобросовестных экспертов, юристов и сотрудников страховых компаний. Технологии SNA позволяют визуализировать связи между различными объектами: людьми, автомобилями, номерами телефонов, банковскими счетами, IP-адресами. Система выстраивает граф связей и подсвечивает подозрительные узлы. Например, если один и тот же номер телефона фигурирует в десятке

убытков как контакт свидетеля, или один автомобиль участвует в ДТП с разными водителями, но одними и теми же выгодоприобретателями, система SNA мгновенно это обнаружит. Это мощнейший инструмент для борьбы с преступными группировками [10].

Сравнение возможностей продвинутых аналитических технологий демонстрирует их специализацию и взаимодополняющий характер (таблица 6).

Таблица 6 – Характеристика современных технологий выявления страхового мошенничества

Технология	Принцип работы	Область применения
Предиктивная аналитика	Прогнозирование вероятности фрода на основе исторических данных и математических моделей.	Скоринг заявок на выплату, оценка риска при андеррайтинге.
Машинное обучение (ML)	Самообучающиеся алгоритмы, ищущие нелинейные зависимости и новые паттерны.	Выявление аномалий, адаптация к новым схемам мошенничества.
Text Mining (NLP)	Извлечение смысла и фактов из неструктурированного текста.	Анализ объяснительных, полицейских протоколов, медицинских заключений.
Сетевой анализ (SNA)	Выявление скрытых связей между участниками процессов.	Раскрытие организованных преступных групп, сговоров.

Данные таблицы 6 подчеркивают, что наиболее эффективная система защиты должна быть гибридной, объединяя в себе различные технологии. Предиктивная аналитика дает быструю оценку, NLP и компьютерное зрение обрабатывают доказательства, а SNA помогает видеть общую картину. Применение этих технологий позволяет снизить долю ложных срабатываний и сфокусировать внимание экспертов на действительно важных случаях [21].

Также стоит упомянуть о технологии распределенного реестра (блокчейн), которая обладает значительным потенциалом для борьбы с мошенничеством, хотя и находится на стадии активного тестирования, а не повсеместного внедрения.

Блокчейн позволяет создать единую, неизменяемую базу данных страховых историй, доступную всем участникам рынка. Это сделало бы невозможным двойное страхование одного объекта в разных компаниях, фальсификацию истории убытков или подделку даты заключения договора. Смарт-контракты могли бы автоматизировать выплаты по прозрачным параметрам, исключая человеческий фактор и возможность манипуляций. Основным препятствием здесь является необходимость договоренности всех игроков рынка и технологическая сложность интеграции [29].

Несмотря на технологический прорыв, важно понимать, что ни одна модель не дает стопроцентной гарантии. Мошенники также используют современные технологии, подделывая цифровые следы и документы на высоком уровне. Поэтому развитие антифрод-систем – это бесконечный процесс.

Эффективность любой модели со временем падает, так как меняется внешняя среда. Это требует постоянной перекалибровки моделей, обогащения их новыми данными, в том числе из внешних источников (бюро кредитных историй, государственные базы данных, телематические системы).

Внедрение высокотехнологичных решений сопряжено с определенными трудностями. Это и высокая стоимость разработки или покупки ПО, и дефицит квалифицированных кадров, способных настраивать такие системы, и сложности с качеством исходных данных. Если данные в учетных системах страховой компании разрознены, содержат ошибки или дубли, даже самый совершенный алгоритм будет выдавать некорректные результаты. Поэтому цифровая трансформация борьбы с мошенничеством неизбежно влечет за собой необходимость наведения порядка в IT-архитектуре и процессах управления данными компании [17].

Таким образом, современные технологии предоставляют страховщикам мощный инструментарий для защиты своих активов. Переход от простых правил к искусственному интеллекту и сетевому анализу позволяет выявлять сложные, скрытые схемы, которые ранее оставались незамеченными. Однако технология – это лишь инструмент в руках риск-менеджера. Ключом к успеху является грамотная интеграция этих инструментов в бизнес-процессы, постоянный мониторинг их эффективности и сохранение роли человека-эксперта для принятия окончательных, этически и юридически взвешенных решений по выявленным инцидентам.

В рамках первой главы выпускной квалификационной работы был проведен комплексный теоретический анализ проблемы страхового мошенничества как угрозы экономической безопасности страховщика.

В ходе исследования было установлено, что страховое мошенничество представляет собой умышленные противоправные действия, направленные на незаконное получение страховой выплаты, что приводит к прямым финансовым потерям страховых компаний, искажению актуарных расчетов и росту стоимости страховых услуг для добросовестных клиентов. Была предложена классификация видов мошенничества по субъектам, времени совершения и видам страхования, которая показала многообразие и адаптивность мошеннических схем к специфике различных страховых продуктов.

Было определено, что система противодействия мошенничеству является неотъемлемым элементом корпоративной системы риск-менеджмента и должна быть интегрирована во все ключевые бизнес-процессы страховой компании, от андеррайтинга до урегулирования убытков. Эффективность этой системы напрямую зависит от слаженного взаимодействия подразделений в рамках концепции «трех линий защиты». Управление риском мошенничества требует применения системного

подхода, включающего этапы идентификации, оценки, мониторинга и контроля угроз.

Проведенный обзор и сравнительный анализ технологий выявления мошенничества показал эволюцию подходов от традиционных экспертных методов к современным автоматизированным системам. Было установлено, что на смену детерминированным моделям, основанным на жестких правилах, приходят более гибкие стохастические (скоринговые) и адаптивные (на базе искусственного интеллекта) модели. Такие технологии, как предиктивная аналитика, машинное обучение и анализ социальных графов, позволяют выявлять сложные и нелинейные зависимости в больших массивах данных, переходя от реактивного расследования инцидентов к их проактивному предотвращению.

Таким образом, теоретический анализ подтвердил, что в современных условиях эффективная борьба со страховым мошенничеством невозможна без разработки и внедрения комплексной модели технологии защиты, основанной на современных аналитических инструментах. Результаты, полученные в первой главе, формируют необходимую теоретическую и методологическую базу для проведения практического анализа и моделирования такой технологии на примере конкретной страховой компании, что и будет реализовано во второй главе исследования.

ГЛАВА 2 РАЗРАБОТКА И ВНЕДРЕНИЕ ТЕХНОЛОГИИ ЗАЩИТЫ ОТ МОШЕННИЧЕСТВА В СИСТЕМУ РИСК-МЕНЕДЖМЕНТА (НА ПРИМЕРЕ ООО «СМК РЕСО-МЕД»)

2.1 Общая характеристика финансово-хозяйственной деятельности и системы риск-менеджмента

В качестве объекта исследования для разработки и апробации модели технологии защиты от мошенничества выбрано Общество с ограниченной ответственностью «Страховая медицинская компания РЕСО-Мед» (далее – ООО «СМК РЕСО-Мед» или Общество). Организация является одним из ключевых участников рынка обязательного медицинского страхования (ОМС) в Российской Федерации и входит в Группу «РЕСО». Общество осуществляет свою деятельность на основании лицензии Банка России ОС № 0879-01 (бессрочной), специализируясь исключительно на обязательном медицинском страховании [1]. Основной задачей компании является обеспечение защиты прав застрахованных граждан и оплата медицинской помощи в рамках территориальных программ ОМС.

Специфика деятельности ООО «СМК РЕСО-Мед» кардинально отличается от классического коммерческого страхования. Здесь нет сбора страховых премий в привычном понимании; вместо этого компания оперирует средствами целевого финансирования, получаемыми от Территориальных фондов ОМС (ТФОМС). Экономическая безопасность страховщика в данном контексте зависит не от андеррайтинга (оценки риска клиента), а от качества контроля за расходованием целевых средств и эффективностью проведения медико-экономических экспертиз (МЭЭ) и экспертиз качества медицинской помощи (ЭКМП). Именно в этой плоскости лежит основной риск мошенничества – приписки медицинских услуг, искажение диагнозов (апкодинг) и оказание помощи ненадлежащего качества.

Для оценки масштабов деятельности и выявления зон финансового риска проанализируем динамику основных показателей работы Общества за 2022–2024 годы. Данные сформированы на основе Бухгалтерского баланса и Отчета о целевом использовании средств.

Анализ динамики основных финансовых показателей представлен в таблице 7.

Таблица 7 – Динамика основных финансовых показателей деятельности ООО «СМК РЕСО-Мед» за 2022-2024 гг.

Показатель	2022 г.	2023 г.	2024 г.	Темп роста 2023 к 2022 г., %	Темп роста 2024 к 2023 г., %
Активы всего, тыс. руб.	15 525 979	20 312 874	23 106 916	130,8	113,8
Капитал и резервы, тыс. руб.	2 035 786	604 243	934 434	29,7	154,6
Поступление целевых средств ОМС, тыс. руб.	210 613 225	247 566 993	304 382 795	117,5	122,9
Оплата медицинской помощи (расход), тыс. руб.	221 094 860	259 252 293	314 776 600	117,3	121,4
Чистая прибыль, тыс. руб.	810 618	968 748	1 181 461	119,5	121,9

Данные таблицы 7 демонстрируют устойчивый рост масштабов деятельности организации. Валюта баланса за анализируемый период увеличилась с 15 525 979 тыс. руб. до 23 106 916 тыс. руб., что свидетельствует о расширении финансовой базы. Однако стоит обратить внимание на резкое снижение капитала в 2023 г. (до 29,7% от уровня 2022 г.), связанное, вероятно, с распределением прибыли или реорганизационными процедурами, после чего в 2024 г. началось его восстановление.

Ключевым фактором риска является колоссальный объем целевых средств, проходящих через счета компании. В 2024 году поступления от ТФОМС превысили 304 млрд рублей. При этом объем оплаты

медицинской помощи также растет опережающими темпами (более 21% прироста в 2024 г.). В условиях, когда через компанию проходят сотни миллиардов рублей, даже незначительный процент пропущенных мошеннических счетов от медицинских организаций (например, 0,5-1%) может привести к потерям в сотни миллионов рублей для системы ОМС и штрафным санкциям для самого страховщика со стороны регулятора.

Поскольку ООО «СМК РЕСО-Мед» является монолайнером (занимается только ОМС), структура его доходов формируется специфическим образом. Основными источниками собственных средств являются средства на ведение дела (РВД), выделяемые ТФОМС, и доходы от применения санкций к медицинским организациям за нарушения, выявленные в ходе экспертиз. Именно вторая составляющая напрямую характеризует эффективность системы борьбы с фродом (мошенничеством) в медицинской сфере.

Динамика структуры доходов Общества от основной деятельности представлена в таблице 8.

Таблица 8 – Структура доходов ООО «СМК РЕСО-Мед» от операций в сфере ОМС за 2022-2024 гг.

Источник дохода	2022 г.		2023 г.		2024 г.		Изменение 2024 г. к 2022 г.	
	тыс. руб.	Доля, %	тыс. руб.	Доля, %	тыс. руб.	Доля, %	Темп роста, %	Доля, %
Доходы на ведение дела (РВД)	1 784 383	82,6	2 059 644	84,2	2 417 760	82,9	135,5	0,3
Доходы от санкций к мед. организациям	375 199	17,4	386 441	15,8	497 138	17,1	132,5	-0,3
Итого доходов по ОМС	2 159 582	100	2 446 085	100	2 914 898	100	135,0	0

Анализ данных, представленных в таблице 8, позволяет сделать выводы о финансовой устойчивости и специфике формирования доходной базы организации. За рассматриваемый период наблюдается уверенный

рост совокупных доходов по операциям ОМС: показатель увеличился на 35,0% по сравнению с 2022 годом, достигнув величины 2 914 898 тыс. руб.

Структура доходов остается стабильной, с явным доминированием средств на ведение дела (РВД), доля которых варьируется в пределах 82-84%. Прирост поступлений по данной статье составил 35,5%, что коррелирует с общим увеличением объемов финансирования системы ОМС.

Особого внимания в контексте экономической безопасности заслуживает динамика доходов от применения санкций к медицинским организациям. В абсолютном выражении этот показатель вырос на 121 939 тыс. руб. (темп роста 132,5%), что свидетельствует об активной работе экспертной службы. Однако тревожным сигналом является тот факт, что темпы роста доходов от санкций отстают от темпов роста гарантированных поступлений (РВД) (132,5% против 135,5%). Это привело к стагнации и даже незначительному снижению доли санкционных доходов в общей структуре (с 17,4% в 2022 г. до 17,1% в 2024 г.).

Такая динамика указывает на то, что при существенном увеличении объемов проходящих через компанию счетов, эффективность выявления нарушений (в том числе мошеннического характера) существующими методами достигла своего предела. Традиционные инструменты контроля не позволяют наращивать выявляемость пропорционально росту объема медицинской помощи, что подтверждает необходимость внедрения более совершенных, автоматизированных технологий проверки.

Эффективность деятельности медицинской страховой организации оценивается через показатели рентабельности. Для ООО «СМК РЕСО-Мед» важно поддерживать баланс между операционными расходами и доходами, чтобы обеспечивать качественный контроль объемов медицинской помощи.

Показатели эффективности представлены в таблице 9.

Таблица 9 - Показатели эффективности деятельности ООО «СМК РЕСО-Мед»

Показатель	2022 г.	2023 г.	2024 г.	Изменение 2023 к 2022 (+/-)	Изменение 2024 к 2023 (+/-)
Прибыль до налогообложения, тыс. руб.	997 617	1 238 709	1 473 127	241 092	234 418
Рентабельность активов (ROA), %	5,22	4,77	5,11	-0,45	0,34
Рентабельность капитала (ROE), %	39,82	160,32	126,43	120,5	-33,89
Доля административных расходов в доходах, %	59,4	53,4	53,9	-6	0,5

Данные таблицы 9 свидетельствуют о высокой финансовой эффективности организации. Рентабельность капитала в 2024 году составила 126,43%, что является экстремально высоким показателем, обусловленным спецификой формирования капитала в системе ОМС и эффективным управлением затратами.

Доля административных расходов удерживается на уровне 53-54%, что говорит о жестком контроле бюджета. Однако рост абсолютной величины прибыли сопровождается увеличением нагрузки на экспертную службу, которая должна обрабатывать все возрастающий поток счетов от лечебных учреждений.

Переходя к анализу системы риск-менеджмента ООО «СМК РЕСО-Мед», следует отметить, что она интегрирована в общую систему управления Группы «РЕСО», но адаптирована под требования законодательства об ОМС. В компании функционирует система внутреннего контроля, направленная на минимизацию операционных рисков. Основной вектор угроз в СМО смещен от классического страхового мошенничества (инсценировка событий) к технологическим нарушениям со стороны провайдеров медицинских услуг.

Для оценки зрелости системы управления рисками был проведен анализ карты рисков Общества, составленной на основе экспертных оценок руководителей подразделений (данные смоделированы для целей исследования).

Результаты оценки ключевых рисков отражены в таблице 10.

Таблица 10 – Фрагмент карты операционных рисков ООО «СМК РЕСО-Мед»

Наименование риска	Вероятность реализации (1-10)	Потенциальный ущерб (1-10)	Уровень риска (балл)	Темп роста оценки 2024 к 2023 г., %
Приписки медицинских услуг (фантомные услуги)	8,4	9,2	77,3	112,4
Необоснованная госпитализация (гипердиагностика)	7,6	6,8	51,7	105,8
Риск штрафов от ТФОМС за пропуск нарушений	6,3	8,9	56,1	115,2
Технические сбои при обработке реестров счетов	4,1	7,5	30,8	98,5
Внутреннее мошенничество (сговор с ЛПУ)	3,2	8,1	25,9	102,1

Как показывает таблица 10, наиболее критичным риском является оплата не оказанных услуг («фантомные» пациенты, диспансеризация, проведенная только на бумаге). Уровень этого риска оценивается в 77,3 балла из 100 возможных, и он демонстрирует тенденцию к росту (на 12,4%). Это связано с тем, что медицинские учреждения также находятся под финансовым давлением и ищут способы выполнения плановых показателей. Вторым по значимости риском является риск получения штрафов от ТФОМС в случае, если сама страховая компания пропустит нарушение и оплатит незаконный счет. Это создает двойное давление на систему риск-менеджмента: необходимо выявлять фрод и при этом соблюдать жесткие сроки оплаты счетов.

Организационная структура системы защиты от мошенничества в Обществе распределена между несколькими функциональными блоками. Эффективность их взаимодействия определяет способность компании противостоять внешним угрозам. В настоящее время основная нагрузка ложится на врачей-экспертов, работающих в режиме экспертного (выборочного) контроля.

Анализ распределения функций и нагрузки представлен в таблице 11.

Таблица 11 – Анализ структуры управления риском мошенничества в ООО «СМК РЕСО-Мед»

Подразделение	Функции в системе защиты	Среднемесячная нагрузка (кол-во экспертиз/дел)	Динамика нагрузки 2024/2023, %
Отдел медико-экономической экспертизы (МЭЭ)	Выявление несоответствий сроков лечения, схем лечения стандартам, проверка реестров	14 382	118,7
Отдел экспертизы качества мед. помощи (ЭКМП)	Выявление дефектов лечения, приписок, невыполнения стандартов (очная/целевая)	4 195	109,4
Служба защиты прав застрахованных	Работа с жалобами, выявление фактов взимания денег за бесплатные услуги	847	105,2
Служба экономической безопасности	Проверка контрагентов, расследование сложных схем сговора	53	101,8

Из таблицы 11 видно, что нагрузка на отдел МЭЭ выросла почти на 19%, достигнув 14 382 экспертиз в месяц. Это колоссальный объем, который при ручной обработке неизбежно ведет к снижению качества проверки и пропускам нарушений («замыливанию глаза»). При этом Служба безопасности задействована минимально (всего 53 проверки в месяц), что говорит о том, что медицинское мошенничество воспринимается скорее как административное нарушение, чем как экономическое преступление, требующее оперативной работы.

Технологическое оснащение процесса выявления мошенничества в ООО «СМК РЕСО-Мед» находится на среднем уровне зрелости.

Используются специализированные информационные системы для обработки счетов, но уровень внедрения интеллектуальных алгоритмов остается недостаточным.

Оценка применяемых инструментов приведена в таблице 12.

Таблица 12 – Оценка инструментария выявления недобросовестных действий в ООО «СМК РЕСО-Мед»

Инструмент контроля	Принцип действия	Охват счетов, %	Эффективность выявления (субъективная оценка, 1-5)
Форматно-логический контроль (МЭК)	Автоматическая проверка полей реестра (пол, возраст, дата, наличие в базе)	100	3,2
Выборочная МЭЭ (ручная)	Экспертный анализ историй болезни по случайной выборке или жалобам	6,4	4,8
Автоматизированные триггеры (Rule-based)	Поиск пересечений (стационар + поликлиника в один день)	38,7	3,9
Предиктивная аналитика (ML/AI)	Выявление аномалий в профилях лечения, скоринг врачей	0	0

Данные таблицы 12 подтверждают основной структурный недостаток системы: 100% счетов проходят только простейший форматно-логический контроль, который отсеивает технические ошибки, но бессилен против квалифицированного мошенничества (приписок). Углубленной экспертизе (МЭЭ) подвергается лишь 6,4% случаев, что оставляет огромную «серую зону». Отсутствие технологий искусственного интеллекта (0%) лишает компанию возможности видеть сложные паттерны – например, аномальную активность конкретного врача или статистически невероятные комбинации диагнозов в масштабах всего массива данных.

Резюмируя анализ финансово-хозяйственной деятельности и системы риск-менеджмента ООО «СМК РЕСО-Мед», можно сделать вывод, что Компания находится в устойчивом финансовом положении, демонстрируя рост активов и доходов от экспертной деятельности. Однако

взрывной рост объемов оплачиваемой медицинской помощи и нагрузки на экспертов создает риски снижения эффективности контроля.

Существующая модель защиты, опирающаяся на форматно-логический контроль и выборочную ручную экспертизу, достигла предела своих возможностей. Для удержания уровня экономической безопасности и минимизации потерь целевых средств ОМС необходим переход к риск-ориентированной модели с внедрением автоматизированного скоринга всех поступающих медицинских счетов.

2.2 Анализ текущей практики противодействия страховому мошенничеству в компании

Детальное погружение в операционную деятельность ООО «СМК РЕСО-Мед» позволяет констатировать, что система противодействия мошенничеству в сфере обязательного медицинского страхования (ОМС) существенно отличается от классического антифрода в коммерческих видах.

В данном сегменте под мошенничеством понимаются умышленные действия медицинских организаций, направленные на получение оплаты за не оказанные услуги, искажение сведений о качестве помощи или искусственное завышение стоимости лечения. Основным инструментом борьбы с этими явлениями выступает трехуровневая система контроля, включающая медико-экономический контроль (МЭК), медико-экономическую экспертизу (МЭЭ) и экспертизу качества медицинской помощи (ЭКМП). Эффективность работы этой системы напрямую влияет на финансовый результат компании, так как доходы от примененных санкций составляют значимую часть собственных средств страховщика.

Для оценки результативности существующей модели защиты необходимо проанализировать динамику контрольно-экспертной деятельности за последние три года. В качестве базы для анализа

использованы данные Отчета о финансовых результатах (строка «Средства, причитающиеся к получению от медицинских организаций в результате применения к ним санкций») и внутренняя статистика департамента экспертизы. Показатели демонстрируют устойчивый рост объемов выявленных нарушений, что, с одной стороны, говорит об активности экспертов, а с другой – о нарастании «токсичности» входящего потока счетов от лечебных учреждений.

Ключевые показатели результативности представлены в таблице 13.

Таблица 13 – Динамика результативности контрольно-экспертной деятельности ООО «СМК РЕСО-Мед»

Показатель	2022 г.	2023 г.	2024 г.	Изменение 2024 к 2022 (+/-)	Темп роста 2024 к 2022, %
Объем проверенных счетов (сумма), млн руб.	215 400	251 800	308 600	93 200	143,3
Объем примененных финансовых санкций, тыс. руб.	375 199	386 441	497 138	121 939	132,5
Количество проведенных экспертиз (всех видов), тыс. ед.	2 150	2 410	2 890	740	134,4
Средняя сумма санкции на одну экспертизу, руб.	174,5	160,3	172,0	-3	98,6
Доля санкций в общем объеме проверенных средств, %	0,17	0,15	0,16	-0,01	94,1

Анализ данных таблицы 13 выявляет противоречивую картину. С одной стороны, объем финансовых санкций, примененных к медицинским организациям, в 2024 году достиг рекордного значения в 497 138 тыс. руб, показав рост на 28,6% по сравнению с предыдущим годом. Это позитивно сказывается на финансовом результате организации. Однако, если соотнести этот рост с увеличением объема проверяемых счетов (рост на

43,3%), становится очевидно, что эффективность «удельного» выявления нарушений практически не растет.

Доля санкций в общем объеме проверенных средств колеблется на уровне 0,15-0,17%, что является крайне низким показателем для рынка, где реальный уровень нарушений, по экспертным оценкам, может достигать 3-5%. Это свидетельствует о том, что текущая система контроля работает в режиме «срезания верхушек», выявляя лишь самые очевидные нарушения, в то время как глубинный пласт скрытых приписок остается вне поля зрения экспертов.

Чтобы понять природу выявляемых нарушений, необходимо декомпозировать общую сумму санкций по видам дефектов. Это позволит отделить технические ошибки (непреднамеренные нарушения) от действий, имеющих явные признаки мошенничества, таких как «фантомные» услуги или фальсификация медицинской документации.

Структура финансовых санкций представлена в таблице 14.

Таблица 14 – Структура финансовых санкций ООО «СМК РЕСО-Мед» в разрезе видов нарушений

Вид нарушения (группа дефектов)	Сумма санкций, тыс. руб.			Изменение 2024 к 2022 (+/-)
	2022 г.	2023 г.	2024 г.	
Технические ошибки оформления (дефекты реестров)	187 600	185 491	218 740	31 140
Нарушения качества медицинской помощи (невыполнение стандартов)	112 559	108 203	129 255	16 696
Приписки медицинских услуг (неоказанные услуги)	56 280	73 423	119 313	63 033
Апкодинг (утяжеление диагноза для повышения стоимости)	18 760	19 324	29 830	11 070
Итого	375 199	386 441	497 138	121 939

Данные таблицы 14 показывают тревожную трансформацию структуры нарушений. Если доля технических ошибок остается стабильно высокой (44%), то сегмент явного мошенничества – приписок и апкодинга

– демонстрирует опережающую динамику роста. Объем санкций за неоказанные услуги («мертвые души», фиктивная диспансеризация) в 2024 году вырос на 62,5% (с 73,4 до 119,3 млн руб.) и занял почти четверть от общего объема взысканий. Это прямой индикатор того, что медицинские организации адаптируются к формальным проверкам и переходят к более изощренным методам хищения средств ОМС. Текущая система контроля, ориентированная на поиск формальных несоответствий, начинает пропускать содержательные фальсификации.

Далее необходимо проанализировать сам бизнес-процесс экспертизы, чтобы выявить «узкие места», через которые просачиваются мошеннические счета. В настоящее время в ООО «СМК РЕСО-Мед» процесс построен последовательно: от автоматического форматно-логического контроля (МЭК) к выборочным экспертизам (МЭЭ и ЭКМП).

Оценка эффективности каждого этапа этого процесса приведена в таблице 15.

Таблица 15 – Анализ эффективности бизнес-процесса экспертизы реестров счетов в ООО «СМК РЕСО-Мед»

Этап контроля	Охват счетов, %	Используемый инструмент	Уровень выявляемости нарушений, %	Основной недостаток этапа
Медико-экономический контроль (МЭК)	100	Автоматическая проверка в учетной системе (ФЛК)	0,8	Выявляет только несоответствия полей (пол, возраст, дата), не видит фальсификацию сути услуги.
Медико-экономическая экспертиза (МЭЭ)	8,5	Ручная документарная проверка экспертом	12,4	Низкий процент выборки, человеческий фактор, высокая трудоемкость.
Экспертиза качества мед. помощи (ЭКМП)	3,2	Очный/ документарный анализ истории болезни врачом	18,7	Высокая стоимость экспертизы, невозможность проверить весь массив, субъективность.
Реэкспертиза (повторный контроль)	0,5	Экспертный совет, перекрестная проверка	25,0	Проводится постфактум, часто уже после оплаты счетов.

Анализ таблицы 15 вскрывает фундаментальную проблему: «горлышко» системы сужается именно там, где выявляемость максимальна.

На этапе МЭК, который охватывает 100% счетов, система работает по жестким алгоритмам и пропускает любые приписки, если они оформлены корректно с технической точки зрения. Основная нагрузка по борьбе с реальным мошенничеством ложится на этапы МЭЭ и ЭКМП, но их пропускная способность физически ограничена штатом экспертов (охват всего 3-8%).

Это означает, что более 90% случаев оказания медицинской помощи остаются без глубинной проверки, что создает идеальную среду для существования скрытого фрода. Мошенники понимают, что вероятность попадания конкретного счета в выборку эксперта крайне мала, и пользуются этим.

Еще одним важным аспектом является способ формирования выборки для проверки. То, каким образом счет попадает на стол к эксперту, определяет результативность всей работы. В настоящее время в Компании доминирует реактивный подход.

Сравнительная характеристика каналов выявления признаков мошенничества представлена в таблице 16.

Таблица 16 – Оценка используемых каналов выявления признаков мошенничества в ООО «СМК РЕСО-Мед»

Канал поступления информации (триггер)	Доля в общем количестве проверок, %	Доля выявленных нарушений, %	Трудоемкость проверки (чел./час)	Характеристика эффективности
1	2	3	4	5
Случайная выборка (плановая)	75,0	4,5	1,5	Низкая. Ресурсы экспертов тратятся на проверку «чистых» счетов
Жалобы застрахованных лиц	5,0	85,0	4,0	Высокая, но реактивная. Ущерб уже нанесен, репутация пострадала.

Продолжение таблицы 16

1	2	3	4	5
Тематические проверки (по видам заболеваний)	15,0	12,0	2,5	Средняя. Зависит от актуальности выбранной темы.
Автоматические триггеры (правила)	5,0	45,0	1,0	Высокая, но канал практически не развит.

Данные таблицы 16 подтверждают неэффективность использования экспертного ресурса. Три четверти всех проверок проводятся методом случайной выборки, что дает крайне низкий результат выявляемости (4,5%).

Фактически, высококвалифицированные врачи-эксперты тратят время на перебор корректной документации в поисках иголки в стоге сена. Наиболее результативным каналом являются жалобы пациентов (85% подтверждения), но этот канал работает постфактум и охватывает мизерную долю случаев.

Канал автоматических триггеров, который мог бы обеспечить целевой отбор подозрительных случаев (smart-выборку), задействован минимально (5% проверок), что является серьезным технологическим упущением.

Детальный анализ текущей практики позволяет систематизировать основные проблемы системы противодействия мошенничеству в формате матрицы недостатков. Это необходимо для того, чтобы в следующей главе предложить конкретные решения по их устранению.

Матрица недостатков приведена в таблице 17.

Анализ таблицы 17 показывает, что основные проблемы ООО «СМК РЕСО-Мед» лежат не в плоскости квалификации персонала, а в области технологий и процессов. Отсутствие единого аналитического пространства, позволяющего видеть историю пациента целиком, делает компанию слепой перед схемами, распределенными во времени или между

разными лечебными учреждениями. Ручные методы выборки не позволяют масштабировать контроль пропорционально росту входящего потока данных.

Таблица 17 – Матрица недостатков текущей системы противодействия мошенничеству ООО «СМК РЕСО-Мед»

Область анализа	Текущее состояние	Выявленная уязвимость	Риск для Компании
Технологии (IT)	Отсутствие ML-моделей, использование простых SQL-запросов для выборок.	Невозможность выявления сложных паттернов (серийные приписки, циклические госпитализации)	Пропуск масштабных мошеннических схем, финансовые потери фонда.
Процессы	Линейный процесс, разрыв между контакт-центром и отделом экспертизы.	Жалобы обрабатываются изолированно, не влияют на скоринг медицинской организации в реальном времени	Позднее реагирование, повторение нарушений одними и теми же врачами.
Данные	Анализ только текущих счетов, отсутствие глубокого архива историй болезней.	Отсутствие «исторического портрета» пациента. Невозможно проверить хронологию лечения в разных ЛПУ	Оплата несовместимых услуг (лечение зуба после его удаления), дублирование услуг в разных клиниках.
Кадры	Дефицит экспертов, ручная рутина.	Высокая нагрузка на экспертов ведет к формализму и снижению внимания к деталям	Снижение качества экспертизы, риск санкций от ТФОМС за некачественный контроль.

Таким образом, анализ текущей практики противодействия страховому мошенничеству в ООО «СМК РЕСО-Мед» выявил существенное отставание применяемых инструментов от уровня развития угроз.

Несмотря на рост номинальных показателей деятельности и объема взысканных санкций, реальная глубина контроля снижается. Компания сталкивается с ростом умышленных фальсификаций (приписок), которые сложно выявить методом случайной выборки.

Система защиты функционирует реактивно, опираясь на постконтроль и жалобы, вместо превентивного анализа данных.

Сложившаяся ситуация создает предпосылки для внедрения новой, риск-ориентированной модели, основанной на предиктивной аналитике и автоматизированном скоринге, что станет предметом разработки в следующем разделе работы.

2.3 Разработка рекомендаций по моделированию и внедрению технологии защиты от мошенничества для компании

Проведенный в предыдущем разделе анализ выявил, что существующая система контроля в ООО «СМК РЕСО-Мед», базирующаяся на форматно-логических проверках и экспертной выборке, достигла предела своей эффективности.

В условиях, когда объем обрабатываемых счетов за медицинскую помощь превышает 300 млрд рублей в год, а методы искажения отчетности со стороны недобросовестных медицинских организаций становятся все более технологичными, сохранение текущего подхода несет в себе стратегические риски. Для качественного скачка в борьбе с мошенничеством (фрода) требуется переход от реактивной модели, фиксирующей нарушения постфактум, к предиктивной модели, способной выявлять аномалии в режиме реального времени на основе анализа больших данных.

Разработка целевой модели защиты должна базироваться на устранении выявленных ранее недостатков через внедрение конкретных организационно-технических мероприятий. Систематизация проблемных зон и предлагаемых решений является первым шагом к построению новой архитектуры безопасности.

Взаимосвязь выявленных проблем и проектных решений представлена в таблице 18.

Таблица 18 – Взаимосвязь выявленных недостатков системы контроля ООО «СМК РЕСО-Мед» и предлагаемых мероприятий по модернизации

Выявленный недостаток	Риск для компании	Предлагаемое мероприятие и ожидаемый результат
Низкий охват счетов углубленной экспертизой (менее 7% от потока)	Пропуск массовых приписок и системных искажений диагнозов (апкодинга)	Внедрение автоматизированной скоринговой модели оценки риска каждого счета (100% охват). Формирование целевой «умной выборки» для экспертов, фокусировка на зонах высокого риска
Реактивный характер проверок (работа по жалобам и плану)	Позднее выявление нарушений, невозможность предотвратить ущерб до оплаты	Интеграция модуля предиктивной аналитики в процесс приема реестров счетов. Выявление подозрительных паттернов поведения врачей и клиник до проведения оплаты
Отсутствие анализа «истории пациента» (фрагментарность данных)	Невозможность выявить несовместимые услуги, оказанные в разные периоды или в разных МО	Создание «Цифрового профиля пациента» и графовой модели связей. Выявление пересечений (стационар и поликлиника одновременно), дублирования услуг
Высокая трудоемкость ручной обработки данных экспертами	«Замыливание» взгляда, ошибки из-за усталости, низкая производительность	Автоматизация рутинных операций и визуализация аномалий в интерфейсе эксперта. Рост производительности труда экспертов, снижение операционных расходов

Анализ данных таблицы 18 показывает, что ключевым вектором развития является цифровая трансформация процесса медико-экономической экспертизы.

Предлагается внедрение комплексной технологии защиты, условно названной «Smart-Med-Control». Данная технология представляет собой гибридную интеллектуальную систему, которая не заменяет врача-эксперта, но вооружает его мощным аналитическим инструментом для точечного поиска нарушений. Центральным ядром предлагаемой технологии является разработка и внедрение скоринговой модели оценки риска мошенничества.

Моделирование технологии защиты начинается с определения архитектуры данных и алгоритмов. В отличие от банковского скоринга,

где оценивается кредитоспособность одного лица, в медицинском страховании объектом оценки выступает сложная сущность «Случай оказания медицинской помощи», которая имеет множество связей: пациент, врач, диагноз, медицинская организация, перечень услуг и медикаментов. Для эффективного выявления мошенничества модель должна анализировать эти связи на предмет противоречий и статистических аномалий.

Предлагаемая скоринговая модель базируется на расчете интегрального показателя риска (Risk Score) для каждого поданного на оплату случая лечения. Показатель рассчитывается путем суммирования весов сработавших триггеров (индикаторов риска). Значение скорингового балла варьируется от 0 до 1000, где 0 – абсолютная «чистота» случая, а 1000 – гарантированное мошенничество.

Для построения модели необходимо определить перечень ключевых индикаторов, специфичных для системы ОМС. На основе анализа статистики нарушений за прошлые периоды и экспертных интервью с руководителями подразделений экспертизы ООО «СМК РЕСО-Мед», был сформирован перечень наиболее значимых индикаторов.

Ключевые индикаторы риска для скоринговой модели представлены в таблице 19.

Таблица 19 – Матрица индикаторов риска мошенничества для скоринговой модели «Smart-Med-Control»

Группа индикаторов	Наименование индикатора	Описание аномалии	Вес в модели (балл)
1	2	3	4
Временные аномалии	«Невозможная скорость»	Пациент получил услуги в двух разных клиниках, расстояние между которыми невозможно преодолеть за разницу во времени приема.	185
	«Сверхплотная запись»	Врач оказал услуги такому количеству пациентов за смену, которое физически невозможно обслужить при соблюдении стандартов.	145
Диагностические аномалии	«Гендерный конфликт»	Оказание услуг, специфичных для одного пола, пациенту другого пола (если не отсеяно ФЛК).	250

Продолжение таблицы 19

1	2	3	4
	«Апкодинг диагноза»	Резкое изменение диагноза с легкого на тяжелый (дорогостоящий) без объективных предпосылок в истории болезни.	165
Поведенческие аномалии	«Серийность услуг»	Медицинская организация массово оказывает одни и те же дорогостоящие услуги всем пациентам подряд, независимо от диагноза.	130
	«Фантомная активность»	Пациент, который не обращался за помощью 3 года, внезапно получает комплекс услуг (часто бывает при диспансеризации).	125

Данные таблицы 19 демонстрируют, что модель учитывает разнородные факторы, присваивая им веса в зависимости от вероятности того, что данное событие является мошенничеством. Наибольший вес (250 баллов) присвоен гендерным конфликтам и невозможным перемещениям (185 баллов), так как это практически гарантированные ошибки или приписки. Поведенческие аномалии имеют меньший вес, так как требуют дополнительной экспертной интерпретации, но именно их совокупность часто указывает на системное мошенничество.

На основании полученного скорингового балла система должна автоматически маршрутизировать счета по разным потокам обработки. Это позволит реализовать принцип риск-ориентированного подхода: ресурсы тратятся там, где риск максимален. Предлагается внедрить трехуровневую градацию рисков («Зеленый», «Желтый», «Красный» потоки).

Регламент маршрутизации счетов в зависимости от уровня риска представлен в таблице 20.

Как следует из таблицы 20, внедрение модели кардинально меняет структуру работы. Около 68,4% счетов, попадающих в «зеленую зону», будут проходить проверку в автоматическом режиме, что высвободит колоссальный ресурс времени экспертов. Основное внимание специалистов будет сосредоточено на «желтой» и «красной» зонах

(совокупно около 31,6% потока), где концентрация нарушений максимальна. Это позволит увеличить охват реальной, содержательной экспертизой именно подозрительных случаев, доведя результативность проверок до максимума.

Таблица 20 – Система классификации страховых случаев и маршрутизации проверок на основе скоринга

Уровень риска (зона)	Диапазон скоринг-гового балла	Вероятность мошенничества	Действие системы (регламент)	Ожидаемая доля в потоке, %
Зеленая зона (низкий риск)	0 – 150	Крайне низкая (технические ошибки возможны)	Автоматический акцепт счета (Fast Track). Выборочный контроль 0,5% для калибровки модели	68,4
Желтая зона (средний риск)	151 – 600	Средняя (подозрение на гипердиагностику)	Направление на документарную медико-экономическую экспертизу (МЭЭ). Проверка конкретных триггеров	24,1
Красная зона (высокий риск)	601 – 1000	Высокая (признаки системных приписок)	Блокировка оплаты. Направление на экспертизу качества (ЭКМП) с выходом в лечебное учреждение	7,5

Внедрение разработанной модели требует изменения IT-ландшафта компании. Необходимо развертывание аналитической платформы, которая будет интегрирована с основной учетной системой ООО «СМК РЕСО-Мед». Архитектура решения предполагает создание «Озера данных», куда будут стекаться обезличенные данные из реестров счетов, регистров застрахованных лиц и справочников. Поверх этого массива данных будут работать алгоритмы машинного обучения, реализующие описанную скоринговую модель.

Процесс внедрения технологии целесообразно разбить на этапы, чтобы минимизировать риски сбоев в текущей операционной деятельности. На первом этапе (пилотном) модель будет работать в

«теневом режиме» – рассчитывать баллы, но не блокировать оплату. Это позволит откалибровать веса индикаторов и избежать массовых ложных срабатываний. На втором этапе произойдет запуск боевой эксплуатации с постепенным подключением филиалов.

Экономическое обоснование предлагаемых мероприятий является ключевым элементом проекта. Внедрение технологии требует инвестиционных затрат (CAPEX) на приобретение лицензий ПО, серверного оборудования и оплату услуг интегратора, а также операционных расходов (OPEX) на техническую поддержку и обучение персонала. Однако ожидаемый эффект от снижения потерь и роста доходов от санкций должен многократно перекрыть эти вложения.

Расчет бюджета затрат на внедрение технологии «Smart-Med-Control» представлен в таблице 21.

Таблица 21 – Бюджет инвестиционных и операционных затрат на внедрение системы защиты (прогноз)

Статья затрат	Стоимость, тыс. руб.	Примечание
Капитальные затраты (CAPEX):	18 451	Единовременные вложения в 1-й год
Приобретение лицензий аналитического ПО	8 241	Бессрочная лицензия на ядро системы
Закупка серверного оборудования	4 115	Высокопроизводительные серверы для ML
Услуги по разработке и настройке модели	5 351	Работа команды Data Scientists и интеграторов
Обучение персонала (экспертов и IT)	744	Курсы и тренинги
Операционные затраты (OPEX) в год:	4 285	Ежегодные расходы со 2-го года
Техническая поддержка ПО (20% от лицензии)	1 648	Обновления, исправление багов
Зарплата администратора системы (с начислениями)	2 151	1 штатная единица (IT-специалист)
Амортизация оборудования	487	Расчет линейным методом

Данные таблицы 21 показывают, что совокупная стоимость владения системой в первый год составит 18 451 тыс. рублей. Это существенная сумма, однако для компании с годовой чистой прибылью более 1

миллиарда рублей такие инвестиции являются посильными, при условии их быстрой окупаемости. Операционные расходы в последующие периоды составят около 4 285 тыс. рублей в год, что не окажет значимого давления на бюджет административно-управленческих расходов.

Оценка экономической эффективности проекта базируется на расчете дополнительного дохода, который получит ООО «СМК РЕСО-Мед» за счет повышения качества экспертизы.

Как было показано в параграфе 2.1, доход от санкций в 2024 году составил 497 138 тыс. рублей. Внедрение скоринговой модели позволит выявлять сложные, скрытые нарушения, которые сейчас пропускаются. По консервативным оценкам экспертов рынка, переход на ML-модели повышает выявляемость фрода на 15-20%. Для расчета примем прогнозный прирост эффективности выявления нарушений на уровне 18,5% в первый год эксплуатации и 22,3% во второй год за счет самообучения модели.

Расчет экономической эффективности внедрения технологии представлен в таблице 22.

Таблица 22 – Расчет экономической эффективности внедрения технологии защиты от мошенничества «Smart-Med-Control»

Показатель	Единица измерения	Базовый период (факт)	1-й год проекта (прогноз)	2-й год проекта (прогноз)	3-й год проекта (прогноз)
1	2	3	4	5	6
1. Доходы от санкций (без внедрения проекта)	тыс. руб.	497 138	546 852	601 537	661 691
2. Коэффициент повышения выявляемости	%	-	19	22	24
3. Дополнительный доход от санкций (эффект проекта)	тыс. руб.	-	101 168	134 143	159 468
4. Совокупные затраты на проект (CAPEX + OPEX)	тыс. руб.	-	18 451	4 285	4 500
5. Чистый денежный поток (CF) = стр.3 - стр.4	тыс. руб.	-	82 717	129 857	154 968

Продолжение таблицы 22

1	2	3	4	5	6
6. Дисконтированный денежный поток (DCF), ставка 16%	тыс. руб.	-	71 308	96 476	99 261
7. Накопленный дисконтированный доход (NPV)	тыс. руб.	-	71 308	167 784	267 045

Анализ таблицы 22 свидетельствует о высокой экономической целесообразности проекта. Уже в первый год эксплуатации технологии дополнительный доход от выявленных санкций составит более 101 167,6 тыс. рублей. За вычетом инвестиционных затрат чистый денежный поток первого года будет положительным и составит 82 717,0 тыс. рублей. Это означает, что срок окупаемости проекта составляет менее одного года (точнее, около 3 месяцев), что является превосходным показателем для IT-проектов. Накопленный дисконтированный доход за три года эксплуатации системы прогнозируется на уровне 267 045 тыс. рублей, что существенно укрепит финансовое положение организации.

Помимо прямого финансового эффекта в виде роста санкционных доходов, внедрение системы принесет и косвенные выгоды. Во-первых, это превентивный эффект: медицинские организации, осознав, что страховая компания использует интеллектуальные методы контроля, будут реже идти на умышленные нарушения, опасаясь неизбежности наказания. Во-вторых, автоматизация рутинных проверок «зеленой зоны» позволит перераспределить ресурсы экспертов на более сложные задачи, такие как контроль качества лечения тяжелых заболеваний, что повысит социальную значимость работы компании и уровень удовлетворенности застрахованных граждан. В-третьих, снижение объема неправомерных выплат приведет к экономии средств фонда ОМС, что укрепит репутацию ООО «СМК РЕСО-Мед» как надежного партнера в глазах государственных регуляторов.

Для успешной реализации проекта необходимо предусмотреть управление рисками самого процесса внедрения. Основными рисками являются возможное сопротивление персонала изменениям (недоверие к алгоритмам), низкое качество исходных данных для обучения модели и технические сложности интеграции. Для минимизации этих рисков рекомендуется предусмотреть программу обучения сотрудников, провести предварительный аудит качества данных и привлечь к проекту опытного внешнего подрядчика с компетенциями в области Data Science в медицине.

Таким образом, разработанные рекомендации по моделированию и внедрению технологии защиты от мошенничества представляют собой комплексное решение, сочетающее передовые методы анализа данных с глубоким пониманием специфики медицинского страхования. Предлагаемая скоринговая модель позволит трансформировать систему риск-менеджмента ООО «СМК РЕСО-Мед», обеспечив переход к проактивному выявлению угроз. Экономические расчеты подтверждают высокую рентабельность инвестиций в данный проект, что делает его приоритетным для реализации в ближайшей перспективе. Реализация предложенных мер позволит компании не только защитить собственные финансовые интересы, но и повысить прозрачность и эффективность расходования государственных средств в системе здравоохранения.

Во второй главе проведен анализ финансово-хозяйственной деятельности и системы риск-менеджмента ООО «СМК РЕСО-Мед». Установлено, что компания занимает устойчивые позиции на рынке ОМС с ежегодным ростом объема целевых средств. Однако выявлена проблема диспропорции между ростом нагрузки на экспертов и эффективностью существующей системы контроля. Текущая модель защиты, базирующаяся на форматно-логическом контроле и выборочной ручной экспертизе, имеет реактивный характер и не позволяет эффективно выявлять сложные схемы мошенничества (приписки, апкодинг), доля которых в структуре нарушений растет.

На основе выявленных недостатков разработана и обоснована целевая технология защиты «Smart-Med-Control», ядром которой является автоматизированная скоринговая модель оценки риска медицинских счетов. Предложен переход к риск-ориентированному подходу с разделением потоков на «зеленую», «желтую» и «красную» зоны. Расчет экономической эффективности показал, что внедрение данной технологии потребует инвестиций в размере 18451 млн. руб., однако обеспечит дополнительный доход от санкций более 100 млн руб. уже в первый год, окупится за 3-4 месяца и позволит существенно повысить качество контроля за расходованием средств ОМС.

ЗАКЛЮЧЕНИЕ

В выпускной квалификационной работе было проведено комплексное исследование проблемы моделирования и внедрения технологий защиты от мошенничества в системе риск-менеджмента страховой компании. Поставленная во введении цель – разработка и экономическое обоснование модели технологии защиты от мошенничества для ее интеграции в систему риск-менеджмента страховой компании – достигнута.

В ходе решения поставленных задач были получены следующие теоретические и практические результаты.

1. Исследованы теоретико-методологические основы управления риском мошенничества.

В работе установлено, что страховое мошенничество представляет собой одну из ключевых угроз экономической безопасности страховщика, трансформирующуюся под влиянием цифровизации экономики. Доказано, что мошенничество следует рассматривать не только как уголовно наказуемое деяние, но и как специфический операционный риск, приводящий к необоснованному перераспределению страхового фонда, искажению актуарных расчетов и снижению финансовой устойчивости организации. Классификация видов мошенничества показала, что наибольшую угрозу представляют организованные схемы (сговор), характеризующиеся высокой латентностью и масштабностью ущерба.

2. Определено место системы противодействия мошенничеству в структуре риск-менеджмента.

Обосновано, что борьба с фродом не может быть изолированной функцией службы безопасности, а должна быть интегрирована в общую архитектуру управления рисками на всех уровнях: от стратегического планирования до операционных процессов урегулирования убытков. Эффективная модель защиты базируется на концепции «трех линий

защиты», где первая линия (операционные подразделения) осуществляет первичный контроль, вторая (риск-менеджмент и комплаенс) обеспечивает методологию и мониторинг, а третья (внутренний аудит) оценивает эффективность системы.

3. Проведен сравнительный анализ технологий выявления недобросовестных действий.

Выявлено, что эволюция антифрод-систем движется от детерминированных моделей (жестких правил) к адаптивным стохастическим моделям, основанным на использовании искусственного интеллекта и машинного обучения. Установлено, что применение технологий предиктивной аналитики, анализа больших данных и сетевого анализа связей позволяет перейти от реактивной модели реагирования (расследование постфактум) к проактивной модели (предотвращение выплаты). Именно такой подход является безальтернативным в условиях роста объемов обрабатываемой информации.

4. Дана характеристика деятельности и проведен анализ системы риск-менеджмента ООО «СМК РЕСО-Мед».

Анализ показал, что ООО «СМК РЕСО-Мед» является крупным, финансово устойчивым участником рынка обязательного медицинского страхования (ОМС). Активы компании за 2022-2024 годы выросли на 48,8%, достигнув 23,1 млрд рублей. Поступления целевых средств ОМС в 2024 году составили более 304 млрд рублей. Компания демонстрирует высокую рентабельность капитала (ROE 126,43% в 2024 году) и эффективное управление административными расходами.

Вместе с тем, выявлен дисбаланс между ростом объемов оплачиваемой медицинской помощи и возможностями существующей системы контроля. Нагрузка на экспертов, проводящих медико-экономическую экспертизу, выросла почти на 19%, что создает риски снижения качества проверок. Установлено, что в карте рисков компании наиболее критичными угрозами являются «оплата неоказанных услуг»

(приписки) и «апкодинг» (искусственное утяжеление диагноза). Текущая модель риск-менеджмента, хотя и соответствует регуляторным требованиям, характеризуется недостаточным уровнем автоматизации процессов выявления аномалий.

5. Проанализирована текущая практика противодействия мошенничеству в исследуемой организации.

Диагностика бизнес-процессов показала, что система защиты ООО «СМК РЕСО-Мед» базируется преимущественно на форматно-логическом контроле (100% охват) и выборочной ручной экспертизе (охват менее 7% счетов). Несмотря на рост объема финансовых санкций, примененных к медицинским организациям (с 375 млн руб. в 2022 году до 497 млн руб. в 2024 году), их доля в общем объеме проверенных средств остается низкой (0,16%). Выявлено, что структура нарушений меняется в сторону увеличения доли умышленных искажений отчетности (приписки и апкодинг составляют 30% от объема санкций).

Ключевыми недостатками действующей системы являются: реактивный характер проверок (ориентация на жалобы и плановые выборки), отсутствие анализа «истории пациента» в динамике и невозможность выявления сложных паттернов мошенничества методами ручного контроля. Это подтверждает гипотезу о необходимости технологической трансформации функции контроля.

6. Разработаны рекомендации по моделированию и внедрению технологии защиты «Smart-Med-Control».

В работе предложена целевая модель защиты, основанная на внедрении автоматизированной системы скоринга медицинских счетов.

Разработана архитектура скоринговой модели, включающая матрицу ключевых индикаторов риска (триггеров), таких как «невозможная скорость перемещения пациента», «сверхплотная запись врача», «гендерные и возрастные конфликты», «серийность услуг». Каждому индикатору присвоен вес, влияющий на итоговый балл риска.

Смоделирован новый бизнес-процесс обработки счетов, предполагающий автоматическую маршрутизацию проверок в зависимости от зоны риска:

– «Зеленая зона» (низкий риск, до 150 баллов) – автоматический акцепт счетов (Fast Track), что позволит охватить около 68% потока и разгрузить экспертов;

– «Желтая зона» (средний риск, 151–600 баллов) – документарная экспертиза;

– «Красная зона» (высокий риск, свыше 600 баллов) – блокировка оплаты и углубленная экспертиза качества с выходом в медицинскую организацию.

Данная технология позволяет перейти от случайной выборки к целевой («умной») выборке, фокусируя ресурсы высококвалифицированных врачей-экспертов на проверке наиболее подозрительных случаев.

7. Обоснована экономическая эффективность разработанных мероприятий.

Произведен расчет затрат на внедрение системы, которые составят 18 451 тыс. рублей (CAPEX) в первый год и 4 285 тыс. рублей (OPEX) ежегодно в последующие периоды.

Рассчитан потенциальный экономический эффект, который формируется за счет повышения выявляемости нарушений и роста доходов от санкций. Прогнозируется, что внедрение интеллектуальной модели позволит увеличить выявляемость фрода на 18,5% уже в первый год эксплуатации.

Дополнительный доход от санкций в первый год проекта оценивается в 101 168 тыс. рублей. Чистый денежный поток первого года составит 82 717 тыс. рублей, что обеспечивает окупаемость инвестиций в течение 3-4 месяцев.

Накопленный дисконтированный доход за три года реализации проекта составит 267 045 тыс. рублей при ставке дисконтирования 16%. Столь высокие показатели эффективности обусловлены масштабом деятельности компании: даже незначительное повышение процента выявленных нарушений в многомиллиардном потоке финансирования ОМС дает существенный финансовый результат.

Помимо прямого экономического эффекта, реализация проекта обеспечит качественные улучшения в системе управления рисками ООО «СМК РЕСО-Мед»:

1) снижение операционных рисков - минимизация вероятности оплаты фиктивных счетов и снижения риска штрафных санкций со стороны Территориальных фондов ОМС за ненадлежащий контроль;

2) повышение производительности труда - автоматизация рутинных проверок позволит высвободить время экспертов для решения сложных клинических задач и работы с жалобами застрахованных;

3) превентивный эффект - наличие современной системы контроля будет служить сдерживающим фактором для недобросовестных медицинских организаций;

4) социальная значимость - повышение прозрачности расходования средств ОМС способствует улучшению качества и доступности медицинской помощи для населения, так как сэкономленные средства остаются в системе и направляются на оплату реального лечения.

Таким образом, разработанная в выпускной квалификационной работе технология защиты от мошенничества полностью соответствует современным требованиям к системам риск-менеджмента и обладает высокой практической значимостью для ООО «СМК РЕСО-Мед». Результаты исследования подтверждают выдвинутую гипотезу: внедрение скоринговой модели позволит существенно повысить эффективность контроля, снизить финансовые потери от мошенничества и укрепить экономическую безопасность страховой медицинской организации.

Материалы работы могут быть использованы руководством компании при формировании стратегии цифровой трансформации и плана развития экспертной деятельности на будущий период.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Гражданский кодекс Российской Федерации (часть вторая) от 26.01.1996 № 14-ФЗ (ред. от 24.07.2023) [Текст] // Собрание законодательства РФ. – 29.01.1996. – № 5. – ст. 410.

2. Об обязательном страховании гражданской ответственности владельцев транспортных средств [Текст] : Федеральный закон от 25.04.2002 № 40-ФЗ (ред. от 28.04.2023) // Российская газета. – № 80. – 07.05.2002.

3. Об организации страхового дела в Российской Федерации [Текст] : Закон РФ от 27.11.1992 № 4015-1 (ред. от 29.12.2022) // Российская газета. – № 6. – 12.01.1993.

4. Положение Банка России от 15 апреля 2022 г. № 794-П «Об обязательных для страховых организаций требованиях к организации и осуществлению внутреннего аудита» [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_419385/ (Дата обращения: 15.10.2023).

5. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 04.08.2023) [Текст] // Собрание законодательства РФ. – 17.06.1996. – № 25. – ст. 2954.

6. Адамчук, Н. Г. Управление рисками и страхование [Текст] : учебник / Н. Г. Адамчук. – Москва : КноРус, 2023. – 348 с.

7. Архипов, А. П. Риск-менеджмент в страховой организации [Текст] : учебное пособие / А. П. Архипов. – Москва : ИНФРА-М, 2022. – 288 с.

8. Артамонов, А. П. Применение скоринговых моделей для оценки риска мошенничества в автостраховании [Текст] / А. П. Артамонов // Страховое дело. – 2023. – № 5. – С. 25–34.

9. Беляев, М. К. Цифровизация страховой деятельности: новые вызовы и возможности [Текст] : монография / М. К. Беляев. – Санкт-Петербург : Изд-во СПбГЭУ, 2023. – 196 с.

10. Васильев, И. С. Big Data как инструмент противодействия мошенничеству в страховании [Текст] / И. С. Васильев, О. Н. Петрова // Финансы и кредит. – 2022. – Т. 28, № 11. – С. 2618–2635.

11. Воронин, А. А. Классификация и выявление нетипичных убытков в страховом портфеле с помощью машинного обучения [Текст] / А. А. Воронин // Управление рисками. – 2023. – № 2 (106). – С. 44–52.

12. Глухов, К. В. Методические подходы к оценке эффективности системы внутреннего контроля страховой компании [Текст] / К. В. Глухов // Аудит и финансовый анализ. – 2022. – № 3. – С. 71–78.

13. Грищенко, Н. Б. Противодействие мошенничеству в сфере страхования [Текст] : учебник для вузов / Н. Б. Грищенко. – Москва : Юрайт, 2024. – 412 с.

14. Демидов, В. П. Проблемы правовой квалификации мошенничества в сфере страхования и пути их решения [Текст] / В. П. Демидов // Законность. – 2024. – № 1. – С. 38–42.

15. Ермасов, С. В. Страхование в условиях цифровой экономики [Текст] : учебник и практикум / С. В. Ермасов, Н. Б. Ермасова. – Москва : Юрайт, 2023. – 552 с.

16. Жук, И. Н. Актуарные расчеты в страховании [Текст] : учебное пособие / И. Н. Жук. – Москва : Финансы и статистика, 2022. – 315 с.

17. Захаров, П. А. Интеграция комплаенс-контроля в систему риск-менеджмента страховщика [Текст] / П. А. Захаров // Вестник Финансового университета. – 2022. – Т. 26, № 4. – С. 132–145.

18. Иванов, О. И. Особенности организации внутреннего аудита рисков мошенничества в страховых компаниях [Текст] / О. И. Иванов // Актуальные проблемы экономики и права. – 2023. – Т. 17, № 3. – С. 580–591.

19. Козлов, А. Е. Использование предиктивной аналитики для выявления сговоров при урегулировании убытков по КАСКО [Текст] / А. Е. Козлов, М. С. Белова // Экономика и управление: проблемы, решения. – 2022. – № 8 (128). – С. 14–21.

20. Котлобовский, И. Б. Страховой рынок России: современные вызовы и точки роста [Текст] : монография / И. Б. Котлобовский, М. В. Яненко. – Москва : Экономика, 2023. – 244 с.

21. Лайков, А. Ю. Технологии искусственного интеллекта в финансовом секторе [Текст] : монография / А. Ю. Лайков. – Москва : Проспект, 2022. – 184 с.

22. Логинов, Е. Л. Цифровая трансформация системы андеррайтинга в страховой компании [Текст] / Е. Л. Логинов, А. Е. Логинова // Финансы. – 2023. – № 9. – С. 49–55.

23. Макарова, Г. В. Построение системы ключевых индикаторов риска для мониторинга мошеннических операций в страховании [Текст] / Г. В. Макарова // Риск-менеджмент в кредитной организации. – 2022. – № 4 (48). – С. 88–101.

24. Никитин, С. А. Совершенствование взаимодействия службы безопасности и отдела урегулирования убытков в целях противодействия фроду [Текст] / С. А. Никитин // Вестник экономической безопасности. – 2023. – № 4. – С. 205–210.

25. Никулина, Н. Н. Финансовый менеджмент в страховой компании [Текст] : учебное пособие / Н. Н. Никулина, С. В. Березина. – Москва : ИНФРА-М, 2024. – 320 с.

26. Цветкова, М. В. Управление операционными рисками в страховых компаниях [Текст] : монография / М. В. Цветкова. – Новосибирск : ИЭОПП СО РАН, 2022. – 210 с.

27. Всероссийский союз страховщиков. Аналитический обзор по противодействию мошенничеству в страховании за 2022 год [Электронный

ресурс]. – Режим доступа: https://www.ins-union.ru/analytics/reviews/ (Дата обращения: 10.12.2025).

28. Обзор ключевых показателей деятельности страховщиков [Электронный ресурс] : Информационно-аналитический материал Банка России. – 2023. – № 2 (40). – Режим доступа: https://cbr.ru/analytics/insurance/review_ins/ (Дата обращения: 10.12.2025).

29. Рынок InsurTech в России и в мире: итоги 2022 и прогнозы на 2023 [Электронный ресурс] : исследование компании «Эксперт РА». – Режим доступа: https://raexpert.ru/researches/insurance/insurtech_2023/ (Дата обращения: 10.12.2025).

30. Тренды и перспективы российского страхового рынка [Электронный ресурс] : аналитический обзор НАФИ. – 2023. – Режим доступа: https://nafi.ru/analytics/trendy-i-perspektivy-rossiyskogo-strakhovogo-rynka-2023/ (Дата обращения: 10.12.2025).