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:
92,44 % авторского текста

Работа *рекомендована* к защите
«15» 06 2025 г.
Зав. кафедрой ЭУ и П
_____ Корнеев Д.Н.

Выполнил(а):
студентка группы ЗФ-509-081-5-1
Антропова Юлия Владимировна

Научный руководитель:

Кандидат технических наук, доцент
Плужникова Ирина Ивановна

Челябинск
2025

СОДЕРЖАНИЕ

ВВЕДЕНИЕ……3

ГЛАВА 1. ТЕОРЕТИКО-МЕТОДОЛОГИЧЕСКИЕ ОСНОВЫ ЗАЩИТЫ ОТ СТРАХОВОГО МОШЕНИЧЕСТВА В РАМКАХ РИСК-МЕНЕДЖМЕНТА……....7

1.1 Понятие и сущность страхового мошенничества…….……....7

1.2 Информационные технологии и модели выявления страхового мошенничества……..……11

1.3 Организационно-правовые основы противодействия страховому мошенничеству в Российской Федерации……..……13

Выводы по первой главе……...18

ГЛАВА 2. МОДЕЛИРОВАНИЕ ТЕХНОЛОГИИ ЗАЩИТЫ ОТ СТРАХОВОГО МОШЕННИЧЕСТВА В КОНТЕКСТЕ РИСК-МЕНЕДЖМЕНТА..... 24

2.1 Изучение опыта работы страховой и продуктовой линейки компании «Совкомбанк страхование»……..24

2.2 Трансформация российского рынка страхования под влиянием инновационных технологий……28

2.3 Оценка эффективности антимошеннической стратегии страховой компании 38

Выводы по второй главе……...43

ЗАКЛЮЧЕНИЕ 51

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ 56

ВВЕДЕНИЕ

В настоящее время страхование стало одним из значимых финансовых секторов. Которое так же подвергается мошенническим нападкам. Страховые компании моделируют технологии защиты от мошенничества в сфере страхования в рамках риск-менеджмента, а именно внедряют финансовые технологии и инновационные подходы к разработке новых продуктов.

Актуальность исследования обусловлена частым мошенничество в сфере страхования — это серьёзная проблема, которая становится всё более актуальной и наносит значительный финансовый ущерб страховым компаниям по всему миру. Эта проблема требует внимания как со стороны регулирующих органов, так и от самих участников рынка — страховых компаний, посредников и профессиональных объединений.

Суть страхового мошенничества заключается в намеренном искажении информации с целью получения незаконных выплат или других преимуществ, которые противоречат условиям страхового полиса. Это имущественные преступления, которые совершаются на разных этапах оформления, действия или прекращения страхового договора.

Мошенничество может быть совершено как клиентами, так и сотрудниками страховых компаний, агентами, независимыми экспертами, представителями автосервисов, медицинских учреждений и других организаций. Более того, мошенничество может носить организованный и системный характер, включая так называемые «серые схемы» и картельные сговоры с участием различных посредников. В некоторых случаях в мошеннических действиях могут быть задействованы лица, обладающие служебным положением и административными полномочиями, что значительно усложняет их выявление и доказывание.

Степень разработанности темы в учебно-методической и научной литературе. В теоретической базе исследования используются справочные методики российских так же и зарубежных экономистов, и ученых. Которые занимаются развитием и проблемами рынка страхования, а также внедряют новые технологии защиты и анализа информации. Это такие ученные как Косаренко Н.Н., Ефимов О.Н., Томилова Н.А., Балабанов И.Т., Уайт Л.Дж., Фрэйм В.С. В своих работах ученный раскрывают проблемы связанные с защитой информации от мошенников на рынке страхования, а также методы защиты данных. Однако данная проблема мошенничества существует на данном этапе в сфере страхования и развивается так же быстро, как и сам рынок страхования и его информационная защита. Рынок страхования стремительными темпами переходит на цифровой обмен данными, усиливает защиту от утечки информации и в параллель с ними мошенники становятся более изощрёнными.

Актуальность рассматриваемой проблемы и специфика руководства проектной деятельностью обучающихся в процессе изучения экономических дисциплин обусловили выбор **темы исследования**: «Моделирование технологии защиты от мошенничества в сфере страхования в рамках риск-менеджмента страховой компании».

Цель исследования: теоретически обосновать и разработать методические рекомендации по защите от мошенничества в сфере страхования страховые компании.

Объект исследования: модели технологии защиты от мошенничества в сфере страхования в рамках риск-менеджмента страховой компании.

Предмет исследования: Моделирование технологии защиты от мошенничества в сфере страхования в рамках риск-менеджмента страховой компании.

Задачи исследования:

1. Проанализировать моделирование технологий защиты от мошенничества в сфере страхования в рамках риск-менеджмента в страховой компании.

2. Раскрыть методику риск-менеджмента страховой компании.

3. Выявить особенности мошенничества и риск-менеджмента в страховом рынке.

4. Изучить опыт защиты от мошенничества в проектной деятельности на примере страховой компании ПАО Совкомбанк Страхование.

5. Разработать методические рекомендации по защите от мошенничества.

Теоретико-методологической базой исследования выступили: федеральные законы и нормативно-законодательные акты Российской Федерации по вопросам финансовых технологий в страховании; аналитические материалы научно-практических конференций; экспертные сведения периодических изданий; справочные материалы и электронные системы информации; аналитическая и финансовая отчетность исследуемого объекта. Информационная база вполне репрезентативна, в связи с этим имеется надежная основа для создания комплексного подхода к совершенствованию деятельности современных банков.

Практическая значимость исследования состоит в том, что моделирование технологий защиты от мошенничества в сфера страхования

в рамках риск-менеджмента страховой компании могут быть использованы в ПАО Совкомбанк Страхование, а также и в других страховых компаниях.

В соответствии с целью и задачами в ходе данного исследования применялись следующие **методы:**

- законодательные: изучение законов по защите от мошеннических действие в сфере страхования;

– теоретические: анализ специальной литературы, синтез, обобщение, сравнение;

– эмпирические: наблюдение, анкетирование, анализ учебных материалов и педагогическое проектирование, направленное на разработку методических рекомендаций;

– количественной и качественной обработки данных: вычисление среднего арифметического значения, табулирование, построение диаграмм, интерпретация данных.

База исследования: исследование проводилось в течение 2024–2025 гг. на базе ПАО Совкомбанк Страхования, расположенного по адресу: 125284 г. Москва вн.тре.г. Муниципальный Округ Береговой, пр-кт Ленинградский д.35 стр.1

Структура исследования. Выпускная квалификационная работа включает в себя основные разделы: введение, две главы (теоретическую и практическую) с выводами по ним**,** заключение, список использованных источников (всего 34 источник). Работа изложена на 61 страницах.

ГЛАВА 1. ТЕОРЕТИКО-МЕТОДОЛОГИЧЕСКИЕ ОСНОВЫ ЗАЩИТЫ ОТ СТРАХОВОГО МОШЕННИЧЕСТВА В РАМКАХ РИСК-МЕНЕДЖМЕНТА

1.1. Понятие и сущность страхового мошенничества

Страховое мошенничество представляет собой преднамеренные действия, направленные на получение необоснованных выплат от страховых организаций. Оно может быть выражено как в умышленном искажении сведений при заключении договора страхования, так и в инсценировке страхового случая. Мошенничество в страховании наносит ущерб не только страховым компаниям, но и добросовестным страхователям, так как ведет к росту тарифов и снижению уровня доверия к системе страхования в целом.

Существует несколько классификаций страхового мошенничества. По субъекту его совершающего, различают: мошенничество со стороны страхователей; мошенничество, совершаемое сотрудниками страховых компаний; мошенничество с участием посредников (агентов, брокеров, экспертов).

По стадии совершения выделяют:

- Мошенничество при заключении договора (предоставление ложной информации);

- Мошенничество при наступлении страхового случая (инсценировка, преувеличение ущерба);

- Мошенничество на стадии урегулирования (представление фальсифицированных документов).

Кроме того, в зависимости от методов реализации мошеннических действий можно выделить:

- Активное мошенничество (инсценировка ДТП, поджог, повреждение имущества);

- Пассивное мошенничество (непредоставление информации, умолчание значимых фактов);

- Коллективное мошенничество (сговор между несколькими лицами).

Экономические последствия страхового мошенничества значительны: по различным оценкам, до 20% страховых выплат может приходиться на мошеннические действия. Это приводит к финансовым потерям компаний, росту цен на страховые продукты и снижению доступности страхования для населения. Таким образом, понимание сущности и форм страхового мошенничества является первым шагом на пути к формированию эффективной антимошеннической политики в рамках системы риск-менеджмента страховой компании.

Современная практика страхования характеризуется высокой степенью неопределенности и значительным уровнем рисков, включая риски мошенничества. В связи с этим управление этими рисками становится приоритетной задачей в рамках комплексной стратегии риск-менеджмента страховой компании. Под управлением рисками страхового мошенничества понимается совокупность организационных, правовых и аналитических мероприятий, направленных на идентификацию, оценку, минимизацию и мониторинг мошеннических угроз. На первом этапе важнейшей задачей является выявление потенциальных угроз. Для этого используется:

- Сбор и анализ исторических данных о страховых мошенничествах;

- Выявление уязвимостей в бизнес-процессах компании;

- Проведение интервью и анкетирования сотрудников, особенно в службах урегулирования убытков;

- Применение сценарного анализа и риск-карт;

- Использование внешних источников информации (базы данных ЦБ РФ, данные НАПФ, СМИ).

Идентификация рисков позволяет создать каталог рисков, ранжировать их по степени вероятности и значимости, а также подготовить базу для дальнейшего анализа.

Следующим этапом является количественная и качественная оценка выявленных рисков. Это может включать: оценку вероятности наступления мошеннического инцидента; анализ финансовых последствий реализации риска; построение матриц рисков (вероятность/влияние); применение статистических методов и моделей прогнозирования; использование методик экспертной оценки и Delphi-метода.

Оценка рисков служит основой для принятия управленческих решений и выделения приоритетных направлений профилактики мошенничества.

На данном этапе формируются конкретные мероприятия и процедуры, внедрение стандартных операционных процедур (СОП) при рассмотрении страховых случаев. Использование программ автоматизированного контроля и аналитики, регулярное обучение и повышение квалификации персонала. Организация службы внутреннего

контроля и аудита, закрепление ответственности за выявление мошенничества в должностных инструкциях.

Особое внимание уделяется созданию системы «двойного контроля» при принятии решений по спорным случаям, а также применению принципов разделения функций (segregation of duties).

Система управления рисками должна быть гибкой и адаптивной. Для этого необходимо:

– Регулярно пересматривать внутренние регламенты и процедуры;

– Анализировать тренды мошенничества и новые схемы;

– Оценивать эффективность реализуемых мероприятий (KPI);

– Проводить внутренние и внешние аудиты по вопросам противодействия мошенничеству;

– Обеспечивать обратную связь с клиентами, сотрудниками и государственными органами.

Мониторинг позволяет своевременно реагировать на возникающие угрозы и обеспечивать устойчивость антимошеннической стратегии.

– Эффективная борьба с мошенничеством невозможна без формирования внутри компании культуры нетерпимости к таким правонарушениям. Для этого:

– Разрабатываются и реализуются этические кодексы;

– Формируются каналы «горячей линии» для анонимного сообщения о злоупотреблениях;

– Внедряется система мотивации сотрудников за предотвращение мошенничества;

- Повышается прозрачность процедур и отчётности;
- Руководство демонстрирует приверженность принципам добросовестности и соблюдения законодательства.

1.2. Информационные технологии и модели выявления страхового мошенничества

С развитием цифровых технологий страховые компании получили возможность интегрировать современные инструменты анализа данных в процесс борьбы с мошенничеством. Информационные технологии позволяют не только ускорить обработку страховых дел, но и выявлять подозрительные случаи до момента принятия решения о выплате. Использование таких решений становится частью стратегического подхода к цифровой трансформации страховой отрасли.

Одним из ключевых инструментов в борьбе с мошенничеством стали специализированные ИТ-системы, позволяющие автоматизировать процесс анализа страховых дел. Сопоставляют данные страховых заявлений с типовыми шаблонами мошенничества, а также проверяют достоверность представленных сведений через внешние базы данных (ГИБДД, ФНС, Росреестр). Подсвечивают аномалии и повторяющиеся элементы (одинаковые адреса, контактные лица, телефоны и пр.). Создают по данным мошенничества портрет мошенника: его возраст, социальный статус, уровень дохода.

Современные модели на базе машинного обучения позволяют выявлять сложные корреляции, недоступные для традиционного анализа. Используемые алгоритмы:

- Классифицируют обращения как подозрительные или безопасные на основе обучающих выборок;

- Прогнозируют вероятность мошенничества с учетом поведения клиента, истории обращений, типов страхования;

- Используют нейросетевые модели для обработки неструктурированных данных (тексты заявлений, фото, видео);

- Обучаются на постоянно обновляемых данных, тем самым адаптируясь к новым схемам мошенничества;

- Повышают точность принятия решений при снижении числа ложноположительных срабатываний.

Big Data-технологии играют значительную роль в построении цифровых моделей поведения. Они: позволяют анализировать огромные массивы данных, включая социальные сети, телематические устройства, открытые базы данных; интегрируются с CRM-системами и системами клиентского анализа; используются для скоринга обращений, клиентского ранжирования и выявления нетипичных событий;

применяются для построения поведенческих моделей на основе многолетней статистики; способствуют формированию «черных списков» и базы подозрительных действий. Геоинформационные и визуальные технологии. Инструменты визуализации и пространственного анализа позволяют выявлять закономерности, скрытые при табличной обработке. Карты страховых событий позволяют определить аномальные кластеры активности. Анализ временных окон событий указывает на синхронные инциденты. Визуализация связей между участниками (клиентами, агентами, автосервисами) помогает выявить мошеннические группы. Применение графовых баз данных способствует более наглядному анализу сложных

структур. Интеграция с дронами, видеонаблюдением и геолокацией повышает точность подтверждения событий.

Примеры успешного внедрения ИТ-моделей в страховом секторе. Некоторые компании уже добились значительных успехов благодаря цифровым технологиям. Российские страховые организации внедрили системы анализа по принципу «красных флагов», выявляя более 70% подозрительных обращений. Зарубежные страховщики, такие как Allstate и Zurich Insurance, используют собственные антифрод-платформы на базе нейросетей. Компании активно используют «умные» мобильные приложения, фиксирующие факт страхового случая и отправляющие данные в режиме реального времени. Специализированные стартапы в сфере InsurTech предлагают решения по распознаванию фальсификаций документов и фотографий. Использование голосовой биометрии и анализа речи в колл-центрах позволяет выявлять повторяющихся мошенников.

1.3. Зарубежный опыт противодействия страховому мошенничеству и возможности адаптации в российской практике.

Изучение зарубежного опыта позволяет выявить эффективные практики противодействия страховому мошенничеству, которые могут быть адаптированы к российским условиям. Развитые страны накопили богатый опыт в создании институциональных, правовых и технологических механизмов борьбы с мошенничеством, обеспечивая прозрачность и устойчивость страховых рынков. Институциональные модели борьбы с мошенничеством

Во многих странах функционируют специализированные организации, координирующие усилия страхового сектора в борьбе с мошенничеством. В США действует Национальное бюро страховых преступлений (NICB), объединяющее страховые компании и правоохранительные органы. В Великобритании — Ассоциация по борьбе со страховым мошенничеством (IFB), которая управляет централизованной базой данных о подозрительных случаях. Германия действует Федеративное объединение страховщиков, занимающееся координацией антимошеннических мер на федеральном уровне. Нидерланды и странах Скандинавии внедрены национальные платформы обмена данными между страховщиками и государством. В Японии разработаны отраслевые стандарты и системы саморегулирования по выявлению мошенничества.

Законодательные и нормативные подходы в зарубежных странах играет ключевую роль в борьбе с мошенничеством. В США существует уголовная ответственность за страховое мошенничество на федеральном уровне, а во многих штатах работают специализированные прокуроры. В Великобритании принят Закон о мошенничестве (Fraud Act), в котором подробно описаны составы преступлений в сфере страхования. Страны ЕС внедрены директивы, обязывающие страховщиков внедрять системы внутреннего контроля и отчетности по подозрительным операциям.Во Франции предусмотрены механизмы принудительного возмещения ущерба, причиненного страховщикам, а в Австралии и Канаде реализуются совместные программы государственного и частного партнерства по контролю за страховыми выплатами.

Использование цифровых решений и аналитики, в зарубежных страховых компаниях активно используют цифровые инструменты для

борьбы с мошенничеством. Применяются решения на базе искусственного интеллекта для анализа страховых заявлений и анкет. Расширяется использование биометрии, блокчейн-технологий и автоматических триггеров для отслеживания подозрительных операций. Компании используют поведенческий скоринг и анализ эмоциональных реакций клиентов в ходе общения с операторами. В США и Канаде популярны платформы по обмену информацией между страховщиками в режиме реального времени. На международных платформах типа SAS Fraud Management используются глобальные алгоритмы и большие базы данных для выявления аномалий.

Роль страхового сообщества и профессиональных ассоциаций играют страховые ассоциации и саморегулируемые организации. Они разрабатывают и внедряют единые стандарты антимошеннической деятельности. Проводят профессиональную сертификацию сотрудников и агентов по вопросам этики и борьбы с мошенничеством. Организуют регулярные конференции и обучение по обмену практиками между странами, так же проходит создание рабочих групп по реагированию на новые виды мошенничества. Обеспечивают взаимодействие с органами государственной власти и международными организациями.

Возможности адаптации международного опыта в России может извлечь пользу из зарубежного опыта при соблюдении следующих условий, а именно создание централизованного координирующего органа, аналогичного NICB или IFB, внедрение обязательных стандартов антимошеннического контроля на уровне отрасли. Повышение открытости и обмена данными между страховщиками, включая участие в международных платформах, поддержка цифровой трансформации страховой отрасли государством и ЦБ РФ. Развитие

общественного доверия через просветительские и репутационные кампании.

Организационно-правовые механизмы борьбы со страховым мошенничеством в России представляют собой совокупность нормативных актов, институтов и процедур, направленных на предупреждение, выявление и пресечение мошеннических действий в страховой сфере. Эти меры реализуются на уровне законодательства, надзорной практики и внутрикорпоративной политики страховых компаний.

Законодательное регулирование борьбы со страховым мошенничеством составляет Уголовный кодекс РФ, в частности статья 159.5 «Мошенничество в сфере страхования», предусматривающая уголовную ответственность за противоправные действия в целях незаконного получения страховой выплаты. Дополнительно применяются нормы:

- Гражданского кодекса РФ — в части регулирования обязательств по страхованию;
- Закона «Об организации страхового дела в Российской Федерации» № 4015-1 — устанавливает требования к лицензированию, отчетности и стандартам деятельности страховщиков;
- Кодекса РФ об административных правонарушениях — в части ответственности за нарушение условий договора страхования;
- Федерального закона «О противодействии легализации доходов, полученных преступным путем» — при рассмотрении подозрительных операций.

- Правовая база постоянно обновляется с учетом роста цифровизации и появления новых форм мошенничества.

Роль Центрального банка Российской Федерации выполняет функции мегарегулятора страхового рынка, и в его полномочия входит, контроль за соблюдением законодательства страховыми компаниями. Так проводит ряд проверок и расследований при наличии признаков мошенничества. При выявлениях систематических нарушений грозит страховым компаниям отзыв лицензии. Обобщение и публикация статистики по обращениям граждан и страховых споров. Разработка методических рекомендаций и разъяснений для страхового сектора.

ЦБ РФ также курирует межведомственные инициативы, направленные на цифровую трансформацию антимошеннической деятельности.

В рамках борьбы с мошенничеством важное значение имеет оперативное и правовое сотрудничество между страховщиками и правоохранительными структурами. Страховые компании обязаны уведомлять органы внутренних дел о признаках преступлений, выявленных в ходе своей деятельности, МВД РФ имеет специализированные подразделения по борьбе с экономическими преступлениями, в том числе в страховой сфере. Проводятся совместные расследования, обыски, опросы свидетелей и фигурантов, осуществляется передача материалов из страховых компаний по фактам подозрительных обращений. Налажены каналы межведомственного взаимодействия через прокуратуру, суды и следственные органы.

В страховой отрасли действуют профессиональные объединения, играющие важную роль в развитии культуры противодействия мошенничеству. СРО устанавливают стандарты ведения страховой

деятельности, включая меры внутреннего контроля и комплекса. Организуют курсы повышения квалификации, семинары и вебинары для сотрудников страховых организаций. Ведут базы данных подозрительных случаев и черных списков недобросовестных агентов. Содействуют внедрению единых цифровых платформ для анализа обращений и урегулирования убытков. Участвуют в подготовке инициатив по изменению законодательства.

Каждая страховая компания обязана формировать внутреннюю нормативную базу по борьбе с мошенничеством. В неё входят:

- Антимошенническая политика компании и кодексы этики;
- Регламенты проверки страховых случаев и документов;
- Порядок взаимодействия с клиентами при подозрении на мошенничество;
- Процедуры внутреннего аудита, отчетности и хранения информации;
- Механизмы реагирования на выявленные нарушения (включая дисциплинарные меры).

Эти меры позволяют создать многоуровневую систему контроля, обеспечивающую своевременное выявление и предотвращение мошенничества.

Выводы по первой главе

Последствия страхового мошенничества не ограничиваются прямым экономическим ущербом, понесённым страховыми

организациями. Они затрагивают широкие пласты экономики и общества, подрывая доверие к финансовым институтам, способствуя росту недовольства потребителей и искажая принципы справедливого распределения ресурсов. Ниже рассмотрим ключевые аспекты таких последствий. Прямые убытки от мошенничества составляют значительную долю в общем объёме страховых выплат. По оценкам экспертов, от 10% до 25% выплат приходится на мошеннические обращения. Эти потери для доходности страхового бизнеса. Компании начинают увеличивать резервы на сомнительные случаи, за счет чего происходит повышение тарифов на страхование для клиентов страховых компаний. Снижают инвестиционную привлекательность сектора. Кроме того, рост мошенничества вынуждает страховщиков инвестировать значительные средства в антимошеннические технологии и обучение персонала, что увеличивает операционные издержки.

Для компенсации убытков от мошенничества страховщики часто прибегают к повышению стоимости страховых продуктов. Это приводит к удорожанию страхования для добросовестных клиентов, а ведет это все к снижению количества застрахованных лиц и объектов. Росту числа отказов от добровольных видов страхования (например, КАСКО, ДМС, НС). Ухудшению восприятия страхования как социально полезного института.

Нарушение справедливости и снижение доверия к институту страхования. Обнаружение фактов мошенничества, особенно резонансных, приводит к росту общественного недоверия. Возникает ощущение безнаказанности злоумышленников, в связи с этим растёт подозрительность к работе страховых компаний. Увеличивается число конфликтов между клиентами и страховщиками которые как правило заканчиваются судебными процессами, нарастает негатив со стороны

клиента. В то время как добросовестные страхователи подвергаются излишнему контролю и проверкам, это все влияет на имидж страхового сектора и тормозит его развитие.

Возникает угроза финансовой не стабильности и увеличиваются системные риски, что провоцирует недостаточность резервов у страховых организаций, а так же ухудшение финансовых показателей компаний (solvency, ликвидность). Массовые банкротства небольших и региональных страховщиков, ухудшение позиций российского страхования на международном уровне. Особенно остро такие угрозы проявляются при масштабных мошеннических схемах, вовлекающих множество компаний, агентов и клиентов.

Дестабилизация смежных рынков и отраслей негативное влияние распространяется и на другие сектора банковскую сферу при залоговом и ипотечном страховании. Автомобильный рынок в связи с массовыми случаями инсценировок ДТП и автоподстав. Здравоохранение через злоупотребления в ДМС. Юридические и оценочные услуги при фальсификации документов.

Происходит рост нагрузки на судебную и правоохранительную систему, факты мошенничества влекут за собой. Увеличение количества гражданских и уголовных дел, рост судебных издержек страховых компаний, перегрузку следственных органов и судов. Сложности в доказывании вины и обжаловании решений. Нередко дела по страховым мошенничествам затягиваются, а злоумышленники избегают ответственности, что дополнительно снижает эффект превенции.

Социальные последствия и моральные издержки мошенничество в страховании порождает распространение девиантных форм поведения, снижение правовой культуры населения. Рост

недоверия к государственным институтам формирование «серых зон» в экономике.

На уровне конкретного человека это может привести к ощущению социальной несправедливости, демотивации добропорядочного поведения, искаженному восприятию норм морали и закона.

Понимание психологических и поведенческих аспектов страхового мошенничества играет важную роль в разработке эффективных превентивных стратегий. Мошенничество — это не только правонарушение, но и результат определённых мотиваций, личностных качеств, восприятия социальной нормы и внешних обстоятельств. Изучение этих факторов позволяет выявлять потенциальные угрозы до их реализации. Мотивационные факторы страхового мошенничества среди людей находят массу причин, среди которых финансовые трудности, необходимость получить средства в условиях экономического давления. Ощущение несправедливости: убеждение, что страховые компании сами ведут нечестную игру. Легкость получения выгоды: восприятие мошенничества как «быстрого и простого» дохода. Оправданность действий: «возврат» уплаченных ранее взносов как форма личной компенсации. Влияние окружения: наличие аналогичных примеров среди знакомых, родственников.

Часто мотивация строится на внутреннем конфликте между моральными нормами и материальной выгодой, где второе берёт верх.

Существуют также поведенческие модели мошенников, можно выделить более яркие шаблоны в поведении. Манипулятивное поведение: активное убеждение в своей правоте, давление на сотрудников. Противоречивые объяснения: изменяющиеся версии событий при расследовании. Избыточная активность: частые обращения,

желание ускорить выплаты, проявление нетерпения. Эмоциональное воздействие: использование жалости, угроз или демонстрация агрессии. Уклонение от предоставления информации: затягивание сроков, частичная подача документов.

Подобные модели часто фиксируются в базах данных антимошеннических систем и становятся основой для оценки риска обращения.

Роль когнитивных и социальных искажений мошенника, они нередко подвержены искажённому восприятию реальности. «эффект ложного консенсуса»: убеждение, что «все так делают», «рационализация вреда»: минимизация последствий и отрицание вреда для общества. «Моральное исключение»: отделение себя от общих правил морали и закона. «Феномен анонимности»: ощущение безнаказанности в цифровой среде. Социальное давление: стремление к поддержанию статуса через незаконное обогащение.Эти искажения затрудняют профилактическое воздействие простыми методами убеждения или информирования.

На основе исследований можно выделить общие черты потенциальных мошенников это люди склоны к риску и авантюрам. У них высокий уровень рационализации и самооправдания, за частую они верят в то, что все делают правильно. Пониженный уровень эмпатии к чужим потерям, люди более жесткие. Конформизм и чувствительность к мнению окружающих. Часто наличие предыдущего негативного опыта общения со страховыми компаниями.

Однако важно понимать, что единый психологический портрет отсутствует — мотивации и черты могут варьироваться в зависимости от обстоятельств и вида страхования.

Противодействие мошенничеству требует учёта поведенческих и психологических факторов. Использование поведенческой аналитики при скоринге клиентов. Обучение сотрудников навыкам выявления отклоняющегося поведения. Создание условий, снижающих соблазн совершить мошенничество (прозрачность, обратная связь). Этическое информирование клиентов о последствиях нарушений. Формирование социально одобряемой модели взаимодействия со страховщиком.

ГЛАВА 2. МОДЕЛИРОВАНИЕ ТЕХНОЛОГИИ ЗАЩИТЫ ОТ СТРАХОВОГО МОШЕННИЧЕСТВА В КОНТЕКСТЕ РИСК-МЕНЕДЖМЕНТА

2.1 Изучение опыта работы страховой и продуктовой линейки компании «Совкомбанк страхование»

Страховая компания «Совкомбанк страхование» — универсальная страховая компания, ранее входила в группу «КИТ Финанс», затем в международную страховую группу Liberty Mutual, с 2020 года — дочерняя компания «Совкомбанка». Головной офис расположен в Санкт-Петербурге.

ОАО "КИТ Финанс Страхование" - российская страховая компания, основанная в 1993г. В Санкт-Петербурге. Акционерами являются "КИТ Финанс Холдинговая компания" (конечные владельцы - консорциум инвесторов во главе с ОАО "Российские железные дороги") и менеджмент страховой компании. Уставный капитал "КИТ Финанс Страхования" составляет 480 млн 760 тыс. руб. "КИТ Финанс Страхование" обладает индивидуальным рейтингом надежности Национального рейтингового агентства на уровне "А" (высокая надежность, второй уровень). Клиентами страховщика являются более 150 тыс. физических и 3 тыс. юридических лиц. ООО "КИТ Финанс Холдинговая компания" закрыло сделку по продаже 99,99% акций своей страховой "дочки" ОАО "КИТ Финанс Страхование" международной страховой группе Liberty Mutual. Такая информация содержится в официальном сообщении "КИТ Финанса". Сумма сделки не раскрывается. Сделка по продаже компании "КИТ Финанс Страхование" состоялась в рамках стратегии по реализации

непрофильных активов в интересах банка "КИТ Финанс". Вырученные от продажи акций средства будут направлены на погашение займа ОАО "Российские железные дороги", говорится в сообщении. После завершения сделки компания "КИТ Финанс Страхование" вошла в международный дивизион Liberty Mutual, предлагающий розничные и корпоративные страховые продукты в трех регионах: Европе (включая Испанию, Португалию, Турцию, Польшу, Ирландию, теперь и Россию), Латинской Америке (Венесуэла, Бразилия, Колумбия, Аргентина и Чили) и Азии (Таиланд, Сингапур, Китай, включая Гонконг, и Вьетнам).

Ключевые направления бизнеса компании останутся прежними: автострахование, страхование имущества, грузов, банкострахование, добровольное медицинское страхование и страхование выезжающих за рубеж. При этом компания планирует и дальше активно развивать модель прямого страхования (директ) в рознице, а также корпоративный и банковский сегменты бизнеса.

Группа Liberty Mutual (центральный офис расположен в Бостоне, США) - крупная компания на рынке страхования имущества и личного страхования. Международный бизнес Liberty Mutual сосредоточен в двух основных направлениях: продажа розничных и корпоративных страховых продуктов на местных рынках и специальные программы корпоративного страхования и перестрахование (входит в блок Liberty International Underwriters). Подписанная премия страховой группы Liberty Mutual в 2011г. составила 31,2 млрд долл., из которой 8,2 млрд долл. приходится на международный бизнес.

СК "Либерти страхование" официально сменила название на "Совкомбанк страхование" в связи с вхождением в группу Совкомбанка, говорится в сообщении страховщика. О том, что компания сменит название, стало известно после того, как банк приобрел 99,99% ее акций у

американского страховщика Liberty Mutual Group в феврале 2020 года. Все обязательства по полисам и договорам страхования, агентским договорам, соглашениям о сотрудничестве, депозитным договорам, а также по иным формам договоров и соглашений, заключенных от имени СК "Либерти страхование", остаются в силе и продолжают исполняться в полном объеме и на прежних условиях, отмечает страховщик.

По данным СК "Совкомбанк страхование", премии компании за 2019 год составили 5,2 млрд рублей, что на 8% выше по сравнению с 2018 годом, выплаты - 2,5 млрд рублей, коэффициент убыточности по всем видам страхования - 46,7%. По данным ЦБ РФ за 2019 год, компания занимала 37-е место по объему премий среди российских страховщиков.

В феврале 2025 года стало известно о том, что страховая компания «Совкомбанк Страхование» увеличила чистую прибыль после налогообложения на 60% до ₽16,9 млрд в 2024 году по сравнению с ₽10,5 млрд в 2023 году. Капитал компании составил ₽19,8 млрд. Структура страхового портфеля компании в 2024 году:

Каско — ₽12 млрд (47% портфеля).

Страхование от несчастных случаев — ₽3,8 млрд (15%).

Добровольное медицинское страхование — ₽2,2 млрд (8%).

ОСАГО — ₽1,7 млрд (7%).

В 2024 году страховые выплаты увеличились на 28% и достигли ₽10 млрд против ₽7,8 млрд годом ранее. Основная часть пришлась на моторные виды страхования. По каско выплаты составили ₽5,7 млрд, по ОСАГО — ₽1 млрд. Рост выплат связан с увеличением числа страховых случаев и удорожанием ремонта автомобилей.

Некоторые продукты из продуктовой линейки «Совкомбанк Страхование»:

- КАСКО. Добровольное страхование интересов обладателей транспортных средств. Есть варианты: «МиниКАСКО», «СуперКАСКО», «МикроКАСКО», «КиберКАСКО».

- ОСАГО. Финансовая защита ответственности перед другими участниками дорожного движения. Полис можно купить как на специальном бланке через контакт-центр, так и онлайн на сайте в виде электронного полиса.

- КАСКО ЛАЙТ. Страховая защита автомобиля от самых крупных рисков: тотального уничтожения (ремонт составляет свыше 75% страховой суммы) и хищения/угона.

- Страхование выезжающих за рубеж. Включает широкий спектр услуг: от покрытия медицинских расходов до страхования багажа.

- Страхование квартиры. Предлагает защиту от повреждений имущества, пожаров, наводнений и других чрезвычайных ситуаций.

- Страхование жизни. Обеспечивает финансовую защиту семьи в случае непредвиденных обстоятельств. Полис покрывает расходы на медицинские услуги и выплаты при наступлении страхового случая.

- «МегаПолис». Продукт, который сочетает в себе защиту жизни, здоровья, имущества, благосостояния. В нём собраны самые востребованные риски и страховое покрытие.

Внутренняя система финансового контроля, основанная на постоянном анализе текущей ситуации, заложила прочный фундамент прибыльности всех видов страхования. Совкомбанк Страхование имеет диверсифицированный, а значит, устойчивый страховой портфель.

Уставный капитал составляет 1 850 435 346, 4 ₽, стоимость чистых активов на 31.12.2023 составляет 25 919 306 206,54 ₽

Таблица 1 – Финансовые показатели

Год	2023	2022	2020
Премии	16,9 млрд ₽	17,3 млрд ₽	6,6 млрд ₽
Выплаты	7,8 млрд ₽	7,6 млрд ₽	2,2 млрд ₽

Совкомбанк страхование обладает кредитным рейтингом AA (RU) со стабильным прогнозом от Аналитического кредитного рейтингового агентства (АКРА). Присвоение рейтинга обусловлено сильной оценкой бизнес-профиля, средним финансовым профилем, адекватным качеством управления, а также поддержкой со стороны нового акционера – ПАО «Совкомбанк» рейтинг АКРА-АА, прогноз стабильный. Совкомбанк страхование обладает рейтингом надежности от рейтингового агентства «Эксперт РА» на уровне ruAA, прогноз стабильный.

2.2 Трансформация российского рынка страхования под влиянием инновационных технологий

Современные вызовы, стоящие перед страховыми компаниями в борьбе с мошенничеством, требуют кардинального переосмысления подходов к мониторингу, выявлению и предотвращению мошеннических действий. Использование цифровых платформ на основе анализа больших данных (Big Data) и технологий искусственного интеллекта (ИИ) открывает качественно новые возможности в построении эффективной системы защиты от страхового

мошенничества. Цифровая антимошенническая платформа представляет собой интеграционную ИТ-среду, в которой автоматизированы процессы сбора, обработки, анализа и интерпретации информации, связанной со страховыми событиями. Архитектура такой платформы, как правило, включает в себя:

- Модуль сбора данных — сбор информации из внутренних и внешних источников: CRM, базы клиентов, данные ГИБДД, Росреестра, социальных сетей и др.;
- Хранилище больших данных (Data Lake) — структурированное и неструктурированное хранение данных для последующего анализа;
- Аналитический модуль — реализация алгоритмов машинного обучения, скоринга и поведенческого анализа;
- Система принятия решений — автоматическое присвоение уровня риска обращению, направление на ручную проверку, блокировка сомнительных операций;
- Панель мониторинга и визуализации — интерфейс для сотрудников андеррайтинга, безопасности и аналитики;
- Механизмы самообучения — постоянное обновление моделей на основе новых кейсов и обратной связи.

Применение технологий больших данных позволяет страховой компании обрабатывать массивы информации объёмом в терабайты, включая изображения, видеозаписи, голосовые сообщения и метаданные. Проводить кросс-анализ данных из разных источников: идентификация совпадений между клиентами, авто, адресами и сценариями обращений. Выявлять аномальные закономерности и нетипичное поведение (например, частые обращения с похожими

сценариями, многократные страховые случаи в одном районе). Анализировать социальные связи (social graph analysis), чтобы установить вероятные группы мошенников. Построить поведенческие профили клиентов на основе временных рядов и истории действий. Пример: клиент обращается за выплатой по КАСКО. Система находит, что тот же человек под другим именем уже получал аналогичную выплату в другой компании за похожий случай. Такие совпадения становятся маркером потенциального мошенничества.

В рамках антимошеннической платформы применяются следующие алгоритмы. Супервизируемое обучение (например, градиентный бустинг, случайный лес) — для классификации обращений на честные и мошеннические. Нейросетевые модели — для работы с неструктурированными данными (изображения, тексты, видео). Нейронные сети глубокого обучения (deep learning) — выявление скрытых признаков в страховых кейсах. Кластеризация и аномалия-дитекшн — для поиска нетипичных обращений. NLP (обработка естественного языка) — анализ заявлений, жалоб, переписок с клиентами. Особое внимание уделяется explainable AI (XAI) — системам, которые не только выдают решение, но и объясняют его, что важно при принятии юридических решений.

У цифровых платформ есть как положительные, так и отрицательные стороны. Преимущества цифровых платформ существенное сокращение времени на обработку и проверку обращений. Снижение количества ложноположительных и ложноотрицательных решений. Повышение прозрачности внутренней аналитики, возможность масштабирования и адаптации под новые угрозы. Ограничения цифровых платформ необходимость наличия обученных датасетов с размеченными случаями мошенничества, возможные

ошибки при внедрении (overfitting, недостаточная интерпретируемость моделей). Требования к защищённости персональных данных (ФЗ-152, GDPR). Риск предвзятости алгоритмов (bias), особенно при обучении на ограниченном наборе данных. Есть ряд компаний которые внедрили цифровую платформу. СберСтрахование внедрила ИИ-систему для анализа обращений по ДМС, которая выявляет аномалии в частоте обращений, совпадениях IP-адресов и шаблонах поведения. АльфаСтрахование использует нейросеть для анализа фотографий повреждённого авто, сравнивая их с базой типовых повреждений и выявляя признаки подделки. Английская компания Aviva построила распределённую платформу на базе Apache Hadoop и TensorFlow, анализирующую до 2 миллионов кейсов в реальном времени. Такие кейсы показывают высокую эффективность платформенного подхода и важность системного подхода к ИИ в сфере страхования.

Прогнозирование мошенничества в страховании — это ключевая составляющая современной стратегии противодействия рискам. Оно позволяет страховым компаниям не просто реагировать на уже совершённые мошеннические действия, а предупреждать их заранее, выстраивая эффективную систему превентивного контроля. В центре этой системы — математическое моделирование и скоринговые технологии, основанные на анализе данных и поведенческих закономерностях. Математическое моделирование предполагает формализацию процессов принятия решений и выявления рисков на основе количественных данных. Прогнозные модели строятся с учётом. Наличия обучающей выборки, база исторических данных по обращениям, разделённым на мошеннические и добросовестные. Определения целевой переменной (например, вероятность мошенничества). Выделения информативных признаков — возраст

страхователя, регион, история обращений, характер ущерба, поведение в цифровых каналах. Калибровки модели тестирование точности предсказаний и минимизация ошибок (ложноположительных и ложноотрицательных). Обратной связи обновление модели по мере поступления новых кейсов. рогнозные модели делятся на две группы: Детерминированные с фиксированными параметрами, основанные на правилах, порогах и логике; Стохастические модели с элементами случайности, чаще всего основанные на статистике и машинном обучении. Скоринговая система — это инструмент, который присваивает оценку риска (скор) каждому заявлению или страхователю. Чем выше балл, тем выше вероятность мошенничества. Для работы скоринговой модели необходимо вводные данные, анкета клиента, история заявлений, географическая информация, цифровой след. Далее происходит обработка информации линейная регрессия, логистическая регрессия, случайный лес, градиентный бустинг и др. После обработки информации программа выдает балл например, от 0 до 100, где значение выше 70 указывает на высокий риск. Далее программа выдает автоматическую блокировку, направление на ручную проверку, допрасследование. Пример: при подаче заявления по КАСКО система обнаруживает, что клиент ранее подавал аналогичные заявления в разные компании, имеет подозрительные IP-адреса и подгружает фотографии низкого качества — скор = 87/100 → ручная проверка. В числе наиболее популярных моделей. Логистическая регрессия: применяется для бинарной классификации (мошенничество/не мошенничество). Простая и интерпретируемая модель. Деревья решений и ансамбли (Random Forest, XGBoost): позволяют учитывать сложные взаимодействия между признаками. Нейросетевые модели (MLP, CNN): используются, если данные включают изображения, тексты, видео — особенно актуальны в КАСКО. Байесовские модели: дают вероятность

события при заданных условиях, полезны при отсутствии полной информации. Когортный и временной анализ: изучают изменения поведения клиента во времени, выявляют «взрывной» рост обращений или подозрительную активность. Применение ансамблей моделей (Stacked Models) позволяет повысить точность, снижая риски ошибок.

Для оценки эффективности моделей используются метрики:

- Accuracy — доля правильно предсказанных случаев;
- Precision и Recall — баланс между чувствительностью и точностью;
- ROC-AUC — площадь под кривой ошибок, отображает общую эффективность;
- Lift Chart — показывает преимущество модели по сравнению с случайным выбором;
- Матрица ошибок (confusion matrix) — даёт информацию о типах ошибок модели.

Также важно отслеживать реальную бизнес-ценность модели. Сколько мошеннических выплат удалось предотвратить.Сколько честных клиентов было ошибочно заблокировано. Как изменилась общая убыточность страхового портфеля. Хотя скоринговые системы и математические модели являются мощным инструментом, они имеют ограничения. Необходимость качественной обучающей выборки, сложности в интерпретации сложных моделей (нейросети). Подверженность дрейфу данных — изменения поведения клиентов делают модели менее актуальными со временем. Правовые и этические аспекты — автоматическое принятие решений может быть оспорено клиентом. Пути совершенствования включают, постоянную перекалибровку моделей. Введение гибридных схем — сочетание

автоматических и ручных проверок. Обратную связь от андеррайтеров и службы безопасности. Интеграцию с внешними базами и аналитическими платформами (например, АИС «Антифрод»).

Борьба со страховым мошенничеством требует системного подхода, охватывающего все стадии взаимодействия клиента со страховой компанией. Управление рисками мошенничества не ограничивается работой службы безопасности или внутреннего контроля — это бизнес-процесс, который должен быть интегрирован в каждое звено страховой деятельности. Такой процесс строится поэтапно, начиная с выявления подозрений и заканчивая реализацией механизмов пресечения и последующего анализа. Инициация процесса выявление потенциальных признаков мошенничества. Первый шаг — обнаружение сигналов риска. Эти сигналы могут поступать из разных источников. Автоматические системы скоринга и фильтрации (на основе ИИ и аналитики). Внутренние сотрудники — андеррайтеры, ликвидаторы, колл-центр. Анализ клиентского поведения (необычная активность, смена IP, неконсистентные данные). Обратная связь от внешних партнёров — брокеров, медицинских учреждений, СТО, правоохранительных органов. Сравнение заявлений по времени, географии, шаблонам — выявление серийных случаев. При обнаружении подозрений формируется сигнал в системе управления мошенничеством (Fraud Management System), который направляется на дальнейшую обработку. На этом этапе проводится всесторонний анализ. Проверка документов на оригинальность, достоверность, соответствие шаблонам. Анализ истории клиента, частота обращений, связи с другими подозрительными лицами. Оценка цифровых следов IP, устройство, геолокация, браузерные параметры. Экспертиза событий повторное изучение обстоятельств страхового случая (например,

техническая экспертиза повреждённого автомобиля). Оценка взаимодействий клиента с компанией — коммуникации, жалобы, манипулятивное поведение. Проверка проводится либо внутренним отделом, либо с привлечением внешних специалистов (аудиторов, судебных экспертов, юристов).

Принятие решений и реализация антимошеннических мер на основе анализа принимаются управленческие решения. Отказ в выплате с мотивировкой (согласно ГК РФ и условиям договора). Возбуждение внутреннего расследования, передача дела в правоохранительные органы (в случае выявления состава преступления). Внесение клиента в чёрный список или в общую базу мошенников (при участии в консорциуме страховщиков). Инициация регрессного иска — если ущерб был уже компенсирован, но впоследствии выявлен обман. На этом этапе важно действовать строго в правовом поле, с соблюдением требований законодательства, чтобы избежать претензий со стороны клиента и регуляторов. Каждый случай мошенничества должен быть тщательно зафиксирован во внутренней базе инцидентов, отчётности службы внутреннего контроля, отчётах в ЦБ РФ и других контролирующих органах (при необходимости). Внутренней аналитике для последующей оптимизации процессов. Фиксация инцидентов позволяет строить историческую базу знаний, на основании которой совершенствуются алгоритмы детектирования и риск-оценки. Финальный, но не менее важный этап — рефлексия и обновление. Оценка эффективности реакции насколько быстро и точно была выявлена схема. Модернизация процедур внесение изменений в операционные стандарты. Обучение персонала на базе кейса, перекалибровка скоринговой модели, если случай не был заранее

предсказан системой. Анализ упущенных возможностей — почему мошенник смог пройти контроль и как этого избежать в будущем.

Процесс управления рисками мошенничества должен быть итеративным на каждом этапе извлекается опыт, который используется для улучшения всей системы. Только так можно достичь устойчивости в условиях динамичных угроз. Несмотря на технологические достижения в борьбе с мошенничеством, решающим фактором устойчивости страховой компании остаётся человеческий капитал и организационная среда, в которой он функционирует. Корпоративная культура, основанная на принципах честности, прозрачности и нулевой терпимости к нарушениям, является фундаментом эффективной системы противодействия мошенничеству. Без этически зрелой внутренней среды даже самые совершенные технологические решения оказываются уязвимыми. Этика как барьер к внутреннему и внешнему мошенничеству. Этические установки сотрудников напрямую влияют на риск мошенничества. Согласно исследованиям в области поведенческой экономики, вероятность участия в противоправных действиях резко снижается. Сотрудники идентифицируют себя с компанией и разделяют её ценности. Имеются чёткие внутренние нормы поведения и санкции за их нарушение. Подчёркивается неотвратимость последствий, руководство демонстрирует собственный пример соблюдения норм. Отсутствие этических ориентиров может вести к внутреннему мошенничеству — например, сговору сотрудников с клиентами, манипуляциям при рассмотрении дел, сокрытию рисков. Поэтому развитие корпоративной этики выступает важным элементом профилактики. Формирование антимошеннической культуры в страховой организации включает, кодекс этики и делового поведения, закрепляющий допустимые нормы, политику "нулевой терпимости" к

обману и махинациям. Прозрачную систему мотивации, исключающую искушение фальсификациями. Механизмы внутреннего контроля, позволяющие выявлять отклонения. Коммуникации и обучение, направленные на формирование этического иммунитета. Корпоративная культура становится устойчивой, когда все уровни сотрудников — от линейного персонала до топ-менеджмента — осознают свою ответственность за соблюдение антимошеннических принципов. Установку на этичность и правомерность задаёт, прежде всего, руководящий состав компании. Именно управленцы формируют «тон сверху» (tone at the top), который определяет поведение всей организации. Это выражается личном соблюдении руководителями норм корпоративной политики. Неприменении двойных стандартов при рассмотрении дисциплинарных нарушений. Прозрачной отчётности и подотчётности, поддержке сотрудников, отказавшихся участвовать в сомнительных схемах. Неприменении репрессий за сообщения о правонарушениях («принцип защиты добросовестного информатора»).

Эффективная кадровая политика также предполагает оценку сотрудников не только по результатам, но и по соблюдению корпоративных стандартов, что снижает риски мотивационного мошенничества. Одним из ключевых элементов антикоррупционной культуры является наличие доверительных каналов связи, позволяющих сотрудникам, клиентам и партнёрам сообщать о подозрениях. «Горячая линия» или электронные ящики доверия — с анонимной подачей информации. Внутренние платформы обратной связи — с возможностью оставить комментарий по ситуации. Регулярные опросы и анкетирования персонала о восприятии корпоративной среды. Программа защиты информаторов, исключающая репрессии и давление.

Важно, чтобы сообщения рассматривались оперативно, а результаты действий доносились до коллектива. Это формирует доверие и демонстрирует реальное противодействие мошенничеству.

Оценка корпоративной культуры в сфере этики и противодействия мошенничеству может осуществляться с помощью внутренних аудитов и опросов удовлетворённости сотрудников. Анализа дисциплинарной практики и частоты нарушений. Методики оценки этического климата (Ethical Climate Questionnaire). Внешней сертификации по стандартам управления рисками и комплаенс-контроля (например, ISO 37001). Пути совершенствования состоят из регулярное обновление этических кодексов. Проведение тренингов и семинаров по этике и антимошенничеству, внедрение этических KPI. Привлечение этических комиссий и советников по комплаенсу, повышение прозрачности внутрикорпоративных процедур.

Таким образом, корпоративная культура и этика — это не формальность, а стратегический актив в борьбе с мошенничеством. Сильная этическая среда позволяет не только снижать риски, но и формировать устойчивую репутацию компании на рынке страхования.

2.3 Оценка эффективности антимошеннической стратегии страховой компании

Эффективность антимошеннической стратегии невозможно оценить субъективно — необходимы методологически обоснованные критерии и показатели, позволяющие анализировать достигнутые результаты и выявлять узкие места в системе противодействия мошенничеству. Это особенно важно в условиях ограниченных

ресурсов, когда требуется оптимизация мер контроля без ущерба для защиты. Методика оценки направлена на достижение следующих целей, выявление степени достижения запланированных результатов. Оценка экономической целесообразности и возврата инвестиций (ROI). Контроль устойчивости и динамики мошеннических инцидентов. Определение слабых звеньев в системе защиты. Обоснование корректировки стратегических и тактических мер. Для количественной оценки используются следующие показатели (KPI). Уровень выявленного мошенничества (%) — отношение числа подтверждённых случаев мошенничества к общему числу страховых дел. Сумма предотвращённых мошеннических выплат (руб./%) — объём средств, сэкономленных за счёт отказа в необоснованных выплатах. Среднее время выявления инцидента (часы/дни), процент автоматических срабатываний, подтверждённых расследованием (accuracy rate). Доля случаев, переданных в правоохранительные органы. Снижение количества повторных обращений от лиц с историей мошенничества. Рентабельность антимошеннической программы (анализ затрат и результатов).Также важно учитывать нематериальные эффекты — рост доверия клиентов, снижение внутренних конфликтов, повышение корпоративной дисциплины. На практике используется комбинация количественных и качественных методов, SWOT-анализ антимошеннической стратегии. Benchmarking — сравнение с практиками лидеров отрасли. Метод "контрольной группы" — сравнение показателей до и после внедрения мероприятий. Анализ трендов во времени — позволяет отследить устойчивость достигнутого эффекта. Экспертные оценки и внутренние аудиты. При необходимости можно привлекать внешние консалтинговые организации, которые предоставляют независимую оценку эффективности внутренней политики. Современные страховые компании внедряют

информационные панели (dashboards) и аналитические модули в рамках корпоративной BI-системы (Business Intelligence), которые позволяют отслеживать KPI в режиме реального времени. выявлять аномалии и отклонения. Формировать регулярные отчёты для руководства. Визуализировать риски и достижения (графики, тепловые карты и т.д.). Устанавливать контрольные пороги и пороговые значения (thresholds). Такие системы повышают прозрачность, ускоряют принятие решений и улучшают контроль за исполнением антимошеннических процедур.

Полученные данные должны быть не просто зафиксированы, но интерпретированы с позиции менеджмента, в каких звеньях процесса защита работает неэффективно? Какие методы выявления оказываются недостаточно точными? Какой ROI от внедрённой системы автоматического анализа? Какие внешние изменения (законодательство, поведение клиентов) влияют на результат? Результаты оценки служат основой для корректировки стратегии. Модификация процедур (например, усиление проверки конкретных видов страхования), обновление программного обеспечения и алгоритмов. Перераспределение ресурсов между службами (аналитики, расследования, IT). Проведение дополнительных обучающих мероприятий.

В условиях цифровизации страховой отрасли и роста числа мошеннических схем становится всё более актуальным использование инструментов моделирования и прогнозной аналитики, позволяющих выявлять потенциальные инциденты ещё до наступления страхового случая. Моделирование — это не только способ автоматизировать проверку, но и средство перехода от реактивного к проактивному управлению рисками. Один из классических подходов к прогнозированию страхового мошенничества — использование

регрессионных моделей, в которых на основе исторических данных оценивается вероятность мошеннического поведения. Наиболее часто применяются. Логистическая регрессия — для бинарной классификации (мошенничество / нет). Дисперсионный и корреляционный анализ — для выявления взаимосвязей между признаками. Регрессия Пуассона — для оценки числа страховых случаев в заданный период. Методы анализа главных компонент (PCA) — для снижения размерности признаков. Эти методы хорошо работают при наличии большого объёма структурированных и чистых данных, но хуже справляются с нестандартными, изменяющимися схемами мошенничества.

Наиболее эффективным направлением в выявлении скрытых паттернов мошенничества становится машинное обучение (ML), включающее Supervised Learning (обучение с учителем) обучение модели на размеченных данных, с примерами мошеннических и честных обращений. Unsupervised Learning (обучение без учителя) — кластеризация и выделение аномалий при отсутствии чёткой маркировки. Reinforcement Learning — адаптивное обучение с корректировкой поведения модели по результатам.

Часто используются алгоритмы Decision Trees и Random Forests, Gradient Boosting (XGBoost, LightGBM), Support Vector Machines (SVM), Neural Networks (глубокое обучение). Такие модели обладают высокой точностью и могут самостоятельно выявлять корреляции, недоступные для аналитика-человека.

Мошенничество всё чаще принимает коллективный характер, включающий группы лиц, связанных между собой (например, автоподставы, серийные обращения). Для выявления таких схем применяются графовые модели, где узлы — участники (страхователи, агенты, СТО), а связи — отношения между ними, анализ плотности

связей, циклов и аномалий в графах. Алгоритмы PageRank и Community Detection — для оценки центральности и поиска аномальных сообществ.

Сетевой подход позволяет обнаружить скрытые мошеннические синдикаты, действующие систематически и скрытно. Методы анализов аномалий (anomaly detection) предполагают выявление отклонений от нормального поведения. Пороговые модели (если заявленный ущерб превышает 3 сигмы от среднего). Autoencoders и рекуррентные нейросети — для обнаружения аномалий в последовательностях. Time-series models (например, ARIMA) — для выявления временных паттернов. Результатом становится система раннего предупреждения (Early Warning System), которая автоматически выделяет «красные флаги» — потенциально мошеннические события до завершения анализа или выплаты. Помимо оперативной аналитики, важна и стратегическая оценка рисков. Сценарное моделирование построение моделей развития мошеннических схем при различных условиях. Имитационное моделирование (simulation modelling) — повторяющееся случайное воспроизведение процессов с учётом вероятностей. Агентное моделирование имитация действий участников системы (страхователя, агента, эксперта, аудитора) в рамках бизнес-процесса. Системная динамика (System Dynamics) моделирование обратных связей и накоплений (например, как рост объёма страхования влияет на частоту мошенничества). Эти методы позволяют принимать обоснованные управленческие решения: например, где усилить контроль, как перераспределить ресурсы, стоит ли вводить новую технологию или изменить процедуру урегулирования.

Выводы по второй главе

Формирование эффективной системы противодействия страховому мошенничеству требует не только теоретических моделей и технологий, но и реалистичных, практико-ориентированных шагов, адаптированных под конкретные условия страховой компании. Ниже представлены ключевые направления совершенствования, основанные на обобщении современной практики и аналитических исследований. Во многих страховых компаниях антимошеннические функции распылены между различными подразделениями или осуществляются в фоновом режиме. Рекомендуется создание специализированного отдела (или службы) по противодействию мошенничеству, обладающего чёткими полномочиями и регламентами. Назначение ответственного за антимошенническую политику на уровне топ-менеджмента. Внедрение системы межфункционального взаимодействия (служба безопасности, андеррайтинг, урегулирование, IT, комплаенс). Регулярное проведение координационных совещаний по рискам мошенничества. Формирование внутренней базы данных подозрительных клиентов с учётом законодательства. Организационная устойчивость антимошеннической системы должна быть сопоставима с другими ключевыми направлениями управления рисками.

Страховое мошенничество часто проникает через уязвимости в устаревших или избыточно формализованных процедурах. Проведение регулярного аудита бизнес-процессов на предмет мошеннических рисков. Оптимизация этапов урегулирования убытков — снижение доли ручного ввода, обязательная верификация информации. Внедрение принципов "двойного контроля" и "разделения обязанностей". Разработка чек-листов и критериев риска для специалистов

урегулирования. Перевод наиболее чувствительных процессов в цифровую среду с логированием действий. Цель — сделать систему непрозрачной и невыгодной для потенциального злоумышленника.

Даже простые аналитические инструменты могут многократно окупиться за счёт предотвращённых убытков. Внедрение систем машинного обучения и скоринга подозрительных обращений. Использование графовых баз данных для сетевого анализа. Интеграция систем анализа с CRM и учетными платформами. Регулярное обновление алгоритмов и сценариев детекции на основе новых кейсов. При ограниченных ресурсах — аутсорсинг аналитических модулей или использование облачных решений с готовыми моделями (Fraud-as-a-Service). Технологическая инфраструктура — ключевой компонент устойчивой антимошеннической защиты. Эффективность борьбы с мошенничеством во многом зависит от уровня подготовки сотрудников.

Периодические тренинги по идентификации признаков мошенничества, обучение работе с автоматизированными системами и алгоритмами скоринга. Внедрение системы мотивации за предотвращённые убытки. Разработка этического кодекса, подчёркивающего нетерпимость к злоупотреблениям. Формирование каналов обратной связи (горячая линия, внутренние обращения). Цель — сформировать атмосферу предупреждения и активной защиты, а не пассивного реагирования.

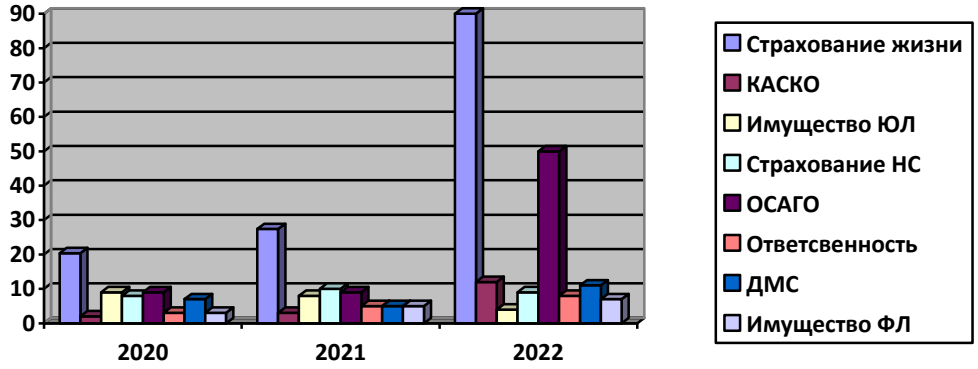
Эффективная антимошенническая система не может быть замкнутой сотрудничество с ЦБ РФ, НАПФ, МВД, ФССП, обмен информацией по выявленным случаям. Взаимодействие с другими страховыми организациями — создание общих чёрных списков и обмен данными. Партнёрство с технологическими компаниями, поставщиками антимошеннических решений. Участие в профильных

профессиональных объединениях. Обратная связь с клиентами: просветительская работа и предупреждение вовлечения в мошеннические схемы. Чем больше вовлечено контрагентов и заинтересованных сторон, тем выше шансы на снижение ущерба от мошенничества.

Финансовые технологии позволяют повысить эффективность страховой компании, а также появляются возможности внедрения новых методов предоставления услуг. Помимо этого, появляются широкие возможности для сбора данных и обнаружения мошенничества, которые могут привести к лучшему выявлению рисков и мерам по их снижению. На сегодняшний день, большинство страховых компаний внедряют финансовые технологии в свои бизнес-процессы. Среди таких компаний ПАО «Совкомбанк Страхование» стало не исключением. Мало того, компания возглавила рейтинг digital-зрелости страховых компаний в 2022 году, составленный агентством SDI360°.

Исходя из рисунка, в период с 2020 по 2022 года процент страховых премий, полученных через интернет, увеличился. Почти все сегменты страхования показали рост числа страховых премий, полученных через интернет, за исключением, страхования жизни и страхования несчастных случаев и болезней. Наиболее ярко видно увеличение в ОСАГО. В 2021 году 49,9% (14 329 305 тыс. руб.) страховых премий было получено онлайн, тогда как в 2020 году через интернет было приобретено полисов всего на 7,6% от общего числа страховых премий по ОСАГО.

Рисунок 2 – Динамика страховых премий, полученных через интернет по отдельным видам страхования ПАО «Совкомбанк Страхование» 2020-2022 гг., %1



Помимо ОСАГО, значительный рост показало КАСКО, с 0,3% (89 514 тыс. руб.) в 2020 году до 11,9% (4 403 712 тыс. руб.) в 2022 году. К тому же неплохо вырос процент страховых премий, полученных через интернет в страховании имущества физических лиц, если в 2020 году он составлял 2,6% (91 128 тыс. руб.), то в 2022 году он достиг 15,3% (979 632 тыс. руб.)

Эту положительную динамику можно описать ростом цифровой грамотности населения Российской Федерации, что в последствии приводит к тому, что люди доверяют интернет-услугам, в том числе услугам страховых компаний и не боятся оплачивать покупки онлайн.

Также на росте продаж страховых полисов через интернет сказывается работа ПАО «Совкомбанк Страхование». А если быть точнее, то компания старается сделать свои продукты в сети понятными простому пользователю и с каждым годом улучшает их и добавляет новые возможности. Помимо этого, SMM-отдел компании упорно работает над социальными сетями компании, что тоже привлекает потенциальных клиентов. Рассмотрим какие технологии внедрялись в компании в 2019 году. 3 апреля 2019 года компания Xerox сообщила, что «Совкомбанк Страхование», в рамках трансформации ИТ-процессов, передал Xerox управление своей печатной инфраструктурой. В результате перехода на аутсорсинг компания высвободила время ИТ-

специалистов для решения приоритетных задач, при этом сократив затраты на печать на 20% и объемы печати на 10%. ПАО «Совкомбанк Страхование» запустил масштабную трансформацию ИТ, изменив сам подход к построению процессов в департаменте информационных технологий и передав функционал, который не является ключевым, внешним провайдерам. По результатам проведенного тендера управление печатным парком было доверено компании Xerox. Перед сервис-провайдером была поставлена задача повысить эффективность работы печатной инфраструктуры, что подразумевает оптимизацию парка печатного оборудования, усовершенствование процессов его использования, а также снижение затрат на одну копию. Первый этап внедрения услуги в головных офисах в Москве специалисты Xerox завершили за месяц, после чего к ним добавились ещё одиннадцать в Московской области. По итогам внедрения услуги компания «Ингосстрах» смогла достичь за 2018 год 20-процентной экономии расходов на печать. На апрель 2020 года проводится оценка потенциала развития данного сервиса в региональной сети. Компания «Техносерв», российский системный интегратор, сообщила о завершении проекта по внедрению решения для мониторинга и анализа производительности сети и приложений в ПАО «Совкомбанк Страхование», одной из российских страховых компаний. У «Совкомбанк Страхование» большое количество филиалов по всей стране и разветвленная ИТ-инфраструктура. Сетевая составляющая напрямую влияет на доступность бизнес-приложений компании. Для поддержания устойчивости ее функционирования требуется оперативный контроль показателей работоспособности, анализ тенденций для планирования ресурсов, сокращение 72 времени локализации и выявление первопричин проблем в работе сервисов. В качестве инструмента для достижения поставленных задач «Совкомбанк Страхование» выбрал

решение для мониторинга и анализа производительности сети и приложений Riverbed SteelCentral . Продукт отлично показал себя на этапе пилотного проекта и полностью отвечал потребностям компании. В рамках проекта были решены задачи контроля основных приложений, обеспечивающих подключение к корпоративным сервисам удалённых офисов и страховых агентов, а также поддерживающих работу распределённого контакт-центра и корпоративного сайта ingos.ru. июня 2021 года стало известно, что «Совкомбанк Страхование» внедрил технологию, которая позволяет страховать грузы в режиме реального времени. При этом система сама отбирает нужные данные и в автоматическом режиме формирует полис с момента, когда груз принимается к перевозке. Это происходит благодаря смарт-контрактам — алгоритмам, которые анализируют поток информации от перевозчика и контролируют заложенные в систему обязательства сторон.

Тенденции страховых технологий в ближайшие несколько лет будут включать в себя улучшение различных технологий во имя повышения точности. Машинное обучение технически является ответвлением ИИ, но оно более конкретно, оно основано на идее, что мы можем создавать машины для обработки данных и обучения самостоятельно, без нашего постоянного наблюдения.

Машинное обучение может не только улучшить обработку претензий, но и автоматизировать ее. Когда файлы являются цифровыми и доступны через облако, их можно анализировать с использованием предварительно запрограммированных алгоритмов, повышая скорость и точность обработки. Это автоматическая проверка может повлиять не только на претензии: ее также можно использовать для администрирования политик и оценки рисков.

Еще одной перспективной технологией является интернет вещей. Большинство потребителей готовы делиться дополнительной личной информацией, если это означает экономию денег на своих страховых полисах, и Интернет вещей (IoT) может автоматизировать большую часть этого обмена данными. Страховщики могут использовать данные с устройств IoT, таких как различные компоненты умных домов, автомобильные датчики и носимые технологии, чтобы лучше определять ставки, снижать риск и даже предотвращать потери в первую очередь. Интернет вещей подкрепит другие страховые технологии данными из первых рук, повысив точность оценки рисков, предоставив клиентам больше возможностей для влияния на ценообразование своих полисов напрямую, а страховщикам – возможность повысить точность и доходы.

Телематика. Возможности телематики по-прежнему будут влиять на автомобильные полисы. В страховых технологиях телематика используется как технология для автомобиля. Автомобили будут оснащаться устройствами мониторинга, которые измеряют различные показатели, такие как данные о скорости, местоположения, авариях и многое другое, которые отслеживаются и обрабатываются с помощью аналитического программного обеспечения, чтобы помочь определить вашу страховую премию. Преимущества телематики многочисленны как для страховщиков, так и для страхователей. Чат-боты. По некоторым оценкам, к 2025 году 95% всех взаимодействий с клиентами будут осуществляться с помощью чат-ботов. Используя ИИ и машинное обучение, чат-боты могут беспрепятственно взаимодействовать с клиентами, экономя время каждого в организации и, в конечном итоге, экономя деньги страховых компаний. Бот может провести клиента через

процесс подачи заявки или претензии, оставляя вмешательство человека для более сложных случаев.

Использование искусственного интеллекта (ИИ) быстро расширилось, и устройства с поддержкой ИИ становятся обычным явлением в домах по всему миру. ИИ предлагает страховщикам возможность создавать эти уникальные впечатления, удовлетворяя высокоскоростные требования современных потребителей [46]. Ключевым моментом является использование возможностей ИИ для использования огромных объемов потребительских данных, доступных для создания персонализированного опыта, основанного на поведении и

привычках человека. Кроме того, с помощью ИИ страховщики могут улучшить циклы обращения претензий и коренным образом изменить процесс андеррайтинга. ИИ также позволяет страховщикам быстрее получать доступ к данным, а сокращение человеческого фактора может привести к более точной отчетности за более короткие периоды времени.

Вероятно первоначальное влияние ИИ будет в первую очередь связано с повышением эффективности и автоматизацией существующих процессов андеррайтинга и претензий клиентов. Со временем его влияние будет более глубоким; он может выявлять, оценивать и страховать возникающие риски и определять новые источники доходов.

Социальные сети и их роль в страховой отрасли выходят за рамки маркетинговых стратегий и умной рекламы. Добыча данных в социальных сетях улучшает оценку рисков для страховщиков, расширяет возможности обнаружения мошенничества и обеспечивает совершенно новый опыт работы.

ЗАКЛЮЧЕНИЕ

Мошенничество в сфере страхования продолжает оставаться одной из наиболее острых проблем как для отдельных страховых компаний, так и для страхового рынка в целом. Несмотря на значительное развитие инструментов внутреннего контроля, цифровых технологий и совершенствование нормативно-правовой базы, мошеннические схемы становятся всё более изощрёнными, адаптивными и масштабными. Это требует от участников рынка формирования устойчивых, адаптивных и технологически подкреплённых антимошеннических стратегий в рамках системы риск-менеджмента.

В ходе выполнения дипломной работы была достигнута поставленная цель — разработка теоретико-практической модели технологии защиты от страхового мошенничества с позиций риск-менеджмента. Были решены следующие задачи: изучены сущность, виды и особенности страхового мошенничества, проанализированы современные методы управления соответствующими рисками, исследованы информационные технологии, модели выявления мошенничества, а также зарубежный и отечественный опыт противодействия.

В первой главе дипломной работы рассмотрены теоретико-методологические основы феномена страхового мошенничества. Определено, что под страховым мошенничеством следует понимать действия, направленные на получение необоснованных страховых выплат посредством предоставления заведомо ложной информации или манипуляций с объектами страхования. Установлено, что мошенничество может быть совершено не только страхователями, но и сотрудниками страховых компаний, экспертами, посредниками и иными вовлечёнными

сторонами. Рассмотрены ключевые классификации страхового мошенничества — по стадии совершения, субъекту, методу, форме участия и другим признакам.

Была раскрыта структура управления мошенническими рисками в рамках риск-менеджмента. Установлено, что эффективная антимошенническая стратегия требует системного подхода, включающего этапы: идентификации, анализа, оценки, минимизации и постоянного мониторинга мошеннических угроз. Рассмотрены практические методы и инструменты, такие как построение риск-матриц, внедрение стандартных операционных процедур, системы автоматизированного контроля, формирование внутренней культуры противодействия злоупотреблениям.

Отдельное внимание уделено информационным технологиям. Были описаны модели машинного обучения и интеллектуального анализа данных, применяемые для выявления нетипичных паттернов поведения, анализа обращений и автоматической фильтрации страховых случаев. Такие технологии, как decision trees, нейронные сети, поведенческий скоринг, фрод-аналитика и биометрия позволяют существенно повысить точность обнаружения мошеннических действий. Выявлено, что использование Big Data и искусственного интеллекта может стать основой для построения адаптивной, самообучающейся системы антимошеннического мониторинга.

Проанализирован международный опыт борьбы со страховым мошенничеством: в США, Великобритании, Германии, Сингапуре и других странах. Установлено, что успешная практика предполагает сочетание правовых, организационных и технологических мер, включая межведомственное сотрудничество, обязательную регистрацию страховых случаев в единой базе, аккредитацию оценщиков, жёсткое регулирование

посреднической деятельности. Сделан вывод о высокой значимости превентивных мер и важности формирования общей культуры нулевой терпимости к мошенничеству.

Изучение российского законодательства показало наличие базовой нормативной базы, включая нормы УК РФ, законы о страховании, положения Банка России, однако выявлены и проблемные зоны. К числу недостатков можно отнести фрагментарность правового регулирования, отсутствие единого реестра мошеннических действий, слабую координацию между страховщиками и органами правопорядка, а также неэффективную судебную практику. Вывод: необходимо расширять законодательную и методологическую основу антимошеннической деятельности.

В заключительной части главы были рассмотрены социально-экономические, поведенческие и психологические аспекты страхового мошенничества. Подчёркнуто, что последствия выходят далеко за рамки материального ущерба: мошенничество подрывает доверие к финансовым институтам, способствует росту страховых тарифов, снижает охват страхованием, увеличивает транзакционные издержки компаний. Также было отмечено, что существует высокий уровень общественной терпимости к определённым видам мошенничества («мягкое мошенничество»), что затрудняет профилактику и требует формирования новой культуры правового сознания.

Практическая значимость исследования заключается в разработке комплексной методологической основы, позволяющей моделировать технологии защиты от страхового мошенничества. Созданная модель ориентирована на реальную практику работы страховых компаний и может быть использована в качестве фундамента для создания

автоматизированной антимошеннической системы, основанной на принципах риск-менеджмента и цифровой аналитики.

Таким образом, дипломная работа позволяет сделать следующие ключевые выводы:

1. Страховое мошенничество — это многоуровневое и многосубъектное явление, требующее системного противодействия;
2. Современный риск-менеджмент предоставляет необходимые инструменты и механизмы для управления мошенническими рисками, однако их применение должно быть комплексным и постоянным;
3. Цифровизация страховой отрасли открывает новые возможности для борьбы с мошенничеством, но требует высокого уровня организационной зрелости и инвестиционной готовности компаний;
4. Зарубежный опыт подтверждает эффективность межведомственного взаимодействия, обязательной отчётности и автоматизации процессов выявления нарушений;
5. Российская практика нуждается в дальнейшей модернизации антимошеннической политики, нормативного регулирования и корпоративной этики.

Продолжением данного исследования может стать разработка прикладного программного обеспечения, реализующего автоматическую модель оценки и предсказания вероятности страхового мошенничества на основе машинного обучения и большого массива поведенческих данных.

Развитие антимошеннических технологий является стратегическим направлением повышения устойчивости страхового бизнеса и всей финансовой системы страны. Преодоление мошенничества возможно только при условии тесного взаимодействия государства, профессионального сообщества, бизнеса и общества.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Об организации страхового дела в Российской Федерации. Федеральный закон от 27.11.1992 N 4015-1 (последняя редакция). – Текст: электронный // Консультант-Плюс: [сайт]. – URL: http://www.consultant.ru/document/ cons_doc_LAW_1307/ (дата обращения 23.09.2021).

2. Атрушкевич Е. Б. Риски внедрения каршеринга во внутренний автопарк компании / Е. Б. Атрушкевич, А. М. Николаев // Экономические и управленческие технологии XXI века: теория и практика, подготовка специалистов: материалы методической и науч.-практ. конф. – 2019. – С. 70-73.

3. Балабанов И. Т. Страхование. Организация. Структура. Практика / И.Т. Балабанов, А.И. Балабанов. — СПб : Питер, 2016. – 256 с. – ISBN 5-318- 00375-3.

4. Белозеров С.А. InsurTech: модификация регуляторных функций / С.А. Белозеров // Сб. трудов XXI Международной научно-практической конференции «Вклад страховой теории и практики в повышение финансовой грамотности населения в координатах меняющейся экономики». – 2020. – С. 59–65.

5. Брызгалов Д. В. Перспективы цифровизации страхового дела в России / Д. В. Брызгалов, Ю. В. Грызенкова, А. А. Цыганов // Финансовый журнал. – 2020. – № 3. – С. 76–90.

6. Вилочкова Е.С. Через конструктивизм к финансовой грамотности / Е.С. Вилочкова, В.И. Прусова // Потенциал российской экономики и инновационные пути его реализации. Материалы

международной научнопрактической конференции студентов и аспирантов: в 2 частях. – 2021. – С. 333-336. 128

7. Винникова И. С. Современные аспекты развития страховой отрасли / И.С. Винникова // Международный журнал прикладных и фундаментальных исследований. — 2020. — № 5. — С. 292-295.

8. Гришин К.В. Тенденции развития цифровых технологий и их влияние на финансовую систему страны / К.В. Гришин, Д.А. Мухина, М.А. Жидкова // Аудит. – 2019. – №9. – С. 36-39.

9. Грошева А.А. Современное состояние, проблемы и перспективы развития страхового рынка РФ / А.А. Грошева, Н.О. Кохно, Д.Г. Хамидулина // Инновационная экономика: перспективы развития и совершенствования. – 2018. – №7 (33). – С. 218-222.

10. Завьялов Д. В. Эволюция концепции городской мобильности / Д. В. Завьялов, О. В. Пищикова, О. В. Сагинова // Экономика, предпринимательство и право. – 2020. – № 2. – С. 309-320.

11. Орланюк-Малицкая Л. А. Страхование: учебник для вузов / под ред. С. Ю. Яновой. — Москва: Издательство Юрайт, 2020. — 481 с. — ISBN 978- 5-534-12272-5.

12. Скамай, Л. Г. Страховое дело: учебник и практикум для среднего профессионального образования / Л. Г. Скамай. — Москва: Издательство Юрайт, 2020. — 322 с. — ISBN 978-5-534-06634-0.

13. Челухина Н. Ф. Финансовые технологии в страховании и проблемы их внедрения в России / Н. Ф. Челухина // Сборник материалов межвузовской научно-методической конференции «Современная экономика, финансы и бизнес: мультидисциплинарные подходы». – 2020. – С. 45–52.

14. Baumol W.J. The free-market innovation machine: analyzing the growth miracle of capitalism / W.J. Baumol // Princeton university press. – 2013. – С. 36-47.

15. Bessant J. Innovation in the twenty-first century / J. Bessant, R. Owen, M. Heintz // John Wiley & Sons. – 2013. – С. 1-26. 129

16. Hausman A. The role of innovation in driving the economy: lessons from the global financial crisis / A. Hausman, W.J. Johnston // J Bus Res. – 2014. – № 67. – С. 2720–2726.

17. Henderson B.J. The dark side of financial innovation: a case study of the pricing of a retail financial product / B.J. Henderson, N.D. Pearson // J Financ Econ. – 2011. – № 100. – С. 227–247.

18. Mention A.L. Innovation in financial services: a dual ambiguity / A.L. Mention, M. Torkkeli // Cambridge Scholars Publishing. – 2014. – С. 43-49.

19. Shiller R.J. In defence of financial innovation / R.J. Shiller // Financial. Times. – 2009. – № 27. – С. 185-204.

20. Frame, W. S., White, L. J. Technological Change, Financial Innovation, and Diffusion in Banking. – Текст: электронный // NYU Working Paper. – 2014. – № 2451. – URL: https://ssrn.com/abstract=2380060 (дата обращения 23.07.2021).

21. Hanusik A. Identification and risk assessment in carsharing. – Текст: электронный // Scientific Journal of Silesian University of Technology. – 2020. – № 109. – С. 33-43. – URL: https://doi.org/10.20858/sjsutst.2020.109.3 (дата обращения 23.09.2021).

22. Zavolokina L., Dolata, M. & Schwabe, G. The FinTech phenomenon: antecedents of financial innovation perceived by the popular

press. – Текст: электронный // Financial Innovation 2. – 2016. – № 16. С. 53-59. – URL: https://doi.org/10.1186/s40854-016-0036-7 (дата обращения 15.08.2021).

23. 5 примеров применения чат ботов для страхования: [сайт]. – URL: https://chatbots.studio/ru/blog/chatbot-uses-for-the-insurance-industry/ (дата обращения 11.05.2021). – Текст: электронный. 130

24. 5 скрытых проблем для Insurtech: [сайт]. – URL: https://www.mantralabsglobal.com/blog/the-5-hidden-problems-for-insurtech/ (дата обращения 30.04.2021). – Текст: электронный.

25. Анализ страхового рынка России в 2021 году: [сайт]. – URL: https://calmins.com/analiz-strakhovogo-rynka-rossii-v-2021/ (дата обращения 30.06.2021). – Текст: электронный.

26. Антонова Л. Электронные технологии в страховании: курс на электронизацию / Л. Антонова, О. Басова, О. Скуратова, А. Янин // «Эксперт РА». – URL: https://raexpert.ru/researches/insurance/ets_1h2018. (дата обращения 24.04.2021). – Текст: электронный.

27. Блокчейн в страховании — популярность обеспечена: [сайт]. – URL: https://calmins.com/blokchejn-v-strahovanii-populyarnost-obespechena/ (дата обращения 17.03.2021). – Текст: электронный.

28. Годовой отчёт ПАО «Совкомбанк Страхование» 2020-2023 гг. [сайт]. – URL:https://www.insurinfo.ru/orgsandcomps/18/analytics/?section=a01&order=un– Текст: электронный.

29. Официальный сайт АО «АльфаСтрахование»: [сайт]. – URL: https://www.alfastrah.ru/ (дата обращения 15.07.2021). – Текст: электронный.

30. Официальный сайт Известия: [сайт]. – URL: https://iz.ru/ (дата обращения 28.11.2021). – Текст: электронный.

31. Официальный сайт КПМГ: [сайт]. – URL:

https://home.kpmg/ru/ru/home.html (дата обращения 16.09.2021). – Текст: электронный.

32. Официальный сайт Рейтингового агентства «Эксперт РА» : [сайт]. – URL: https://raexpert.ru/ (дата обращения 23.01.2021). – Текст: электронный.

33. Официальный сайт СПАО «Ингосстрах»: [сайт]. – URL:

https://www.ingos.ru/ (дата обращения 26.05.2022). – Текст: электронный.

34. Официальный сайт Центрального Банка России: [сайт]. – URL:

https://cbr.ru/ (дата обращения 18.03.2021). – Текст: электронный.