

Big Data как инструмент противодействия мошенничеству на страховом рынке*

Big Data as an Anti-fraud Tool
in the Insurance Market

В статье рассмотрены понятие и основные особенности страхового мошенничества; определены основные модели больших данных (Big Data) как инструмента противодействия мошенничеству на современном страховом рынке.

Ключевые слова: страховое мошенничество; современные технологии; большие данные; страховой рынок; противодействие мошенничеству.

Информационно-коммуникационные технологии на сегодняшний день становятся неотъемлемой составляющей функционирования различных рынков, в том числе и страхового. Активное развитие современных технологий становится причиной появления новых рисков, в дополнение к традиционным – рисков компьютерных атак, хищения денежных средств, умышленных противоправных действий сотрудников организаций. Однако при этом технологии также предоставляют возможности для управления такими рисками на финансовых рынках. На сегодняшний день всё больше страховых компаний во всем мире задействуют сквозные технологии в качестве ключевого инструмента выявления экономических преступлений, в том числе финансового мошенничества.

Цель данного исследования – выявление, с использованием элементов сравнительного анализа, основных моделей сквозной технологии больших данных (Big Data) как инструмента противодействия мошенничеству на современном страховом рынке.

Исследования по проблематике применения современных технологий в противодействии мошенничеству на страховом рынке

Анализ современных публикаций по данной проблематике позволил выявить, что большинство исследований

* Исследование выполнено в рамках проекта «Оптимизация страховой защиты населения в условиях биологической угрозы» (Санкт-Петербургский государственный университет, Pure ID: 75249176).

Соколовская Елена Васильевна,

кандидат экономических наук,
старший научный сотрудник,
Санкт-Петербургский
государственный университет
Sokolovskaya Elena V.,

Candidate of Economic Sciences, Senior
Researcher, St.-Petersburg State University

e.sokolovskaya@spbu.ru

SPIN-код: 4644-0930,
Author ID: 714983

Researcher ID: H-2270-2014

Scopus Author ID: 57193993155

*The author examines
the definition and main features
of insurance fraud and determines
main Big Data models as an anti-
fraud tool in the modern insurance
market.*

Keywords: insurance fraud;
advanced technologies; big data;
insurance market; anti-fraud.

рассматривают современные технологии как элемент экосистемы FinTech и InsurTech в частности [1–4].

Отдельно следует выделить исследования эффективности регуляторных и надзорных технологий (RegTech & SupTech) как инструмента борьбы с мошенничеством на страховом рынке. Противодействие мошенничеству на финансовых рынках, наряду с повышением эффективности соблюдения регуляторных требований и информационной безопасности, является одним из ключевых оснований применения этих технологий [5–10].

Анализ литературных источников позволил понять, что выводы большинства современных исследований касаются сочетания использования технологий как таковых и механизмов взаимодействия между ключевыми контрагентами как одного из направлений эффективного противодействия мошенничеству и противоправным действиям на страховом рынке.

Понятие страхового мошенничества и его основные особенности

Мошенничество в сфере страхования, согласно УК РФ, представляет собой хищение чужого имущества путем обмана относительно наступления страхового случая, а равно размера страхового возмещения, подлежащего выплате в соответствии с законом либо договором страхователю или иному лицу.

С юридической точки зрения страховое мошенничество имеет следующие особенности.

Умышленный характер. Общественная опасность. Нарушаются права как страховой организации, так и иных лиц, связанных с ней обязательствами (например, в случае перестрахования), возникает угроза финансовой устойчивости страховой компании и ее способности выполнить обязательства перед добросовестными страхователями.

Высокая латентность. Это означает, что большая часть таких преступлений не регистрируется правоохранными органами и уголовные дела по ним не возбуждаются.

Подобная латентность обусловлена, во-первых, частым нежеланием страховщиков доводить дело до уголовного преследования по причине, прежде всего, финансовой неэффективности этого процесса, и во-вторых – невыявлением фактов мошенничества в принципе.

Высокая рецидивность (повторяемость), которая обусловлена, в значительной мере, несовершенством обмена данными между страховыми организациями о недобросовестных страхователях, страховых агентах и экспертах, медицинских клиниках и сервисных организациях [11].

Основными «традиционными» методами противодействия страховому мошенничеству со стороны страховых компаний до заключения договора страхования стали качественные предстраховые проверки, осмотр объекта страхования, анализ предыдущих мошеннических эпизодов. Выявление мошенничества после заключения договора страхования требует внутренних расследований страховых компаний и/или обращения в правоохранительные органы.

Современные технологии в противодействии страховому мошенничеству

На рисунке представлены результаты опроса респондентов – российских страховых компаний об оценке эффекта внедрения инновационных технологий в разрезе отдельных операций компании по состоянию на 2020 год.

Как видно на рисунке, большинство респондентов пока затрудняются в оценке эффекта применения технологий как инструмента противодействия мошенничеству на современном страховом рынке.

Тем не менее современные технологии, в частности, машинное обучение с использованием больших данных, позволяют оптимизировать процесс предстраховых проверок, расчетов и сопоставлений, выявлять необычные или подозрительные связи между заявителями, устройствами и информацией, представлен-



■ Пока невозможно оценить эффект ■ Наблюдается положительный эффект

Оценка эффекта внедрения инновационных технологий на страховом рынке России в разрезе отдельных операций страховых компаний, 2020 г.

Источник: составлено автором по данным [12].

ной в страховом требовании, анализировать накопленные данные о страхователе и объекте страхования. Анализ данных по мошенническим эпизодам приводит к изменению правил страхования, стратегий андеррайтинга, скоринга клиентов и страховых событий, тактик, используемых судебными юристами.

Рост объемов цифровой информации обусловил особую значимость технологий сбора, обработки и анализа больших данных. Этот рост обусловлен распространением технологий и доступа к интернету, что позволяет пользователям на постоянной основе создавать новую информацию. К такой информации относятся практически все данные, находящиеся в свободном доступе, включая сайты по поиску работы, новостные источники, социальные сети, блоги. Основным преимуществом таких данных по сравнению с традиционными статистическими данными является их многообразие, а также возможность определить показатели, не учитываемые в официальной статистике. При этом значительная часть информации представлена в неструктурированном виде и требует новых подходов к ее извлечению и анализу [13].

Анализ существующих исследований по применению современных технологий в противодействии страховому мошенничеству позволил определить следующие модели больших данных, которые на сегодняшний день чаще всего используются страховщиками для обнаружения мошенничества.

Анализ социальных сетей (Social Network Analysis, SNA) позволяет страховым компаниям эффективно просматривать большие объемы данных для последующего анализа использованием инструментария теории сетей и теории графов взаимодействий в рамках социальных сетей и социальных отношений [14, 15].

Такие разновидности мошенничества, как инсценировка ДТП или кража автомобиля, страхование жизни, здоровья или имущества у разных страховщиков с целью получить возмещение несколько раз за один страховой случай, обычно имеют признаки сговора. Математически, случаи такого сговора нескольких лиц могут быть представлены как граф, в котором узлы – это экономические агенты, а ребра – взаимоотношения между ними. Кроме того, например, страхование от

несчастливого случая может оказаться мошенничеством, если SNA обнаружит, что адрес, указанный одним из потерпевших, использовался для нескольких страховых претензий. Возможность быстрого сбора такой информации экономит время страховщиков и предупреждает их о скрытых факторах, связанных с потенциальным мошенничеством, до урегулирования претензии.

Разновидностью анализа социальных сетей является **управление информацией о взаимоотношениях с клиентами (Social Customer Relationship Management)**.

Страховщики могут использовать информацию о поведении своих клиентов, анализируя различные ссылки и переходы, с целью борьбы со страховым мошенничеством, особенно в части ложных страховых требований. Например, истец, спрашивающий на форумах о стоимости выставленной на продажу дорогой антикварной вещи за несколько недель до подачи требования о крупной страховой выплате по договору страхования имущества от пожара, может заставить отдел расследований глубже исследовать ситуацию, прежде чем страховщик заплатит по страховке.

Иными словами, анализ данных социальных сетей может позволить страховщикам проверить обоснованность страховых требований. Инструменты Social CRM могут выполнять поиск среди большого количества сообщений в социальных сетях, включая блоги, Facebook, Twitter и другие платформы для поиска информации. Использование неструктурированных данных в социальных сетях может позволить специалистам по урегулированию претензий принимать более информированные и быстрые решения.

Прогностическое моделирование (Predictive Modeling) представляет собой исследование неструктурированных данных, сочетающее различные статистические и аналитические методы, включая анализ текста и его тональность [16]. Отчеты о страховых претензиях обычно занимают несколько страниц, поэтому проверка каждой детали отнимает много времени и зачастую по че-

ловеческим причинам невозможна. Решения для прогнозной аналитики могут исследовать неструктурированные данные и обеспечивать упреждающее обнаружение мошенничества, выявляя закономерности и прогнозы взаимодействия между людьми и данными.

Используя прогнозные модели, основанные как на накопленных данных, так и на данных реального времени, о выплате заработной платы, медицинской информации, информации колл-центра, данных о погоде, страховые компании могут эффективнее выявлять мошеннические требования на ранних этапах. Например, если требование работника о компенсации за серьезную травму глаза расследуется с использованием прогнозной аналитики, можно выявить, что заявитель обсуждал на форуме фильм, который он смотрел в тот же день, вскоре после травмы. Это помогает экспертам изучить возможность неправильной информации о страховой претензии до начала процесса оплаты.

Телематика при анализе данных о вождении. Страховые компании зачастую предлагают установить телематические устройства в автомобили страхователей для получения информации о стиле вождения и предоставления релевантных страховых продуктов, а также для продвижения навыков безопасного вождения. При этом способность телематических устройств предоставлять огромные объемы данных о транспортном средстве в режиме реального времени открывает новые возможности для проверки претензий и выявления попыток мошенничества. Страховщики получают доступ к фактам о транспортном средстве и вождении, которые можно проанализировать для выявления факта мошенничества.

Например, при выяснении обоснованности страхового требования есть возможность проверить, была ли скорость транспортного средства в пределах предписанного лимита, соблюдались ли правила дорожного движения, как произошло торможение, было ли транспортное средство в хорошем состоянии и многое другое.

Регуляторные технологии, которые призваны повысить эффективность выполнения финансовыми организациями требований регулятора и финансового рынка. Используя большие данные в рамках RegTech для автоматизации рутинных процессов, специалисты страховых компаний могут более эффективно реагировать на изменяющиеся нормативные требования и применять аналитические методы для определения областей повышенных нормативных рисков, одним из которых является мошенничество со стороны клиентов страховых компаний и третьих лиц [7].

Выводы

В исследовании определены основные модели Big Data, применяемые для противодействия мошенничеству на страховом рынке, которые могут помочь страховым компани-

ям и сотрудникам правоохранительных органов в расследовании таких противоправных действий, как мошенничество страхователей, оппортунизм страховых агентов, проверка подлинности страхового требования, предотвращение мошенничества в момент представления требования, расчет судебных затрат по спорным заявкам

В этой сфере аналитика больших данных обладает огромным потенциалом для выявления скрытых мошеннических действий. После внедрения в свою бизнес-стратегию сети Интернет, мобильных устройств и социальных сетей страховщики должны обратить внимание на аналитику больших данных, прогнозное моделирование, социальные CRM, телематику и регуляторные технологии, для обеспечения эффективной борьбы со страховым мошенничеством.

Литература:

1. Мировой страховой рынок – современные тенденции развития и финансовые риски России : монография / под ред. И. П. Хоминич. М. : Русайнс, 2018.
2. Соколовская, Е. В. Развитие InsurTech в современных условиях: технологии и рынки / Е. В. Соколовская // Сб. трудов XXI Международной научно-практической конференции «Вклад страховой теории и практики в повышение финансовой грамотности населения в координатах меняющейся экономики». Псков : Псковский государственный университет, 2020. С. 108–113.
3. Chatzara, V. FinTech, InsurTech, and the Regulators / V. Chatzara // InsurTech: A Legal and Regulatory View / ed. by P. Marano, K. Noussia. AIDA Europe Research Series on Insurance Law and Regulation. Vol. 1. Springer Nature Switzerland AG 2020. P. 3–25. <https://doi.org/10.1007/978-3-030-27386-6>.
4. How Technology Can Make Insurance More Inclusive. Finance, Competitiveness & Innovation Global Practice. Fintech Note. No. 2. 2018 The World Bank Group.
5. Белозёров, С. А. InsurTech: модификация регуляторных функций / С. А. Белозёров // Сб. трудов XXI Международной научно-практической конференции «Вклад страховой теории и практики в повышение финансовой грамотности населения в координатах меняющейся экономики». Псков : Псковский государственный университет, 2020. С. 59–65.
6. Вопросы и направления развития регуляторных и надзорных технологий (RegTech и SupTech) на финансовом рынке в России. М. : Центральный банк Российской Федерации, 2018.
7. Соколовская, Е. В. Особенности применения регуляторных и надзорных технологий на современном финансовом рынке: анализ подходов / Е. В. Соколовская // Сб. трудов V Международного экономического Симпозиума, 2021 (в печати).

8. Lemma, V. Fintech, Regtech and Suptech towards a New Market Structure. Ch. 8 / V. Lemma // *FinTech Regulation Exploring New Challenges of the Capital Markets Union*, Palgrave Macmillan, 2020. P. 447–485. <https://doi.org/10.1007/978-3-030-42347-6>.
9. Mayer, N. A risk management framework for security and integrity of networks and services / N. Mayer, J. Aubert // *Journal of Risk Research*. June. 2020. <https://doi.org/10.1080/13669877.2020.1779786>.
10. Singh, A. The Insurance Industry – Cyber Security in the Hyper-Connected Age. Ch. 16 / A. Singh, K. Akhilesh // *Smart Technologies. Scope and Applications* / ed. by K. Akhilesh, D. Möller. Springer Nature Singapore Pte Ltd. 2020. P. 201–219. <https://doi.org/10.1007/978-981-13-7139-4>.
11. Жилкина, М. С. Страхование мошенничества: Правовая оценка, практика выявления и методы пресечения / М. С. Жилкина. М. : Волтерс Клувер, 2005.
12. Russian Insurance Market Survey. 2020. KPMG, 2020.
13. Яковлева, К. Оценка экономической активности на основе текстового анализа / К. Яковлева // *Серия докладов об экономических исследованиях*. № 25. Октябрь 2017. М. : Центральный банк Российской Федерации, 2017.
14. Alt, R. Social Customer Relationship Management. Fundamentals, Applications, Technologies / R. Alt, O. Reinhold. Springer International Publishing, 2019.
15. Knoke, D. Social Network Analysis / D. Knoke, S. Yang. SAGE Publications, 2019.
16. Murphy, D. W. Social Media for Insurance Professionals / D. W. Murphy. Lulu Press, Incorporated, 2011.
17. Strickland, J. Predictive Modeling and Analytics / J. Strickland. Lulu Press, Incorporated, 2014.
18. Умаров, Х. С. Страхование платежных карт от мошеннических операций / Х. С. Умаров // *Страховое дело*. 2020. № 11.