Вестник МИРБИС. 2021. № 1 (25)'. С. 157–162.
Vestnik MIRBIS. 2021; 1(25)': 157–162.

Дискуссионная статья
УДК 338.23
DOI: 10.25634/MIRBIS.2021.1.19

Эффективность машинного обучения как инструмента противодействия корпоративному мошенничеству в организациях розничной торговли

Георгий Алексеевич Зароченцев
Финансовый Университет при Правительстве РФ, Москва, Россия
Nike74oy@gmail.com, https://orcid.org/0000-0003-3117-9309

Аннотация. Цель исследования — раскрыть эффективность такого инструмента как Machine learning в противодействии корпоративному мошенничеству в организациях розничной торговли. В статье дается определение корпоративного мошенничества, рассматриваются его основные виды, а также приводятся новейшие тренды по противодействию данному явлению. Актуальность работы обоснована тем, что согласно отчету, подготовленному Ассоциацией сертифицированных специалистов по расследованию хищений (ACFE), медианная величина потерь от корпоративного мошенничества в сфере розничной торговли, для каждой из компаний, составляет 50 000 долларов США, что является существенной суммой. Результатом исследования является обоснованность внедрения Machine learning для противодействия корпоративному мошенничеству посредством автоматизации контроля и оперативному реагированию на противоправные факты. Материалы статьи представляют практическую ценность прежде всего для внутренних аудиторов, контролеров, аналитиков в сфере розничной торговли.

Ключевые слова: Machine learning, корпоративное мошенничество, розничная торговля, внутренний аудит.

Для цитирования: Зароченцев Г. А. Эффективность машинного обучения как инструмента противодействия корпоративному мошенничеству в организациях розничной торговли / Г. А. Зароченцев // Вестник МИРБИС. 2021; 1(25): 157–162. DOI: 10.25634/MIRBIS.2021.1.19

JEL: Z23

Discussion article

The Perspective of Machine Learning as an Anti-Fraud Tool in Retail Organizations

Georgy A. Zarochentsev
Financial University, Moscow, Russia.
Nike74oy@gmail.com, https://orcid.org/0000-0003-3117-9309

Abstract. The aim of the research is to reveal the effectiveness of such a tool as Machine learning in combating corporate fraud in retail organizations. The article provides a definition of corporate fraud, examines its main types, and also provides the latest trends in countering this phenomenon. The relevance of the work is justified by the fact that according to a report prepared by the Association of Certified Theft Investigators (ACFE), the median loss from corporate fraud in the retail sector for each of the companies is $50,000, which is a significant amount. The result of the research is the validity of the introduction of Machine learning to combat corporate fraud by automating control and prompt response to illegal facts. The materials of the article are of practical value primarily for internal auditors, controllers, analysts in the retail sector.

Key words: Machine learning, corporate fraud, retail, internal audit.

For citation: Zarochentsev G. A. The Perspective of Machine Learning as an Anti-Fraud Tool in Retail Organizations. G. A. Zarochentsev. *Vestnik MIRBIS*. 2021; 1(25)': 157–162. (In. Russ.). DOI: 10.25634/MIRBIS.2021.1.19

JEL: Z23

В сложившейся экономической ситуации одним из важнейших факторов, препятствующим эффективности и результативности бизнеса, является корпоративное мошенничество. В 2016 году 36 % компаний со всего мира признали себя жертвой корпоративного мошенничества, в 2018 году процент увеличился и составил 49 % от числа всех опрошенных по данным PwC [Противодействие мошенничеству.., 2018].

На сегодняшний день, огромные финансовые потоки, бесчисленное количество транзакций и платежных операций для миллионов пользовате-

лей создают благоприятные условия для осуществления различных видов мошенничества. Здесь стоит принять во внимание, что любой случай реализованного мошенничества наносит компании не только материальные убытки (потери имущества, денежных средств, образование упущенной выгоды), но и отложенные последствия, которые оказывают влияние на основные сферы деятельности компании. Также подтверждённый случай корпоративного мошенничества сказывается на внешнем контуре организации, например потеря деловых партнеров, ухудшение деловой репутации на рынке, снижение инвестиционного рейтинга и различные репутационные риски, масштаб которых сложно спрогнозировать.

Доля числа атак, которые нацелены на определенную жертву, сегодня значительно возросла. Сами противоправные действия детально планируются, прорабатываются и осуществляются децентрализовано, автономными группировками преступников, которые специализируются на конкретном виде деятельности: разработка и продажа вредоносного программного обеспечения, обналичивание, взлом каналов связи и другое. Все это, в итоге, приводит к появлению новых схем мошенничества.

Актуальность работы обоснована тем, что согласно отчету, подготовленному Ассоциацией сертифицированных специалистов по расследованию хищений (ACFE), медианная величина потерь от корпоративного мошенничества в сфере розничной торговли, для каждой из компаний, составляет 50 000 долларов США, что является существенной суммой [Report to the nations, 2018].

Рассмотрение данной проблематики необходимо начать с основных понятий. Итак, корпоративное мошенничество – деятельность субъектов экономики, которая направлена на увеличение прибыли или доходов отдельных должностных лиц, имеющая в своей основе противоправный характер. В действительности в совокупности с мошенничеством могут совершаться комплексные преступления, содержащие сразу несколько составов из числа предусмотренных Уголовным кодексом РФ. С точки зрения правоохранительных органов мошенничество отличается латентностью, сложностью и запутанностью расследования и сбора доказательной базы.

Сегодня в законодательстве Российской Федерации отсутствует закрепленное понятие корпоративного мошенничества, единственное упоминание содержится в Разделе 8 «Преступления в сфере экономики». Согласно статье 159 УК РФ мошенничество — это хищение чужого имущества либо приобретение права на чужое имущество, совершаемые обманным путем или злоупотреблением доверием[1]. Уголовный кодекс РФ отдельно устанавливает ответственность за мошенничество: в сфере кредитования (ст. 159.1), при получении выплат (ст. 159.2), с использованием электронных средств платежа (ст. 159.3), в сфере страхования (159.5), в сфере компьютерной информации (ст. 159.6).

МСА 240 «Обязанности аудитора в отношении недобросовестных действий при проведении аудита финансовой отчетности» дает следующее определение корпоративного мошенничества: «это преднамеренное действие одного или нескольких лиц среди руководства субъекта, лиц, наделенных руководящими полномочиями, сотрудников или третьих сторон, с использованием обмана для получения несправедливого или незаконного преимущества»[2].

Ассоциация дипломированных расследователей мошенничества (ACFE) имеет другой подход к определению корпоративному мошенничеству. Так: «это любое преднамеренное действие или бездействие, направленное на обман других, в результате чего потерпевший несет убытки, а преступник получает выгоду» [Ковасич, 2010, с. 52].

Зарубежная и отечественная трактовка корпоративного мошенничества имеют также свои различия.

Джеральд Л. Ковасич в работе «Противодействие мошенничеству. Как разработать и реализовать программу» утверждает: «корпоративное мошенничество является противоправным преступлением, все участники которого получают доступ к корпоративным активам» [Бурдикова, 2013].

Беря во внимание российский опыт к пониманию корпоративного мошенничества, мы можем привести определение И. П. Бурдиковой: «кор-

1 Уголовный кодекс Российской Федерации : Федеральный закон № 63-ФЗ от 13.06.1996 (ред. от 30.12.2020) // СПС КонсультантПлюс.

2 "Обязанности аудитора в отношении недобросовестных действий при проведении аудита финансовой отчетности" устанавливает обязанности аудитора в отношении событий после отчетной даты (МСА 240) // Audit-it.ru : [сайт]. URL: https://www.audit-it.ru/terms/audit/msa_240.html. Дата публикации 17.11.2016,

поративное мошенничество представляет собой любые противоправные действия, которые совершаются сотрудниками компании, связанными с обманом или злоупотреблением ими доверием/полномочиями, в целях личного приобретения или для других лиц, преимуществ неправомерного характера (имеющих любую форму), приводящих к тому, что компания теряет активы (денежные средства, имущество, имущественные права и т. д.), упускает выгоду и/или несет дополнительные убытки и т. д.»[3].

Исходя из выше сказанного, мы можем сделать вывод, что под мошенничество попадают противоправные действия и/или бездействия как со стороны работников компаний (бухгалтеры, менеджеры, топ-менеджмент), так и со стороны сторонних лиц (поставщики, покупатели), которые наносят прямой или косвенный ущерб компании. Стоит отметить, что корпоративное мошенничество невозможно без корреляции с обманом, злоупотреблением доверия и обходом выстроенных контрольных процедур с целью получения выгоды лицом, совершающим противоправное действие и/или бездействие.

Основным составом, вменяемым мошенникам, становится 159 статья УК РФ, но вместе с ней часто появляются и другие — от коммерческого подкупа до фиктивного банкротства. Субъектами таких преступлений в России часто становятся топ-менеджмент, акционеры или генеральный директор организации, хорошо ориентирующиеся в бизнес-процессах компании. Их подготовки хватает на тщательное сокрытие улик, минимизацию всех доказательств, направленных на выявление умысла на совершение именно мошенничества, то есть деяния, направленного на присвоение чужих средств при помощи обмана или злоупотребления доверием. Как правило, мошенничество совершается группой лиц, действия которой направлены на вывод активов, перевод денег в офшоры, подделка отчетность. Нередки у таких групп «лжепредпринимателей» и связи с преступным миром.

Преступники рассчитывают на то, что обманутые не будут сообщать в правоохранительные органы о совершенном факте преступления, так как потерпевшие по тем или иным причинам могут быть привлечены к ответственности, например, за получение наличных денежных средств.

Высокотехнологичные компании из таких отраслей как: промышленность, медицина, финансы, ритейл, транспорт, e-commerce, образование, реклама и маркетинг давно внедрили в свою хозяйствующую деятельность технологии Machine Learning (ML), позволяющие повысить эффективность принимаемых решений высшим руководством и оптимизировать деятельность организации в целом.

На самом базовом уровне машинное обучение — это способ обучения компьютеров, направленный на достижение возможности самообучения системы. Как способ прогнозирования, предотвращения и реагирования на мошенничество, машинное обучение — это мощное сочетание прикладной математики и информатики. Обучая компьютеры, как вести себя и выполнять сложные задачи, машины могут прогнозировать будущие результаты.

Сегодня искусственный интеллект используется для создания «умных» систем во многих сферах экономики, и розничная торговля — не исключение (рисунок 1).

Рис. 1. Проекты по внедрению систем машинного обучения в мире по отраслям 2015–2017 годы (%)

Источник: Форум чемпионов : технологии // "600 крупнейших компаний России". Приложение №179, стр. 14 // Коммерсант : [сайт]. URL: https://www.kommersant.ru/doc/3421530. Дата публикации: 27.09.2017.

Одним из ключевых векторов развития ритейла является оптимизация бизнес-процессов с помощью искусственного интеллекта. Например, для максимально плодотворного взаимодействия с клиентами в аналитический инструментарий и CRM-системы компаний встраиваются алгоритмы машинного обучения, а на сайтах подключаются чат-боты или виртуальные собеседники, цель которых — сразу начать работу с пользователем.

Персональное общение с клиентом с помощью AI, которым сейчас уделяется огромное влияние,

3 Форум чемпионов : технологии // "600 крупнейших компаний России". Приложение №179, стр. 14 // Коммерсант : [сайт]. URL: https://www.kommersant.ru/doc/3421530. Дата публикации: 27.09.2017.

безусловно, играют важную роль, но это слишком узкая сфера применения для AI/ML. Главная ценность этих технологий для ритейла связана с такими областями, как, например, оптимизация товарных матриц и цепочек поставок, прогнозирование спроса и выявление внутрикорпоративного мошенничества. По сути, внутренние бизнес-процессы, невидимые для глаза клиента, как раз и определяют всю эффективность работы [Колесников, 2018].

Хотя машинное обучение является преимуществом практически для любой отрасли, сейчас оно становится все более мощным инструментом управления рисками для компаний, надеющихся выявить и предотвратить мошенничество. По мере развития технологий онлайн-мошенничество становится все более распространенным и более разрушительным, особенно для розничных торговцев, которые работают на разных платформах (например, мобильные приложения, онлайн платформы).

По мере роста электронной коммерции компании подвергаются пропорциональному росту в мошеннических транзакциях. В 2014 году 65 % организаций с доходами свыше 1 млрд. Долл. США стали жертвами мошенничества в режиме онлайн-платежей, и к 2015 году каждый 100 долларов США мошенничества фактически стоил торговцам 223 доллара. Более чем 90 % компаниям, сталкивающимися с онлайн-мошенничеством, машинное обучение дает доступ к мощным инструментам, которые ранее были недостижимы[1].

Перед тем как перейти к описанию Machine Learning как инструмента противодействия мошенничеству, следует рассмотреть общие мошеннические схемы в розничной торговле:

1. Отмененные транзакции: товар оплачивается, доставляется/выдается, а затем транзакция отменяется/товар возвращается в магазин. Это просто, но часто трудно заметить закономерность и корреляцию.
2. Предпочтительные скидки: продажа предметов для семьи и друзей по скидке сотрудника, далее возврат полной стоимости купленного товара в разных магазинах без квитанции.
3. Sweethearting: предоставление бесплатного товара или скидки для семьи и друзей без надлежащего разрешения, часто просто не сканируя продукты. Эта категория также может включать ложные возвращается.
4. Фальшивые возвраты:

- Wardrobing/renting: Покупка товара с намерением вернуть на следующий день, например, платье для большой даты;
- мошенничество с получением возмещения: использование повторно украденных товаров или фальсифицированных квитанций для возврата товара.

5. Тренировка мошенничества: менеджеры во время обучения новых сотрудников имеют право запрограммировать денежные регистры, поэтому продажи не регистрируются. Сотрудники злоупотребляют этой функцией, когда они покупают товары в магазине.

Сейчас большинство розничных продавцов пытаются обнаружить мошенничество устаревшими методами EBR, которые заключаются в идентификации простых транзакции на основе правил аномалий. Эти правила могут включать простое сопоставление, сортировку, фильтрацию или арифметические процедуры. Этот подход часто приводит к большому количеству ложных срабатываний.

Специалисты по борьбе с мошенничеством, которые ориентированы на обнаружение риска потерь, могут потратить слишком много времени и ресурсов на выявления рисков злоупотреблений, в то время как процедура анализа может выдать ложные выводы. Это может происходить, когда аналитические системы дайте слишком много «ложных срабатываний», (т. е. транзакции, которые удовлетворяют определенным показатели риска, но на самом деле не являются ошибочными или мошеннические) или «ложные негативы», (то есть, когда ошибочные или мошеннические транзакции занижены и контроль их не выявил).

Развитие глобального «quick service» ускорило скорость обнаружения кражи и мошенничества со стороны сотрудников прикассовой зоны примерно в три раза. Quick service построены на анализе географии регионов, магазинов, сотрудников и POS-транзакций, а также интеграцию "машинного обучения" для улучшения обнаружения мошенничества.

1 Machine Learning's Growing Role in the Fight Against Payment Fraud // Bluefin : [сайт]. URL: https://www.bluefin.com/bluefin-news/can-machine-learning-fight-fraud/. Дата публикации: 05.07.2017.

Внедрение машинного обучения начинается с моделирования известного поведения сотрудников, крадущих из кассовых аппаратов компании. Пробные модели рассчитывают схемы мошенничества путем объединения нескольких источников данных, которые включали POS, информацию о местоположении магазина и поведение сотрудников. Далее модели машинного обучения используют статистический бенчмаркинг и десятки алгоритмов для оценки и ранжирования рисков, которые потенциально существовали при осуществлении транзакций, деятельности сотрудников, продаже товаров в магазинах и регионах.

Затем модели машинного обучения визуализируют данные, которые позволяют получить общее представление о рисках, специально адаптированных к потребностям организации. При выявлении новых закономерностей или корреляций, они добавляются в систему машинного обучения и уточняют прогнозы в реальном времени.

Основная цель, лежащая в основе построения алгоритмов machine learning, заключается в анализе поведения человека на «способность» к мошенничеству. Например, машинное обучение уже сегодня позволяет выявить мошенничество с картами лояльности. Если система обнаруживает, что за день карта лояльности сотрудника (кассира) работала несколько раз за день в одинаковых точках (магазинах), система идентифицирует это как мошенничество.

Таким образом, внедрение системы противодействия мошенничеству обеспечит ритейлер технологической платформой для обнаружения инцидентов, прямо или косвенно указывающих на возможные случаи мошенничества со стороны клиентов и/или сотрудников. В целом это позволяет предотвращать хищения с помощью применения средств детектирования и оперативного реагирования на попытки совершения мошенничества. Значительно снижается риск возникновения новых схем хищений, готовящиеся операции выявляются еще на этапах подготовки. Идет постоянный контроль над несанкционированными действиями сотрудников в режиме реального времени, оптимизируются процессы проведения проверок и расследований, связанные с превышением должностных полномочий или совершением противоправных действий.

Список источников

1. Бурдикова, 2013 — *Бурдикова И. П.* Системы противодействия мошенничеству и их место в корпоративном управлении / И. П. Бурдикова // Безопасность бизнеса. 2013. № 4. С. 33–36. ISSN: 2072-3644.
2. Ковасич, 2010 — *Ковасич Дж. Л.* Противодействие мошенничеству. Как разработать и реализовать программу мероприятий / Джеральд Л. Ковасич. Москва: Маросейка, 2010. 307 с. ISBN:978-5-903271-31-3.
3. Колесников, 2018 — *Колесников Е.* Перспективы искусственного интеллекта и машинного обучения в сфере ритейла // Retail&Loyalty : [сайт]. URL: https://www.retail-loyalty.org/expert-forum/perspektivy-iskusstvennogo-intellekta-i-mashinnogo-obucheniya-v-sfere-riteyla/. Дата публикации 29.08 2018
4. Противодействие мошенничеству.., 2018 — Противодействие мошенничеству: какие меры принимают компании? Российский обзор экономических преступлений за 2018 год / PwC, 2018. 28 с. URL: https://www.pwc.ru/ru/forensic-services/assets/PwC-recs-2018-rus.pdf.
5. Report to the nations, 2018 — Report to the nations : 2018 Global study on occupational fraud and abuse / ACFE, 2018. 80 p. URL: https://s3-us-west-2.amazonaws.com/acfepublic/2018-report-to-the-nations.pdf.

References

1. Burdikova I. P. Sistemy protivodeystviya moshennichestvu i ikh mesto v korporativnom upravlenii [Anti-fraud systems and their place in corporate governance]. I. P. Burdikova. *Bezopasnost' biznesa* [Business Security]. 2013. No. 4. P. 33–36. ISSN: 2072-3644 (in Russ.).
2. Kovasich J. L. *Protivodeystviye moshennichestvu. Kak razrabotat' i realizovat' programmu meropriyatiy* [Fraud prevention. How to develop and implement a program of events]. Gerald L. Kovasich. Moscow : Maroseyka Publ., 2010. 307 p. ISBN: 978-5-903271-31-3 (in Russ.).
3. Kolesnikov E. Perspektivy iskusstvennogo intellekta i mashinnogo obucheniya v sfere riteyla [Prospects for Artificial Intelligence and Machine Learning in Retail]. *Retail & Loyalty* : [website]. URL: https://www.retail-loyalty.org/expert-forum/perspektivy-iskusstvennogo-intellekta-i-mashinnogo-obucheniya-v-sfere-riteyla/. Publication date 29.08 2018 (in Russ.).

4. *Protivodeystviye moshennichestvu: kakiye mery prinimayut kompanii? Rossiyskiy obzor ekonomicheskikh prestupleniy za 2018 god* [Anti-Fraud: What Measures Are Companies Taking? Russian Economic Crime Survey 2018]. PwC, 2018.28 p. URL: https://www.pwc.ru/ru/forensic-services/assets/PwC-recs-2018-rus.pdf (in Russ.).
5. *Report to the nations : 2018 Global study on occupational fraud and abuse*. ACFE, 2018. 80 p. URL: https://s3-us-west-2.amazonaws.com/acfepublic/2018-report-to-the-nations.pdf.

Информация об авторе:

Зароченцев Георгий Алексеевич —Финансовый Университет при Правительстве РФ, Ленинградский пр-т., 49, Москва, 125167, Россия.

Information about the author:

Zarochentsev Georgy A. – Financial University, 49 Leningradsky prospekt, Moscow, 125167, Russia.

Статья поступила в редакцию 02.12.2020; одобрена после рецензирования 24.12.2020; принята к публикации 24.12.2020.
The article was submitted 12/02/2020; approved after reviewing 12/24/2020; accepted for publication 12/24/2020.