**УДК 657.632 DOI: 10.14451/1.239.215**

# Применение методов интеллектуального анализа данных в аудиторских процедурах в ответ на риски существенного искажения вследствие недобросовестных действий

© 2024 **Сушков Виктор Михайлович**
Ассистент кафедры финансового мониторинга. Национальный исследовательский ядерный университет МИФИ.
E-mail: vmsushkov@mephi.ru

Ключевые слова: аудит, риски, недобросовестные действия, мошенничество, интеллектуальный анализ данных, закон Бенфорда, кластеризация, байесовская статистика.

В условиях роста масштабов финансового мошенничества приобретает актуальность совершенствование подходов к проведению аудиторских процедур в ответ на риски существенного искажения вследствие недобросовестных действий. Данное исследование направлено на восполнение научного пробела, заключающегося в недостаточной интеграции методов интеллектуального анализа данных в аудиторские процедуры для выявления сложных и запутанных схем недобросовестных действий. В работе проведен комплексный анализ сущности недобросовестных действий и методов интеллектуального анализа данных с целью их адаптации под специфику аудиторской детальности. Особое внимание уделено закону Бенфорда, кластеризации и байесовской статистике. Результаты исследования призваны внести вклад в развитие методологии аудита и повысить эффективность и качество аудиторских проверок.

В современных условиях экономической деятельности недобросовестные действия на уровне хозяйствующих субъектов представляют серьезную угрозу экономической безопасности. Внешний финансовый аудит является одним из основных институтов их выявления и предупреждения. Сегодня немодифицированное аудиторское заключение в глазах пользователей отчетности не только служит подтверждением отсутствия ошибок, но также воспринимается в качестве гаранта добросовестности собственников и персонала компании, развитой корпоративной культуры и нетерпимости к мошенническим проявлениям. В то же время с ростом объема финансовых операций и темпов цифровизации процесс разработки и реализации аудиторских процедур в ответ риски существенного искажения финансовой отчетности вследствие недобросовестных действий (далее — РСИНД) становится все более сложным и трудоемким. Для обеспечения разумной уверенности в том, что финансовая отчетность не содержит существенных искажений вследствие недобросовестных действий, аудиторские организации и индиви-

дуальные аудиторы вынуждены разрабатывать и применять новые эффективные подходы.

В соответствии с Международным стандартом аудита (МСА) 240, под недобросовестными действиями (англ. fraud) понимаются умышленные действия одного или нескольких лиц из числа руководства, лиц, отвечающих за корпоративное управление, сотрудников или третьих лиц, совершенные при помощи обмана для получения неправомерных или незаконных преимуществ [3, п. 11 (b)]. Следует отметить, что понятие недобросовестных действий в контексте МСА является специфичной категорией и отличается от понятий мошенничества, корпоративного мошенничества, нарушений требований к бухгалтерскому учету и пр. Ключевые особенности категории «недобросовестные действия» заключаются в следующем:

1. Для целей МСА рассматриваются только те недобросовестные действия, которые могут привести к существенным искажениям в финансовой отчетности [3, п. 3].
2. Недобросовестные действия включают в себя фальсификацию финансовой отчетности и неправомерное присвоение активов [3, п. 3].

Данная особенность отражает отличие недобросовестных действий от корпоративного мошенничества, которое в соответствии с классификацией Ассоциации сертифицированных экспертов по расследованию мошенничества (ACFE, Association of Certified Fraud Examiners) также включает коррупцию. Данная классификация известна как «дерево мошенничества» (рис. 1).

3. Недобросовестным действиям не дается правовая оценка.

Несмотря на то, что аудитор может подозревать или в редких случаях (как указывает МСА 240) выявлять наличие недобросовестных действий, он не определяет с правовой точки зрения, действительно ли имели место недобросовестные действия [3, п. 3]. Кроме того, зачастую аудитору сложно определить, вызваны искажения показателей финансовой отчетности, особенно требующих суждения, недобросовестными действиями или ошибкой [3, п. 6]. Идея об ограниченности возможностей аудитора в части выявления недобросовестных действий превалирует во всем содержании МСА 240.

Согласно исследованию «ACFE Report to the nations» за 2023–2024 годы, масштабы недобросовестных действий в экономической сфере имеют глобальный характер. В частности, результаты исследования демонстрируют следующее:

- в среднем компании теряют 5% своей годовой выручки вследствие различных форм корпоративного мошенничества;
- общемировые финансовые потери от корпоративного мошенничества ежегодно достигают 5 триллионов долларов США;
- более чем в каждом пятом случае корпоративного мошенничества финансовые потери превышают 1 миллион долларов США [10].

Указанные данные подтверждают проблему значительного негативного влияния недобросовестных действий и подчеркивают острую необходимость в разработке и внедрении эффективных мер по предотвращению и выявлению мошеннических действий в корпоративном секторе.

Международные стандарты аудита устанавливают лишь рамочные требования к проведению аудиторских процедур в ответ на РСИНД, что требует от аудиторских организаций и индивидуальных аудиторов разрабатывать собственные методологии. На текущий момент наиболее объемной и, как следствие, эффективной процедурой является проверка надлежащего характера бухгалтерских записей. Целью данной аудиторской процедуры является выявление признаков недобросовестности вследствие обхода руководством средств контроля. Преобладающие практики аудиторских организаций на сегодняшний день включают тестирование массива бухгалтерских записей с помощью простейших статистических методов — отбор, сор-

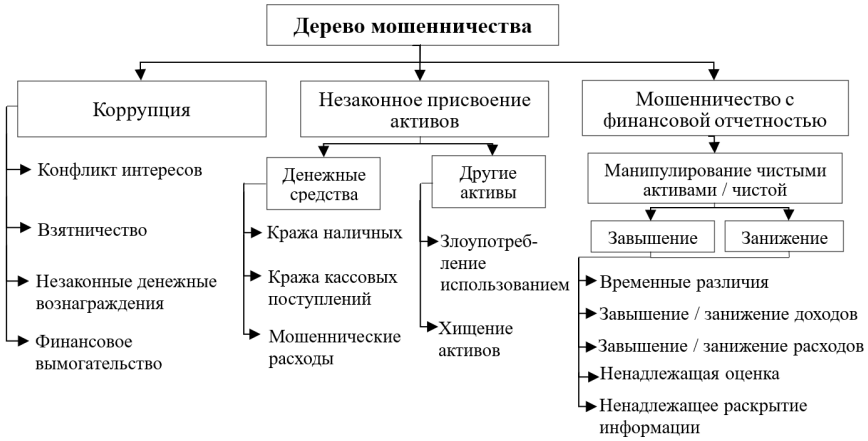


**Рис. 1.** «Дерево мошенничества» ACFE (обобщенная форма).

тировка, фильтрация и группировка по рисковым критериям [8]. В то же время подобный подход доказывает свою неэффективность перед выявлением сложных и запутанных схем недобросовестных действий, признаки которых надежно маскируются. Кроме того, классическая статистика и визуальный анализ ограничены в своей способности выявлять неочевидные закономерности, скрытые аномалии и потенциальные риски в больших объемах данных. В условиях увеличивающейся сложности и структурной изменчивости бухгалтерских операций и финансовой отчетности наиболее актуальными и перспективными методами реализации аудиторских процедур в ответ на РСИНД представляются методы интеллектуального анализа данных, или data mining.

Термин data mining был введен президентом и главным редактором сайта KDnuggets.com Г. И. Пятецким-Шапиро на семинаре Knowledge Discovery in Real Databases [16] в рамках международной научной конференции по искусственному интеллекту IJCAI (The 11th International Joint Conference on Artificial Intelligence) в 1989 году [18]. Г. И. Пятецкий-Шапиро также ввел термин knowledge discovery in databases (KDD), что в переводе означает «обнаружение знаний в базах данных» [16]. Несмотря на потенциально более точное отражение сути концепции, KDD не прижился ни в научных кругах, занимающихся теоретическими исследованиями данной области, ни среди практиков в корпоративном секторе, применяющих указанные методы в реальных условиях. В соответствии с данными онлайн-сервиса Google Ngram Viewer, позволяющим анализировать частотность языковых единиц в печатных источниках, термин data mining встречается в 11 раз чаще, чем термин knowledge discovery in databases (KDD) (рис. 2).

Дословный перевод data mining — добыча данных, однако в российской научной и практической литературе термин, как правило, переводится иначе. При этом общепринятый вариант на сегодняшний день отсутствует. Согласно одному из наиболее полных англо-русских словарей «Мультитран», популярные версии перевода data mining следующие: интеллектуальный анализ данных, анализ данных, интеллектуальный анализ, поиск закономерностей в базах данных, интерпретация и представление данных, извлечение знаний из данных, извлечение информации и др. Анализ перевода термина с использованием сервиса Reverso Context позволил определить, что наиболее частотный вариант перевода — интеллектуальный анализ данных (рис. 3).

Следующим по частотности вариантом является Data Mining, то есть сохранение термина на языке оригинала без транслитерации. При этом оба слова пишутся с прописной буквы. Примером такого перевода в контексте может быть следующее предложение: «Data mining is

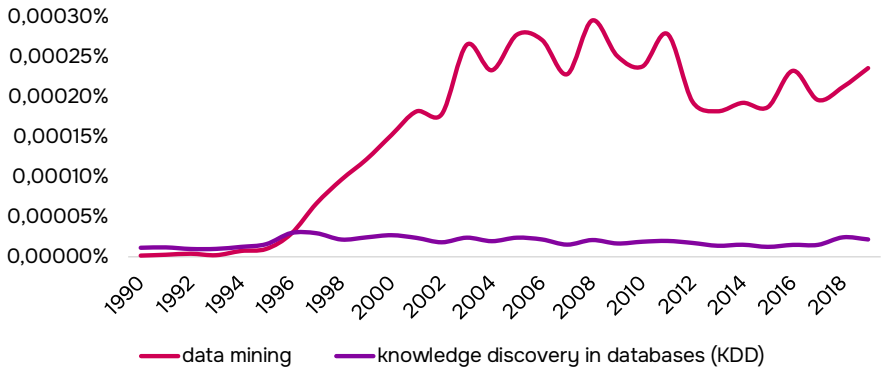


**Рис. 2.** Частотность употребления терминов data mining и knowledge discovery in databases (KDD).

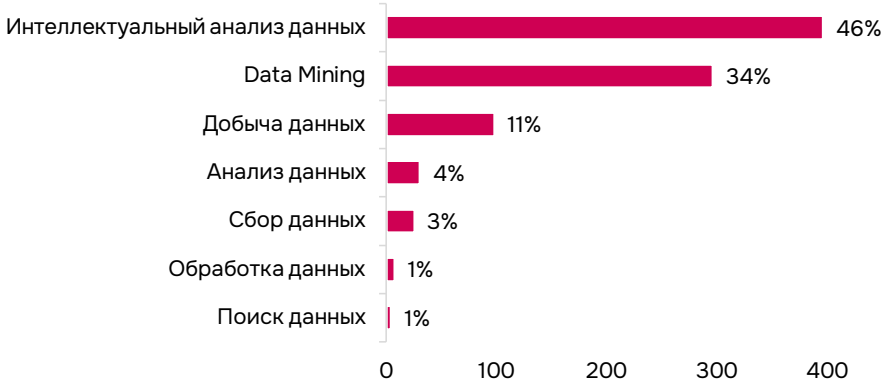


**Рис. 3.** Частотность перевода термина data mining.

used in the banking sector» (англ.) — «Data Mining применяется в банковской сфере» (рус.). Причиной популярности данного варианта является отсутствие универсального термина, эквивалентного английскому data mining, вследствие чего специалисты по переводу прибегают к его сохранению на языке оригинала во избежание двусмысленной интерпретации. Однако учитывая современные требования к использованию общеупотребительных аналогов иностранных терминов во всех случаях, когда они существуют, и во исполнение п. 6 ст. 1 Федерального закона от 01.06.2005 г. № 53-ФЗ «О государственном языке Российской Федерации», в данном исследовании будем придерживаться термина «интеллектуальный анализ данных».

Вопрос корректности использования термина «интеллектуальный анализ данных», тем не менее, остается спорным. Так, например, А. Г. Дьяконов считает, что прилагательное «интеллектуальный» является излишним, поскольку «неинтеллектуального» анализа данных не существует [1]. Кроме того, в английском языке также есть понятие intelligent data analysis, не эквивалентное data mining. В ответ следует привести следующие аргументы. Во-первых, термин «анализ данных» является достаточно широким и встречается в контекстах, выходящих за извлечение из данных знаний с помощью математического и статистического инструментария. Во-вторых, прилагательное «интеллектуальный» указывает на способность методов данного типа выявлять закономерности, недоступные для обнаружения человеком с помощью стандартных подходов. В этом контексте «неинтеллектуальный» анализ — это анализ посредством классических методов математической статистики и визуального наблюдения, в которых задача по интерпретации результатов обработки данных (выявлению знаний) ложится на аналитика. В-третьих, в англоязычных источниках intelligent data analysis используется преимущественно не как самостоятельный термин, а как обычное словосочетание, вследствие чего смешения

или подмены терминов не происходит. Наконец, «анализ данных» в качестве перевода data mining является непопулярным вариантом в российской литературе и встречается лишь в 4% случаев (рис. 3).

Унифицированное определение термина «интеллектуальный анализ данных» (Data Mining) отсутствует как в российской, так и в зарубежной литературе, что обосновывает необходимость его уточнения. Сложность толкования, в частности, связана с неоднозначностью места интеллектуального анализа данных в общей системе наук. Анализ подходов к определению термина «интеллектуальный анализ данных» позволяет выявить его ключевые характеристики, а именно:

- мультидисциплинарность — интеллектуальный анализ данных базируется на методах нескольких научных областей, включая математическую статистику, машинное обучение, теорию баз данных, распознавание образов и др.;
- обобщенность — интеллектуальный анализ данных является собирательным термином, объединяя в себе различные методы анализа данных;
- нетривиальность — интеллектуальный анализ данных позволяет обрабатывать неточные, неполные, разнородные данные, имеет возможность обучаться (делать общие выводы на основе частных наблюдений);
- высокая вычислительная мощность — интеллектуальный анализ данных позволяет обрабатывать массивы данных большого объема;
- полезность — целью интеллектуального анализа данных является выявление знаний, то есть ранее неизвестной (неожиданной), практически полезной, доступной для интерпретации и принятия решений информации [4; 5; 11; 17].

На основе вышеуказанных характеристик можно сформулировать комплексное определение термина «интеллектуальный анализ данных» как мультидисциплинарной научной области, объединяющей в себе совокупность методов нетривиального извлечения из больших объемов данных ранее неизвестной (неожиданной), практически полезной, доступной для интерпретации и принятия решений информации.

Практическая реализация интеллектуального анализа данных производится при помощи методов. На данный момент разработано множество методов интеллектуального анализа данных. Наиболее распространенными являются искусственные нейронные сети, регрессионный, дисперсионный, дискриминантный, факторный анализ, кластеризация, нечеткая логика, байесовская статистика, статистические вычисления на основе закона Бенфорда. Указанные методы, несмотря на их разнообразие, решают ограниченное число практических задач:

1. Кластеризация — процесс распределения объектов в сравнительно однородные группы на основе сходства признаков;
2. Классификация — процесс распределения объектов по заранее известному набору классов на основе обучающей выборки;
3. Выявление аномалий — процесс поиска абнормальных объектов, которые отличаются от ожидаемых и могут являться признаками необычных событий;
4. Прогнозирование — процесс выявления тенденций и закономерностей в исторических данных и предсказывания будущих значений на их основе;
5. Визуализация — процесс преобразования данных в графический вид для облегчения анализа;
6. Распознавание образов — процесс идентификации шаблонов в данных, как правило, текстовых и визуальных;
7. Поиск ассоциаций — процесс выявления скрытых закономерностей, связей или корреляции между различными признаками в данных;
8. Эффективные вычисления — процесс обработки больших объемов данных с высокой скоростью.

Учитывая, что массивы бухгалтерских записей аудируемых лиц содержат большое количе-

ство «тривиальных» данных, то есть стандартных финансово-хозяйственных и технических операций, которые представляют небольшой интерес в рамках рассмотрения недобросовестных действий, аудиторам необходимо выявить среди них лишь небольшое число высокорискованных бухгалтерских записей, обладающих признаками недобросовестных действий. Кроме того, значительный объем операций, совершенных за проверяемый период (как правило, год), увеличивает трудозатраты на проведение процедур. Таким образом, в рамках рассмотрения недобросовестных действий в ходе аудита финансовой отчетности наиболее приоритетными задачами можно назвать выявление аномалий, поиск ассоциаций, кластеризация и классификация.

Анализ научной литературы, практических публикаций, аналитических обзоров, презентаций, мастер-классов и прочих публичных данных в России и за рубежом демонстрирует, что наиболее применимыми методами интеллектуального анализа данных в указанных целях являются закон Бенфорда, кластеризация и байесовская статистика [2; 7; 9; 12–14]. Причиной является их универсальность и возможность разработки единого алгоритма для анализа массива бухгалтерских записей независимо от особенностей хозяйствования аудируемого лица. Иные распространные методы, например, нейронные сети, требуют адаптации под конкретную узкоспециализированную задачу, вследствие чего скорее применимы для согласованных процедур и заданий, обеспечивающих, уверенность, нежели чем для аудиторских проверок. Рассмотрим характеристики каждого из вышеуказанных методов.

**Закон Бенфорда** – это статистическое наблюдение, в соответствии с которым в наборах числовых данных из множества естественных источников первая цифра имеет дискретное экспоненциальное распределение. Так, цифра 1 появляется в качестве первой примерно в 30% случаев, в то время как цифра 9 – только в 4,6% случаев. Закономерность была обнаружена в 1881 году астроном Саймоном Ньюкомбом и формализована в 1938 году физиком Фрэнком Бенфордом. Вероятность цифры $D_1$ оказаться на первом месте исчисляется по формуле (1).

$$P(D_1 = d_1) = \log_b\left(1 + \frac{1}{d_1}\right), \quad (1)$$

где $b$ – система счисления ($b > 2$); $d_1$ – цифры в данной системе счисления ($d_1 \in \{1, \dots, b - 1\}$) [15].

Закон Бенфорда является эффективным инструментом для анализа финансовой информации на предмет возможных искажений, в частности, при исследовании данных бухгалтерского учета. Путем сопоставления частоты появления цифр в исследуемых данных с ожидаемым распределением Бенфорда можно обнаружить отклонения, свидетельствующие о потенциальных недобросовестных действиях. Так, американский ученый Марк Нигрини в работе [15] предложил комплексную методологию применения статистических тестов, основанных на законе Бенфорда, для выявления мошеннических действий в различных корпоративных данных. Тем не менее, в некоторых случаях результаты, достигнутые с использованием предложенных методов, являются противоречивыми и неоднозначными для интерпретации. Указанные ограничения были разрешены, а подходы к анализу данных бухгалтерского учета с помощью закона Бенфорда в ходе аудита финансовой отчетности значительно усовершенствованы в исследованиях российских ученых [2; 6; 12; 13; 20].

**Кластеризация** – это метод интеллектуального анализа данных, который группирует объекты с похожими характеристиками (транзакции, финансовые показатели, данные оперативного учета) в кластеры, выявляя при этом выбросы и аномалии. Кластеризация основана на расчете сходства объектов в многомерном пространстве признаков, используя метрики расстояния (евклидово, Чебышева, Хэмминга и др.) или плотность распределения. Кластерные процедуры делятся на иерархические и итерационные. Иерархические строят последовательную структуру кластеров, в которой каждый объект либо


**Рис. 4.** Система выявления признаков недобросовестных действий с помощью интеллектуального анализа данных.

объединяется с ближайшими кластерами (агломеративные процедуры), либо, наоборот, разделяется на более мелкие кластеры (дивизимные процедуры). Итерационные процедуры, такие как метод К-средних, DBSCAN, искусственные нейронные сети, инициализируют центроиды кластеров и последовательно в ходе нескольких итераций перераспределяют объекты между кластерами с целью минимизации критерия кластеризации, например, суммы квадратов расстояний до центроидов.

Кластерный анализ открывает широкие возможности для выявления признаков недобросовестных действий. Объекты, не входящие ни в один кластер или формирующие небольшие группы, могут сигнализировать о потенциальных нарушениях. Специфика анализируемых объектов и выбор характеристик определяются целями проверки. В качестве примера можно привести исследование [14], в котором авторы применили метод К-средних для кластеризации двумерных данных о дневной выручке АЗС и их доле в недельном обороте. Данный подход позволил обнаружить случаи хищения нефтепродуктов, сократив трудозатраты на 62%.

**Байесовская статистика** – это совокупность методов, основанных на теореме Томаса Байеса, которая позволяет определить вероятность возникновения одного события с учетом другого статистически связанного события и обновлять вероятностные оценки на основе новой информации.

Математически теорема Байеса выражается формулой (2).

$$P(H \mid E) = P(E \mid H) \cdot P(H)/P(E), \qquad (2)$$

где $P(H \mid E)$ – апостериорная вероятность гипотезы $H$ при наличии свидетельства $E$; $P(E \mid H)$ – правдоподобие, вероятность наблюдения свидетельства $E$ при истинности гипотезы $H$; $P(H)$– априорная вероятность гипотезы $H$; $P(E)$ – безусловная вероятность свидетельства $E$.

В соответствии с принципами байесовского подхода изначально задаются априорные вероятности рассматриваемых гипотез, например, наличия или отсутствия недобросовестных действий. Затем, по мере поступления новых данных (свидетельств), данные вероятности последовательно обновляются в соответствии с формулой теоремы Байеса. Апостериорные вероятности, полученные на одном шаге, становятся априорными вероятностями для следующего шага.

Байесовские методы позволяют гибко комби-

нировать имеющиеся знания предметной области через априорные распределения с эмпирическими данными, полученными в ходе аудита. Подход дает возможность явно учитывать неопределенность и находить компромисс между сложностью модели и ее соответствием данным. В рамках выявления признаков недобросовестных действий в ходе аудита с помощью байесовской статистики можно использовать следующий алгоритм:

1. Определить набор признаков, потенциально указывающих на наличие недобросовестных действий (аномалии, несоответствия и пр.);
2. На основе предыдущего опыта и экспертных знаний задать априорные вероятности наличия и отсутствия недобросовестных действий;
3. Для каждого признака рассчитать его правдоподобие при наличии и отсутствии недобросовестных действий;
4. По мере выявления признаков в ходе аудита обновлять апостериорные вероятности недобросовестных действий с помощью формулы теоремы Байеса;
5. Если апостериорная вероятность нарушений превышает определенный порог, считать это сигналом для более детального изучения.

Байесовский подход представляет собой обоснованный и перспективный инструмент, позволяющий более гибко и комплексно подходить к анализу рисков недобросовестных действий за счет:

– интеграции экспертных знаний через априорные распределения;
– динамического обновления вероятностей при поступлении новых данных;
– вероятностной оценки наличия недобросовестных действий вместо бинарного ответа;
– эффективной работы в условиях неопределенности и неполноты информации.

Комплексный подход к интеграции методов интеллектуального анализа данных в аудиторские процедуры в ответ на РСИНД может быть структурирован в виде схемы (рис. 4) [7].

Таким образом, совершенствование методологии аудита посредством интеграции интеллектуального анализа данных в процедуры, направленные в ответ на РСИНД, является не только актуальной задачей, но и стратегическим императивом для аудиторской профессии. Данное направление требует дальнейших исследований, разработки практических руководств и инвестиций в обучение аудиторов новым технологиям. Успешное применение методов интеллектуального анализа данных может значительно повысить качество аудиторских услуг, укрепить доверие к финансовой отчетности и, в конечном итоге, способствовать повышению стабильности и прозрачности бизнеса. В эпоху цифровой трансформации и растущей сложности экономических отношений аудиторская профессия должна идти в ногу с технологическим прогрессом, чтобы эффективно выполнять свою роль в обеспечении достоверности финансовой информации и защите интересов пользователей финансовой отчетности.

**Библиографический список**


1. *Дьяконов А. Г.* Некоторые задачи дискретной математики, возникающие в современных приложениях при анализе данных // Spectral and Evolution Problems. — 2012. — № 22. — С. 66—75.
2. *Леонов П. Ю., Сушков В. М.* Закон Бенфорда как инструментарий выявления признаков недобросовестных действий в бухгалтерском учете. — М. : Российский экономический университет имени Г. В. Плеханова, 2023. — 180 с. — ISBN 978-5-7307-2063-3.
3. Международный стандарт аудита 240 «Обязанности аудитора в отношении недобросовестных действий при проведении аудита финансовой отчетности» (введен в действие на территории Российской Федерации Приказом Минфина России от 09.01.2019 № 2н) (ред. от 16.10.2023) / СПС КонсультантПлюс.
4. *Прокопец Т. Н., Синюк Т. Ю., Рыбалко Ю. А.* Методы интеллектуального анализа данных // Устойчивое развитие экономики: состояние, проблемы, перспективы : сборник трудов XVI международной научно-практической конференции, Пинск, 29 апреля 2022 г. : в 2 ч. Министерство образования Республики Беларусь. — Пинск : ПолесГУ, 2022. — С. 301—304.

5. *Степанов Р. Г.* Технология Data Mining: интеллектуальный анализ данных. — Казань : Казанский государственный университет им. В.И.Ульянова-Ленина (КГУ), 2008. — 58 с.
6. *Сушков В. М.* Классификация и систематизация схем недобросовестных действий, выявляемых в ходе аудита финансовой отчетности // Аудитор. — 2024. — Т. 10, № 6. — С. 10—20. — DOI: 10.12737/1998-0701-2024-10-6-10-20.
7. *Сушков В. М.* Методы интеллектуального анализа данных в аудиторских процедурах оценки рисков существенного искажения вследствие недобросовестных действий // Финансовая безопасность. Современное состояние и перспективы развития : Материалы VIII Международной научно-практической конференции Международного сетевого института в сфере ПОД/ФТ, Москва, 14–15 декабря 2022 года. Т. 1. — М. : МИФИ, 2022. — С. 438—451.
8. *Сушков В. М., Леонов П. Ю.* Методологический подход к оценке риска недобросовестных действий аудируемого лица на основе анализа высокорискованных бухгалтерских записей // Материалы III Международного научно-практического форума по экономической безопасности «VIII ВСКЭБ» : Сборник материалов Международного научно-практического форума, Москва, 26–28 апреля 2022 года. — М. : МИФИ, 2022. — С. 111—126.
9. A Bayesian Network-Based Model for Fraud Risk Assessment / P. Y. Leonov [et al.] // Biologically Inspired Cognitive Architectures 2023. — Springer Nature Switzerland, 2024. — P. 520–527. — ISBN 9783031503818. — DOI: 10.1007/978-3-031-50381-8_55.
10. ACFE Report to the Nations 2024 / Association of Certified Fraud Examiners. — URL: https://legacy.acfe.com/report-to-the-nations/2024 (visited on 10/01/2024).
11. *Han J., Kamber M., Pei J.* Data Mining: concepts and techniques. — Morgan Kaufmann, 2006.
12. Improving the Methodology for Integrated Testing of Journal Entries by Benford's Law / P. Y. Leonov [et al.] // Biologically Inspired Cognitive Architectures 2023. — Springer Nature Switzerland, 2024. — P. 512–519. — ISBN 9783031503818. — DOI: 10.1007/978-3-031-50381-8_54.
13. Integrating Data Mining Techniques for Fraud Detection in Financial Control Processes / V. M. Sushkov [et al.] // International Journal of Technology. — 2023. — Vol. 14(8). — P. 1675–1684. — DOI: 10.14716/ijtech.v14i8.6830.
14. K-Means Method as a Tool of Big Data Analysis in Risk-Oriented Audit / P. Y. Leonov [et al.] // Communications in Computer and Information Science. — 2019. — Vol. 1054. — P. 206–216.
15. *Nigrini M. J.* Benford's Law: Applications for forensic accounting, auditing, and fraud detection. — John Wiley & Sons, 2012.
16. *Piatetsky-Shapiro G. S.* Knowledge Discovery in real databases: A report on the IJCAI-89 Workshop // AI Magazine. — 1991. — Vol. 1, no. 5. — P. 68–70.
17. *Piatetsky-Shapiro G. S., Frawley W. J.* Knowledge Discovery in Databases. — Cambridge, MA : AAAI/MIT Press, 1991.
18. Proceedings of the 11th International Joint Conference on Artificial Intelligence. Detroit, MI, USA, August 1989. — Morgan Kaufmann, 1989. — URL: http://ijcai.org/proceedings/1989-1 (visited on 10/01/2024).
19. *Sharma A. P. P.* A Review of Financial Accounting Fraud Detection based on Data Mining Techniques // International Journal of Computer Applications. — 2013. — No. 39.
20. *Сушков В. М.* Оценка рисков недобросовестных действий в дорожно-строительном секторе экономики // Экономика, предпринимательство и право. — 2024. — Vol. 14, no. 8. — P. 4311–4324. — DOI: 10.18334/epp.14.8.121153.