АНАЛИЗ БОЛЬШИХ МАССИВОВ ДАННЫХ В ЦЕЛЯХ РАССЛЕДОВАНИЯ ФАКТОВ МОШЕННИЧЕСТВА

Сидоренко М.Е., магистрант,
Рогулин Ю.П., кандидат экономических наук, доцент,
Финансовый университет при Правительстве РФ

Аннотация: в эпоху «цифровизации» компании сталкиваются с проблемой эффективного использования цифровых данных для защиты своих интересов, снижения рисков финансовых преступлений, оптимизации деятельности и развития бизнеса. В современном мире технологии развиваются невероятно быстрыми темпами, тем самым оказывая влияние на многие отрасли бизнеса, включая ведение бухгалтерского учета и проведения аудита. Технологическое развитие позволило внедрить в организации автоматизированные системы учета, которые позволяют компаниям перейти от традиционного учета к автоматизированному учету.

Требуется отметить, что недавние законодательные акты и нормативные инициативы направлены на ужесточение мер по противодействию финансовым преступлениям для компаний. Однако, ужесточения контроля приводит к существенному увеличению расходов компаний, связанных с противодействием финансовым преступлениям. Размер дополнительных инвестиции, необходимых в аппаратное обеспечение, программное обеспечение, а также обучение, расширение штата и найм новых сотрудников, чтобы соответствовать принятым нормативным актам, огромен. Столкнувшись с такими проблемами, многие компании инвестировали дополнительные средства в усиление системы внутреннего контроля за финансовыми преступлениями, например, обратились к автоматизации, иными словами к анализу данных, что открывает огромный потенциал для повышения эффективности и результативности мер, направленных на снижение риска финансовых преступлений. В данной статье будут представлены основы методологии анализа цифровых данных с разбором каждого этапа анализа, ее преимуществ, а также ряд инструментов, используемых при анализе данных, включая оценку рисков. В статье предложены возможности для совершенствования анализа данных.

Ключевые слова: анализ данных, большие данные, расследования, мошенничество, аналитика данных, снижение риска, финансовые преступления, комплаенс

Введение

На сегодняшний день многие организации в своей финансово-хозяйственной деятельности сталкиваются с различными мошенническими действиями и финансовыми махинациями со стороны недобросовестных сотрудников, а также иными рисками, связанными с деятельностью организации, которые непосредственно влияют на финансовый результат деятельности организации. В целях оперативного предотвращения мошеннических и противоправных действий в отношении организации становится недостаточно использование исключительно традиционных подходов аудита, так как мошеннические действия зачастую представляют собой детально продуманный механизм действий и мер по его сокрытию.

Общее содержание

Финансово-хозяйственная деятельность любой организации обладает индивидуальными особенностями, такими как организационно-правовая форма, вид деятельности/производимого продукта или услуги, наличие корпоративной культуры и стандартов трудовой этики, что в свою очередь, в условиях несовершенного контроля приводит к увеличению (уменьшению) вероятности возникновения мошеннических действий, нарушению налогового, финансового законодательства и иных нормативных актов при выполнении должностных обязанностей сотрудниками организации и во взаимоотношениях с контрагентами [1]. Следовательно, руководству организации требуется предпринимать дополнительные шаги для выявления фактов мошенничества , а также обнаружения и пресечения финансовых преступлений как со стороны сотрудников, так и со стороны контрагентов. Таким образом, руководству организации наряду с традиционными методами аудита требуется прибегать к дополнительным методам специализированного аудита, финансового контроля и ревизии [2].

Более того, в настоящий момент международные и национальные организации находятся под большим давлением со стороны регуляторных органов для совершенствования своей внутренней программы по борьбе с мошенничеством и коррупцией.

На основании последних принятых нормативных правоприменительных мер и соглашений об урегулировании по всему миру можно отметить особое внимание правительств стран к вопросам противодействия мошенничеству и коррупции. Данное соответствие требованиям продолжает ос-

таваться одним из главных приоритетов для советов директоров, аудиторских комитетов и высшего руководства многих транснациональных корпораций. Один лишь факт наличия программы по борьбе с мошенничеством и противодействию коррупции уже не может считаться достаточным.

Традиционные тесты финансового контроля принципиально отличаются от контроля, необходимого для эффективного выявления и мониторинга мошенничества, взяточничества и коррупции. Чтобы быть успешными, компаниям требуется интегрировать цифровые методы анализа данных, которые включают концепции использования больших данных из нескольких источников данных, списки наблюдения сторонних производителей, транзакционные данные, интеллектуальный анализ текста и даже социальные сети с электронной почтой для определения областей риска или мошеннической деятельности [3].

Внедрение анализа цифровых данных в существующий процесс финансового расследования преступной деятельности позволяет аудитору получать информацию, выходящую за рамки традиционных тестов на основе правил или случайной выборки, которые могут пропустить критичную информацию или создать значительное количество ложных положительных результатов. Например, использование технологий может позволить аудитору определять регионы или подразделения, где возникают повышенные риски на основе нескольких типов данных одновременно. В то же время организации могут сократить общие издержки на внутренний аудит, используя аналитику данных в качестве части процесса оценки риска для проведения предупреждающих мероприятий.

Термин «аналитика данных» определяется как способность сбора и использования данных для получения информации, позволяющей принимать рациональные решения. В контексте управления рисками мошенничества «аналитика данных» может быть конкретизирована до способности сбора и использовании электронной информации как из структурированных, так и неструктурированных источников данных для определения подозрительных платежей, моделей поведения и тенденций. Аналитика цифровых данных включает элементы непрерывного мониторинга, анализа данных в режиме реального времени для предотвращения подозрительных платежей [4]. Примеры аналитики данных могут включать в себя механизмы аналитической обработки данных в реальном времени для принятия быстрых бизнес-решений, таких как остановка потенциально ненадлежащего платежа или бизнес-транзакции, или использование средств контроля за противодействием мошенничеству/коррупции, которые интегрируют визуализацию данных, статистический анализ и интеллектуальный анализ текста. Выходя за рамки традиционных баз данных и электронных таблиц Exel, новые технологии аналитики данных позволяют «идти в ногу» с увеличением объемов цифровых данных, а также бизнесом и нормативным законодательством.

Одним из ключевых моментов анализа данных является ранжирование системы управления рисками. Ранжирование рисков является основным инструментом для сравнения и классификации рисков. Данный подход наиболее целесообразен если выявляются признаки несоответствия между имеющимися ресурсами в организации и затратами на снижение одного или целого ряда рисков, а также если риски обладают различной природой, что существенно затрудняет их оценку единым инструментом [5].

При ранжировании рисков определяются рисковые области, а также их источники, описываются факторы, использующиеся в качестве переменных для количественной оценке риска, а также рассчитывается общая величина риска [6].

К типовым элементам ранжирования рисков относятся (1) выявление факторов хозяйственной деятельности, приводящих к возникновению риска; (2) проведение оценки рисков; (3) отбор рисков.

На первом этапе предоставляется информация от всех бизнес-экспертов о факторах, оказывающих влияние на возникновение рисковых областей, а также иной дополнительной информации, требуемой для последующего анализа рисков. Такого рода анализ, иначе «brainstorm», относится к качественному этапу определения рисковых областей, а также влияющих факторов отдельно для каждого источника при проведении суммарной оценки рисков. Данный первичный анализ позволяет определить множество различных факторов, способствующих появлению рисковых областей, а, следовательно, возникновению рисков. Далее данная информация обрабатывается, обобщается и выделяются факторы в иерархическом виде.

На втором этапе производится оценка риска для каждого отдельно взятого источника риска, выявленного в результате формирования иерархии рисковых областей.

На заключительном этапе производится отбор рисков после проведения оценки каждого риска с помощью значений величины, веса, класса и т.д. На данном этапе производится «взвешивание и отбор» рисков.

На схеме представлена базовая методология проведения аналитики цифровых данных.

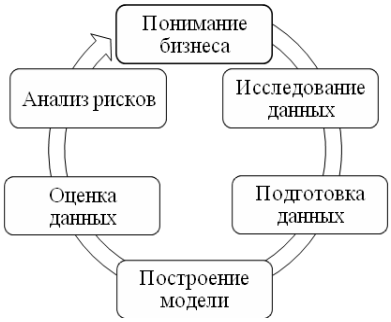

Схема 1. Этапы проведения аналитики данных

Первоначальный этап «Понимание бизнеса» направлен на понимание деятельности организации, основных продуктовых линеек, целей и требований с точки зрения бизнеса с последующим преобразованием этих знаний в определенные индикаторы анализа данных и предварительный план, предназначенный для достижения намеченных целей.

Второй этап «Понимание данных» начинается с первоначального сбора цифровых данных и продолжается с действий, направленных на ознакомление с данными, выявление проблем с качеством данных, обнаружение первых сведений о данных или обнаружение подмножеств для формирования гипотез для скрытой информации.

Третий этап «Подготовка данных» охватывает все действия по построению окончательного набора данных из исходных данных, которые будут поступать в инструменты моделирования.

На четвертом этапе «Построение модели» подбираются и применяются различные методы моделирования, а их параметры уточняются по принятым расчетным оптимальным значениям. Как правило, существует несколько методов для одного типа проблемы анализа данных. Некоторые методы предъявляют особые требования к форме данных. Поэтому часто необходимо вернуться к этапу подготовки данных (третий этап).

На пятом этапе «Оценка данных» строится модель (или модели), которые, предположительно, имеют высокое качество, с точки зрения анализа данных. Прежде чем приступить к окончательному развертыванию модели, важно более тщательно оценить модель и рассмотреть шаги, выполненные для построения модели, чтобы убедиться, что она правильно направлена на достижение бизнес-целей. Ключевая цель состоит в том, чтобы определить, имеется ли какой-либо риск, который не был достаточно рассмотрен. В конце этого этапа должно быть принято решение об использовании результатов анализа данных.

В общем случае такой подход к цифровым данным позволяет осуществлять непрерывный мониторинг, что позволяет снизить риски организации с помощью расширенного и последовательного анализа цифровых данных в дополнение к традиционным методам аудита [4].

На сегодняшний день особое значение принимает фраза: «Данные вокруг нас» – от сложных систем учета до сетевой безопасности и социальных сетей, это так называемая всеохватывающая основа корпоративного мира сегодня. В целях расследования или противодействия мошенничеству, аудитору необходимо понимать порой сложные наборы данных, получаемых из различных источников бизнеса. Ключ к пониманию быстро расширяющейся «границы» состоит в эффективном использовании новых технологий в сочетании с профессиональным опытом.

Понимание больших массивов цифровых данных и их меняющейся парадигмы имеет решающее значение для эффективной реализации в целях безопасности. Кроме того, как инструмент безопасности, он также может быть использован для предотвращения инцидентов мошенничества, поскольку он может выявить потенциальные проблемы безопасности.

Заключение

В целях эффективной борьбы с коррупцией и мошенничеством компании должны изучить более широкий набор рисков, включить большее количество источников данных, использовать лучшие инструменты, перейти к анализу данных в реальном времени или в ближайшее время увеличить объемы данных. Охватывая эти потенциальные области для улучшения, организации будут предоставлять более эффективную и действенную программу по борьбе с мошенничеством и антикоррупционным соответствием, которая в значительной степени сосредоточена на ключевых областях риска мошенничества и улучшенном внутреннем аудите, соответствии или качестве расследования.

Литература

1. Darrell D. Dorrell, Gregory A. Gadawski. Financial Forensics. Hoboken, New Jersey: John Wiley & Sons, 2012. 560 p.

2. Forensic accounting: litigation support.

URL: http://www.forensicaccounting.com (дата обращения: 10.11.2019)

3. Baesens B., Veronique V.V., Verbeke W. Fraud Analytics Using Descriptive, Predictive, and Social Network Techniques: A Guide to Data Science for Fraud Detection (Wiley and SAS Business Series). Wiley, 2015. 400 p.

4. Dutta S.K. Statistical techniques for forensic accounting: understanding the theory and application of data analysis. Upper Saddle River, New Jersey: FT Press, 2016. 400 p.

5. Freeman Sh. How forensic accounting works // Howstuffworks: a division of the research engine In-foSpace.

6. URL: http://science.howorks.com/forensic-accounting.htm (дата обращения: 10.11.2019)

Golden T.W., Skalak S.L., Clayton M.M. A guide to forensic accounting investigation. Hoboken, New Jersey: John Wiley & Sons, 2016. 565 p.

References

1. Darrell D. Dorrell, Gregory A. Gadawski. Financial Forensics. Hoboken, New Jersey: John Wiley & Sons, 2012. 560 p.

2. Forensic accounting: litigation support.

URL: http://www.forensicaccounting.com (data obrashcheniya: 10.11.2019)

3. Baesens B., Veronique V.V., Verbeke W. Fraud Analytics Using Descriptive, Predictive, and Social Network Techniques: A Guide to Data Science for Fraud Detection (Wiley and SAS Business Series). Wiley, 2015. 400 p.

4. Dutta S.K. Statistical techniques for forensic accounting: understanding the theory and application of data analysis. Upper Saddle River, New Jersey: FT Press, 2016. 400 p.

5. Freeman Sh. How forensic accounting works // Howstuffworks: a division of the research engine In-foSpace.

6. URL: http://science.howorks.com/forensic-accounting.htm (data obrashcheniya: 10.11.2019)

Golden T.W., Skalak S.L., Clayton M.M. A guide to forensic accounting investigation. Hoboken, New Jersey: John Wiley & Sons, 2016. 565 p.

METHODS OF ANALYSIS OF BIG DATA FOR FRAUD INVESTIGATION

Sidorenko M.E., Master Student,
Rogulin U.P., Candidate of Economic Sciences (Ph.D.), Associate Professor,
Financial University under the Government of the Russian Federation

Abstract: in the era of big data, companies face the challenge of how effectively they can use data analysis in order to protect their interests, mitigate financial risks and optimize business operations, as well as stipulate business development. Technology is advancing at a rapid pace impacting many industries including accounting and auditing industries. Technological development has enabled implementation of automated accounting systems that make it possible for firms to shift from traditional accounting to automated accounting.

Majority of recent regulations and law enforcement initiatives mainly focus on mitigating financial crime threats, but they also increase the total costs of the company. Additional investments needed in hardware, software, and costs associated with employees to be compliant with regulatory are tremendous. Faced with such challenges, many companies have invested in enhancing their internal controls over financial crime, for instance, turned to automation, so-called data analysis, which offers enormous potential to improve the efficiency and efficacy of financial crime-related operations. The article presents basic methodology of data analysis, its benefits, as well as tools used in data analysis, including risk assessment. The article offers the possibility of improving data analysis.

Keywords: data analysis, big data, investigations, fraud, mitigating, financial crime, compliance