Подход к идентификации новых типов рисков с применением искусственного интеллекта и анализа больших данных

Н.Н. Гоглев, С.А. Мигалин, Е.В. Касаткина

***Аннотация* — Применение в риск-менеджменте технологий искусственного интеллекта и анализа больших данных позволяет снизить нагрузку на экспертов и уменьшить влияния человеческого фактора при оценке рисков. Данные технологии хорошо изучены и активно используются для определения вероятности наступления известных рисков и оценки величины последствий при их наступлении, но при этом остается слабо проработанным вопрос идентификации новых типов рисков. Авторами разработан инновационный подход к идентификации новых типов рисков, основанный на применении методов искусственного интеллекта и анализа больших данных.**

Разработанный подход предполагает идентификацию новых типов риска в три этапа: 1) выявление аномалий в историческом массиве данных; 2) разделение выявленных аномалий на однородные кластеры; 3) профилирование кластеров аномалий как потенциально новых типов рисков, описание характерных признаков выявленных кластеров. Для поиска аномальных наблюдений авторами предлагается использовать технологию ансамблирования статистических методов и методов машинного обучения, таких как метод эллипсоидальной аппроксимации данных, метод локального уровня выбросов и метод изолирующего леса. Для формирования однородных кластеров аномальных наблюдений предлагается использовать один из методов кластерного анализа, выбранный исходя из значений внутренних метрик качества кластеризации. Для профилирования аномальных кластеров как потенциально новых типов рисков используются методы корреляционного и статистического анализа данных. Предложенный подход, в отличие от классических технологий идентификации рисков, позволяет повысить эффективность и качество идентификации. Разработанный подход методологически может встраиваться в стандартные процессы управления рисками и использоваться в различных сферах деятельности для автоматизированного выявления новых типов рисков с целью их последующего анализа и обработки.

***Ключевые слова* — Риск-менеджмент, идентификация рисков, анализ больших данных, искусственный интеллект, машинное обучение, поиск аномалий, кластеризация, профили аномалий.**

Статья получена 19 июля 2022.

Никита Николаевич Гоглев, руководитель направления ООО «ЦИТ», Екатеринбург, РФ (e-mail: Nikita.Goglev@centre-it.com).

Сергей. Алексеевич Мигалин, ведущий системный аналитик ООО «ЦИТ», Екатеринбург, РФ (e-mail: Sergey.Migalin@centre-it.com).

Екатерина Васильевна Касаткина, канд. физ.-мат. наук, доцент, аналитик ООО «ЦИТ», Екатеринбург, РФ (e-mail: Ekaterina.Kasatkina@centre-it.com).

I. Введение

Технологии искусственного интеллекта и анализа больших данных составляют основу цифровой трансформации современного риск-менеджмента [1], [2]. Применение этих технологий открывает новые возможности совершенствования процессов управления рисками за счет снижения нагрузки на экспертов и уменьшения влияния человеческого фактора при оценке рисков, а также за счет повышения качества управленческих решений, опирающихся на рекомендации интеллектуальных систем по обработке рисков.

Сегодня уже достаточно хорошо изучены возможности применения искусственного интеллекта в одной из центральных задач оценки рисков – определении вероятности наступления известных (ранее идентифицированных) рисков, качественной и количественной оценки масштаба вероятных последствий при их наступлении. Обозначенные задачи могут решаться с использованием математических моделей классификации и регрессии, обучаемых на больших массивах исторических данных с зафиксированными фактами наступления рисков и значениями показателей, характеризующих сопутствующий ущерб [3], [4].

Однако предусловием результативного применения таких моделей является идентификация рисков – выявление типов рисков, которые с той или иной вероятностью могут наступить и поэтому должны быть подвергнуты оценке. Существующие технологии идентификации рисков, наиболее распространенными среди которых являются качественные методы FMEA, FTA, ETA, LOPA, HRA и количественные методы (такие как метод мозгового штурма, метод Дельфи, контрольные листы, PHA, HAZOP, HACCP и др.) [5]–[7], опираются преимущественно на методы экспертной оценки, имеют достаточно высокую трудоемкость применения и подвержены упомянутому выше влиянию человеческого фактора. Кроме того, практически в любой сфере деятельности, по отношению к которой применяются инструменты риск-менеджмента, с течением времени под влиянием внутренних и внешних факторов появляются принципиально новые риски. Особенно актуальна данная проблематика сегодня, когда стремительно возрастает скорость внедрения изменений

и повышается уровень неопределенности [8], а для выявления взаимосвязей и закономерностей, образующих в сочетании факторы возникновения новых рисков, необходим глубокий анализ больших объемов информации.

В данной статье формулируется разработанный авторами подход к решению задачи идентификации и выявления новых типов рисков, основанный на применении искусственного интеллекта и анализа больших данных. Для каждого элемента сформулированного подхода в статье предлагаются различные методы и алгоритмы реализации, а также обосновывается целесообразность применения наиболее релевантных из них для решения поставленной задачи. Научная новизна данного подхода заключается в том, что в отличие от существующих известных подходов к идентификации рисков, сформулированный подход позволяет выполнять основные этапы идентификации рисков в автоматическом режиме на основе интеллектуального анализа исторических данных без использования субъективных оценок экспертов, на выходе позволяет получить готовый профиль потенциально нового типа риска и является универсальным, что дает возможность его применения для различных сфер деятельности. В научной литературе и статьях, обзор которых был выполнен в рамках проведенного исследования, информация о существовании аналогичных подходов отсутствует. Поэтому сравнение эффективности сформулированного подхода с аналогами в настоящей статье не приводится.

II. Подход к идентификации новых типов рисков

Предлагаемый инновационный подход к автоматизированной идентификации новых типов рисков укрупненно представлен на Рис. 1 и состоит из трех основных этапов:

1) выявление аномалий в историческом массиве данных;
2) разделение выявленных аномалий на однородные группы (кластеры);
3) профилирование кластеров аномалий как потенциально новых типов рисков, описание характерных признаков выявленных кластеров.

Рис. 1. Подход к идентификации новых типов рисков

Под историческим массивом данных в контексте настоящей статьи понимается совокупность структурированной информации, накапливаемой организацией в ходе ее деятельности. Такая информация содержит качественные и количественные признаки объектов и субъектов, задействованных в процессах организации из области применения риск-менеджмента и являющихся потенциальными источниками рисков.

Применение рассматриваемого подхода предполагает, что исторический массив данных проходит предварительную обработку, в которую входят следующие процедуры:

1) очистка данных (заполнение пропусков в данных и обработка некорректных значений);
2) разработка и расчет производных признаков;
3) кодирование категориальных признаков с использованием различных методов, в том числе таких методов, как «Count Encoder» (кодирование частотным распределением по категориям) и «One Hot Encoder» (кодирование фиктивными переменными);
4) нормализация количественных признаков (в том числе с применением логарифмирования, линейного нормирования, нормализации средним);
5) понижение размерности признакового пространства методом главных компонент (PCA).

Применение процедур предварительной обработки данных позволяет значительно уменьшить вычислительное время и объем требуемых ресурсов для работы алгоритмов подхода за счет сжатия пространства признаков. Результатом предварительной обработки данных является конечный итоговый набор данных для дальнейшего анализа.

III. Выявление аномалий в историческом массиве данных

Задача поиска аномалий в данных (Anomaly Detection) является задачей интеллектуального анализа, в результате решения которой выявляются редкие наблюдения, являющиеся подозрительными, ввиду значимого отличия от стандартных паттернов (шаблонов) поведения [9]. Наличие аномалий в данных может объясняться, в том числе, и проявлением новых (ранее неизвестных) типов рисков. Задача выявления аномалий имеет широкое применение в различных областях, например, таких как финансовая индустрия [10], [11], здравоохранение [12], градостроительство [13], [14], обнаружение неисправностей в технических системах [15], государственное регулирование и выявление фактов нарушения законодательства [16], интеллектуальные транспортные системы [17], обработка потоковых данных [18] и обнаружение сетевых атак [19].

Существует множество методов поиска аномалий, но эффективность методов зависит от набора обучающих данных и используемого вида параметров. Все методы обнаружения аномалий имеют слабые систематические преимущества одного метода перед другими [20]. Таким образом, для формирования оптимального подхода под конкретную прикладную задачу обнаружения аномалий

и проверки устойчивости результатов, полученных разными методами, целесообразно применение подхода, сочетающего в себе различные комбинации известных методов.

Рассмотрим наиболее распространенные методы поиска аномалий.

1) Правило трех сигм (The Three Sigma Rule). Согласно данному методу аномалиями считаются наблюдения, для которых какой-либо количественный признак принимает значение более чем в три раза превышающее стандартное отклонение от среднего уровня в наборе данных [21]. Метод прост в реализации и не требует обучения модели, используется обособленно по каждому количественному признаку, но может быть применим только для нормально распределенных признаков.
2) Эллипсоидальная аппроксимация данных (Elliptic Envelope). Метод преобразует набор данных в N-мерную эллиптическую форму (где N – размерность пространства признаков), тогда типичные наблюдения принадлежат внутренней части эллипсоида, а аномальные – находятся за переделами данного эллипсоида. В параметрах метода можно задать степень загрязнения набора данных (долю аномалий в наборе данных). Метод дает хорошие результаты только на нормально распределенных одномодальных данных [22], [23].
3) Методы кластерного анализа (например, алгоритмы DBSCAN, OPTICS). Аномалиями считаются элементы выборки, значительно удаленные (более чем на заданную величину) от центров кластеров. Данные методы основаны на плотности распределения данных, позволяют находить выбросы вокруг кластеров произвольной формы и поддерживают параллельные вычисления, но имеют высокую вычислительную сложность, качество зависит от выбора метрики расстояния и требует задания обязательных гиперпараметров, которые сильно влияют на результат кластеризации [24]–[27].
4) Метрические методы. Основаны на идеи, что все аномалии являются изолированными от типичных наблюдений выборки [20], [28]. Наиболее распространенный метрический метод – локальный уровень выброса (Local Outlier Factor, LOF). Работа данного метода основана на измерении локального (с учетом k-ближайших соседей) отклонения плотности объекта – степени изолированности объекта по отношению к окружающей среде [29]. Поскольку для аномалий характерно малое число соседей, то наблюдения с высокой степенью изолированности считаются аномалиями. LOF-метод имеет невысокую вычислительную сложность ($O(n \log n)$, где n – кол-во признаков) [19], учитывает различную плотность для каждой группы объектов, может работать с мультимодальными наборами данных и хорошо работает в большинстве реальных задач, часто превосходя другие методы поиска аномалий [29], [30].
5) Метод опорных векторов для одного класса (One Class SVM). Данный метод является одной из форм классического метода опорных векторов [31], но для обучения используется только один класс объектов [32]. Метод предполагает преобразование признакового пространства и проведение гиперплоскости, максимально отделяющей типичные объекты, на которых обучалась модель, от центра координат, тогда аномальными считаются объекты, лежащие со стороны центра координат от найденной гиперплоскости. Построение гиперплоскости сводится к решению задачи квадратичного программирования, имеющей единственное решение, но характеризующейся высокой вычислительной сложностью ($O(N\, n^2)$, где n – количество наблюдений, N – количество признаков). Метод подстраивается под обучающую выборку и поэтому хорошо решает задачу поиска аномалий как новизны, когда для обучения подаются данные без аномалий, и практически не применим в случаях, когда аномалии содержатся непосредственно в обучающей выборке [33].
6) Изолирующий лес (Isolation Forest). Метод представляет собой ансамбль «изолирующих» деревьев для отделения каждого наблюдения от остальных [34]. Основан на том, что путь к аномальным наблюдениям от корневого узла изолирующего дерева имеет меньшую длину, поэтому оценкой аномальности наблюдений служит средняя глубина листьев, в которые попало наблюдение при построении каждого изолирующего дерева. Теоретическая сложность алгоритма эффективнее большинства других алгоритмов ($O(n \log n)$). Аналогично LOF метод может работать с мультимодальными данными. Алгоритм инвариантен к масштабированию признаков, не требует задания метрики или другой априорной информации об устройстве данных. Может находить аномалии различного вида (изолированные наблюдения с низкой локальной плотностью и аномальные наблюдения, входящие в кластеры малых размеров). При наличии мультиколлинеарности в данных наблюдается снижение качества работы алгоритма.
7) Моделирующие методы. Выполняется моделирование на исходном признаковом описании и рассчитываются модельные значения признаков для каждого наблюдения. Наблюдения, у которых исходное признаковое описание сильно отличается от модельного описания, и есть аномалии. Наиболее распространенным моделирующим методом является автоэнкодер, представляющий собой комбинацию двух нейронных сетей: кодирующей («энкодер») и декодирующей («декодер») [35]. На вход подается исходное признаковое описание. Поскольку количество нейронов в скрытых слоях меньше размерности признакового описания, то энкодер обучается сохранять значимую

информацию, характеризующую только типичные наблюдения. Декодер учится отображать информацию из скрытых слоев нейронной сети в модельные значения признаков. За счет сжатия пространства признаков в скрытых слоях автоэнкодер не может воссоздавать исходное признаковое описание аномальных наблюдений и это позволяет идентифицировать выделяющиеся наблюдения. Существует сложность в выборе подходящей структуры нейронной сети для конкретной задачи. Обученные нейронные сети являются практически не трактуемыми моделями наподобие «модели черного ящика», поэтому логическая интерпретация найденных закономерностей представляется невозможной. Автоэнкодеры позволяют успешно решать задачу поиска аномалий как новизны в данных [13], но не дают возможности эффективно решать данную задачу, когда аномалии содержатся в обучающем (историческом) наборе данных, поскольку в этом случае адаптируются под аномалии и перестают работать корректно [36].

Таким образом, наиболее релевантными для задачи поиска аномалий (потенциально характеризующих новые типы рисков) являются:

1) для количественных одномодальных нормально распределенных признаков – правило трех сигм и метод эллипсоидальной аппроксимации;
2) для всех признаков в совокупности – метод локального уровня выброса и метод изолирующего леса.

Недостаток всех рассмотренных методов поиска аномалий заключается в зависимости результатов от входных параметров и структуры данных. Для снижения указанных недостатков целесообразно воспользоваться ансамблированием методов поиска аномалий [37], [38], при котором каждое наблюдение проверяется на аномальность с использованием одновременно нескольких методов и последующим расчетом интегральной метрики аномальности. Эффективность ансамблирования в случае неразмеченных данных (имеется в виду разметка вида «аномалия / норма») на примере поиска аномалий во временных рядах продемонстрирована в работе [39].

Проблема заключается в том, что для различных алгоритмов функция аномальности имеет различные шкалы и масштабы (например, для изолирующего леса – средняя длина пути по дереву, для локального уровня выброса – LOF-оценка), поэтому вариант реализации интегральной метрики аномальности, при котором значения метрик аномальности, полученные различными методами, приводятся к одному диапазону с последующим усреднением, представляется нецелесообразным. Объединение результатов различных методов обнаружения аномалий, основанных на несхожих принципах, лучше выполнить процедурой голосования: результат выделения наблюдения как аномального каждым из используемых методов засчитывается как голос в пользу того, что наблюдение действительно является аномалией. Далее рассчитывается интегральная метрика аномальности – сумма полученных голосов с учетом весовых коэффициентов, характеризующих эффективность соответствующего метода поиска аномалий.

На Рис. 2 представлена схема поиска аномалий с использованием ансамблирования методов.

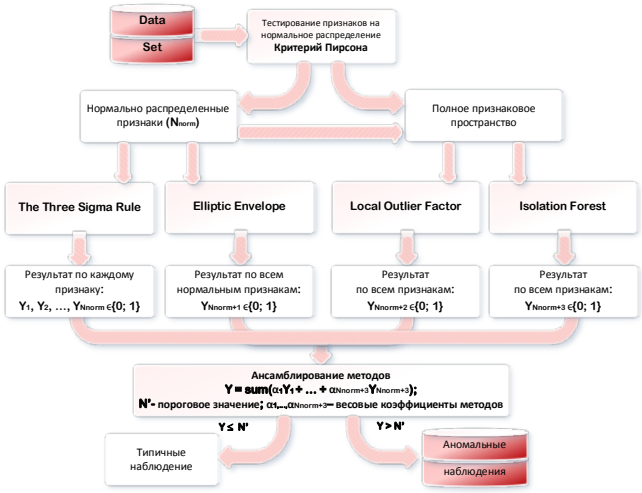

Рис. 2. Поиск аномалий с использованием ансамблирования методов

Результатом применения рассмотренного метода ансамблирования является множество выявленных аномалий, внутри которых далее необходимо выделить однородные группы и выполнить их профилирование.

IV. Разделение выявленных аномалий на однородные группы

Для разделения выявленных аномалий на однородные группы используются методы кластерного анализа. Кластерный анализ реализуется с помощью интеллектуальных алгоритмов машинного обучения без учителя. Можно выделить четыре группы алгоритмов кластеризации:

1) эвристические графовые алгоритмы (алгоритм выделения связных компонент, алгоритм кратчайшего незамкнутого пути, FOREL);
2) статистические алгоритмы (EM-алгоритм, k-means, DBSCAN);
3) иерархические методы (агломеративные и дивизионные методы, метод Варда, Birch);
4) алгоритмы нечеткой кластеризации (FCM, FCS, MM).

Каждая группа методов кластеризации обладает своими преимуществами и недостатками. В частности, графовые алгоритмы достаточно наглядны, но медленны, чувствительны к шумовым выбросам и разреженному фону, образованному нетипичными объектами.

Статистические алгоритмы эффективно работают с большими объемами данных, что не всегда можно отметить для графовых методов кластеризации. EM-алгоритм достаточно эффективен, позволяет определять оптимальное число кластеров, выделять шумовые выбросы и разреженный фон, недостатком является

чувствительность к начальному приближению.

Алгоритм k-средних – упрощенный вариант EM-алгоритма, быстрее сходится, но более чувствителен к выбору начального приближения. Для решения проблемы чувствительности к выбору начального приближения и ускорения конвергенции разработана интеллектуальная надстройка над алгоритмом «k-means++» [40], показывающая хорошие результаты на практике [41], [42].

Алгоритмы иерархической кластеризации, в отличие от графовых и статистических алгоритмов, выявляют детальную кластерную структуру множества объектов в виде таксономического дерева (дендрограммы).

Алгоритмы нечеткой кластеризации имеют недостаток в невозможности корректного разбиения на кластеры в случае наличия большой дисперсии в значениях анализируемых признаков наблюдений.

Важным преимуществом, таким как возможность нахождения кластеров произвольной формы, обладают иерархические методы, метод k-средних. Следует отметить, что для большинства методов кластеризации предварительно требуется принять решение о значениях гиперпараметров алгоритмов [43]. Так, для метода k-средних необходимо знать число кластерных разбиений; для алгоритма DBSCAN нужно подбирать размер окрестности и минимальное число элементов в ней.

Для иерархического алгоритма результат кластеризации сильно зависит от выбора способа расчета расстояний между кластерами. Данные решения исследователь может принять либо опираясь на собственную интуицию, либо проведя предварительный поиск оптимальных значений необходимых гиперпараметров.

Поскольку в задаче разделения аномальных наблюдений на однородные группы нет априорно известного количества кластеров и распределения по кластерам, то для выбора лучшего метода кластерного анализа и настройки его гиперпараметров целесообразно использовать внутренние метрики качества кластеризации, например, такие как:

1) силуэт (Silhouette) [44];
2) индекс Дэвиса-Болдуина [45];
3) индекс Калинского-Харабаша [46].

V. Профилирование кластеров аномалий

Профилирование выявленных аномальных кластеров заключается в определении и описании признаков, по которым выделенные группы (кластеры) аномалий наиболее характерно различаются между собой.

В рамках предлагаемого в настоящей статье подхода профилирование аномальных кластеров выполняется с использованием классических методов анализа данных. Для каждого аномального кластера выполняются следующие шаги:

1) выделение значимых признаков (индикаторов), которые характеризуют выделенные аномальные кластеры, методами корреляционного анализа;
2) расчет перечисленных ниже статистических показателей распределения и граничных значений количественных индикаторов:
   - среднее значение;
   - среднеквадратическое отклонение;
   - первый квартиль (0,25-квантиль;
   - третий квартиль (0,75-квантиль;
   - минимальное значение в кластере;
   - максимальное значение в кластере;
3) расчет частот распределения значимых категориальных индикаторов;
4) формирование профиля потенциально нового типа риска.

Сформированный профиль представляет собой описание соответствующего ему аномального кластера, основанное на значениях статистических показателей, полученных в результате выполнения приведенных выше шагов.

Далее сформированный профиль может быть подвергнут процедурам смысловой интерпретации экспертами и валидации на массивах актуальной информации. В случае положительных результатов валидации соответствующий профилю риск включается в типологию риск-менеджмента предметной области и встраивается в основные процессы анализа (в том числе с использованием упомянутых во введении к статье математических моделей классификации и регрессии) и обработки рисков организации.

VI. Заключение

В настоящей статье сформулирован инновационный подход к идентификации новых типов рисков с применением технологий искусственного интеллекта и анализа больших данных.

В рамках данного подхода предлагается выявлять новые типы рисков на основе интеграции различных методов поиска аномальных наблюдений в историческом массиве данных, разделять выявленные аномалии на однородные кластеры и профилировать аномальные кластеры как потенциально новые типы рисков.

На этапе поиска аномальных наблюдений предлагается использовать ансамблирование статистического подхода (правила 3-х сигм) и методов машинного обучения (метод эллипсоидальной аппроксимация данных, метод локального уровня выбросов и метод изолирующего леса) с помощью процедуры голосования, учитывающей весовые коэффициенты, характеризующие эффективность данных методов. На этапе формирования однородных кластеров аномальных наблюдений предлагается использовать один из рассмотренных в статье алгоритмов кластеризации, при этом конкретный алгоритм и количество групп аномалий (кластеров) подбираются исходя из значений внутренних метрик качества кластеризации. Для профилирования аномальных кластеров как потенциально новых типов рисков предлагается использовать методы корреляционного и статистического анализа данных.

Выявляемые в соответствии с предлагаемым

подходом потенциально новые типы рисков подлежат последующей валидации на актуальных данных и включению в типологию риск-менеджмента предметной области, а также анализу и обработке в рамках основных процессов управления рисками организации.

Таким образом, разработанный подход позволяет автоматизировано выявлять потенциально новые типы рисков на основе накапливаемой организацией исторической информации о процессах из области применения риск-менеджмента, а также о задействованных в этих процессах объектах и субъектах. Предложенный подход повышает эффективность и качество идентификации новых типов рисков в отличие от классических технологий за счет автоматизации соответствующих задач, методологически может быть встроен в стандартные процессы управления рисками и может быть использован в различных сферах деятельности для автоматизированного выявления новых типов рисков с целью их последующего анализа и обработки.

Библиография

[1] *Committee of Sponsoring Organizations of the Treadway Commision*. Enterprise Risk Management. Integrating with Strategy and Performance. Available: https://www.coso.org/documents/2017-coso-erm-integrating-with-strategy-and-performance-executive-summary.pdf.

[2] Artificial Intelligence (AI) Applied to Risk Management. Available: https://www.ferma.eu/publication/artificial-intelligence-ai-applied-to-risk-management.

[3] Aziz S., Dowling M. *Machine Learning and AI for Risk Management* // SSRN Electronic Journal. DOI: 10.2139/ssrn.3201337.

[4] Svistunova S. A., Muzalev S. V. *Usage of Machine Learning in The Process of Risk-Management* // Russian Journal of Management – 2021. – No 3. – P. 126–130, 2021. DOI: 10.29039/2409-6024-2021-9-3-126-130.

[5] IEC 31010:2019 «Risk management – Risk assessment techniques»

[6] ГОСТ Р 58771-2019. Национальный стандарт Российской Федерации. Менеджмент риска. Технологии оценки риска.

[7] Дебердиева Н.П., Воронин А.В. *Идентификация рисков промышленных предприятий в концепции риск-менеджмента* // Экономика, предпринимательство и право. – 2020. – Т. 10. – № 5. – С. 1425–1438. DOI: 10.18334/epp.10.5.100952.

[8] Шаталова О. М. *О методологических подходах к решению проблемы неопределенности в управлении технологическими инновациями на предприятии* // Вестник ИжГТУ имени М. Т. Калашникова. – 2018 – Т. 21. – № 3. – С. 120-126. DOI 10.22213/2413-1172-2018-3-120-126.

[9] Zimek A., Schubert E. *Outlier Detection* // Encyclopedia of Database Systems. Springer New York – 2017. DOI: 10.1007/978-1-4899-7993-3_80719-1.

[10] Beketnova Yu.M. C*omparative Analysis of Machine learning Methods to Identify signs of suspicious Transactions of Credit Institutions and Their Clients*. Finance: Theory and Practice. – 2021. No. 25(5). – P. 186–199. DOI: 10.26794/2587-5671-2020-25-5-186-199.

[11] Laimek R., Kaothanthong N., Supnithi T. *ATM Fraud Detection Using Outlier Detection*. // Intelligent Data Engineering and Automated Learning – IDEAL 2018. Lecture Notes in Computer Science. – Vol. 11314. Springer, Cham. DOI: 10.1007/978-3-030-03493-1_56.

[12] Ray S., Wright A. *Detecting anomalies in alert firing within clinical decision support systems using Anomaly / Outlier Detection Techniques //* Proc. 7th ACM Int. conf. on bioinformatics, computational biology, and health informatics. New York: Association for Computing Machinery. – 2016. – P. 185–190. DOI: 10.1145/2975167.2975186.

[13] Chesnokov A., Mikhailov V., Dolmatov I. *Detection of Structural Deterioration in Hybrid Constructions* // 3rd International Conference on Control Systems, Mathematical Modeling, Automation and Energy Efficiency (SUMMA). – 2021. – P. 479–484. DOI: 10.1109/SUMMA53307.2021.9632014.

[14] Hung D.V., Hung H.M., Anh P.H., Thang N.T. *Structural damage detection using hybrid deep learning algorithm* // Journal of Science and Technology in Civil Engineering (STCE) – HUCE. – 2020. – No. 14(2). – P. 53–64. DOI: 10.31814/stce.nuce2020-14(2)-05.

[15] Alos A., Dahrouj Z. *Detecting Contextual Faults in Unmanned Aerial Vehicles Using Dynamic Linear Regression and K-Nearest Neighbour Classifier* // Gyroscopy and Navigation. – 2020. – No. 28(1). – P. 66–80. DOI: 10.17285/0869-7035.0024.

[16] Maia P., Meira W. Jr., Barbosa B., Cruz G. M*ulticriteria Anomaly Detection in Government Purchases.* In: Anais do VII Symposium on Knowledge Discovery, Mining and Learning, Fortaleza. – 2019. – P. 97–104. DOI: https://doi.org/10.5753/kdmile.2019.8794.

[17] Kaytaz U., Sivrikaya F., Albayrak S. *Competitive Learning for Unsupervised Anomaly Detection in Intelligent Transportation Systems* // Conference: IEEE International Conference on Communications, to be published.

[18] Рзаев Б.Т., Лебедев И.С. *Применение бэггинга при поиске аномалий сетевого трафика* // Научно-технический вестник информационных технологий, механики и оптики. – 2021. – Т. 21. № 2. – С. 234–240.

[19] Alshawabkeh M., Jang B., Kaeli D. *Accelerating the local outlier factor algorithm on a GPU for intrusion detection systems* // Conference: Proceedings of 3rd Workshop on General Purpose Processing on Graphics Processing Units, GPGPU. Pittsburgh, Pennsylvania, USA. – 2010. DOI: 10.1145/1735688.1735707.

[20] Campos G.O., Zimek A., Sander J., Campello R., Micenkova B., Schubert E., Assent I., Houle M.E. *On the evaluation of unsupervised outlier detection: measures, datasets, and an empirical study* // Data Mining and Knowledge Discovery. – 2016. – Vol. 30, No. 4. DOI: 10.1007/s10618-015-0444-8.

[21] Pukelsheim F. *The Three Sigma Rule* // The American Statistician. – 1994. – No. 48(2). – P. 88–91. DOI: 10.2307/2684253

[22] Rousseeuw P.J., Driessen V.K. *A fast algorithm for the minimum covariance determinant estimator* // Technometrics. – 1999. – Vol. 41(3). – P. 212–223.

[23] Дьяконов А.Г., Головина А.М. *Выявление аномалий в работе механизмов методами машинного обучения* // Сборник научных трудов XIX Международной конференции DAMDID: Аналитика и управление данными в областях с интенсивным использованием данных. – 2017. – С. 469–476.

[24] Ester M., Kriegel H.-P., Sander J., Xu X. *A density-based algorithm for discovering clusters in large spatial databases with noise* // Proceedings of the Second International Conference on Knowledge Discovery and Data Mining (KDD-96) / Evangelos Simoudis, Jiawei Han, Usama M. Fayyad. – AAAI Press. – 1996. – P. 226–231.

[25] Schubert E., Sander J., Ester M., Kriegel H. P., Xu X. *DBSCAN revisited, revisited: why and how you should (still) use DBSCAN.* // ACM Transactions on Database Systems. – 2017. – Vol. 42(3), No. 19.

[26] Kriegel H.-P., Kröger P., Sander J., Zimek A. *Density-based clustering* // Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery. – 2011. Vol. 1, No. 3. – P. 231–240. DOI: 10.1002/widm.30.

[27] Breunig M.M., Kriegel H.-P., Ng R.T., *Sander J.R. OPTICS-OF: Identifying Local Outliers* // Principles of Data Mining and Knowledge Discovery. – 1999. Vol. 1704. DOI: 10.1007/978-3-540-48247-5_28.

[28] Knorr E.M., Ng R.T., Tucakov V. *Distance-based outliers: algorithms and applications* // The VLDB Journal – The International Journal on Very Large Data Bases. – 2000. Vol. 8, No. 3-4. – P. 237–253.

[29] Breunig M. M., Kriegel H.-P., Ng R.T., Sander J. *LOF: Identifying Density-based Local Outliers*. Proceedings of the 2000 ACM SIGMOD International Conference on Management of Data. – 2000. – P. 93–104. DOI: 10.1145/335191.335388.

[30] Lazarevic A., Ozgur A., Ertoz L., Srivastava J., Kumar V. *A comparative study of anomaly detection schemes in network intrusion* detection // Proc. 3rd SIAM International Conference on Data Mining. – 2003.

[31] Vapnik V.N. *The Support Vector method* // Artificial Neural Networks – ICANN'97. LNCS. Springer, Berlin, Heidelberg. – 1997. – Vol. 1327. DOI: 10.1007/BFb0020166.

[32] Schölkopf B., Platt J. C., Shawe-Taylor J., Smola A. J., Williamson R. C. *Estimating the Support of a High-Dimensional Distribution* //

Neural Computation. Bernhard. – 2001. – Vol. 13, No. 7. – P. 1443–1471. DOI: 10.1162/089976601750264965.

[33] Schölkopf B, Williamson RC, Smola A, Shawe-Taylor J, Platt J. *Support vector method for novelty detection* // Advances in neural information processing system. – 1999. – No. 12. – P. 582–588.

[34] Liu F.T., Ting K.M., Zhou Z.-H. *Isolation forest* // In Data Mining. ICDM'08. Eighth IEEE International Conference on. – 2008. – P. 413-422. DOI: 10.1109/ICDM.2008.17.

[35] Cheng-Yuan Liou, Wei-Chen Cheng, Jiun-Wei Liou, Daw-Ran Liou *Autoencoder for words* // Neurocomputing. – 2014. – Vol. 139. – P. 84-96.

[36] Zhisheng X., Qing Y., Yali A. *Likelihood Regret: An Out-of-Distribution Detection Score For Variational Auto-encoder* // Advances in Neural Information Processing Systems. – 2020.

[37] Aggarwal C.C., Sathe S. *Outlier Ensembles*: An Introduction. – Springer, 2017. – 276 p.

[38] Benkabou SE., Benabdeslem K., Canitia B. *Unsupervised outlier detection for time series by entropy and dynamic time warping //* Knowl Inf Syst. – 2018. – Vol. 54. – P. 463-486. DOI: 10.1007/s10115-017-1067-8

[39] Чесноков М.Ю. *Поиск аномалий во временных рядах на основе ансамблей алгоритмов DBSCAN* // Искусственный интеллект и принятие решений. – 2018. – № 1. – С. 99–107.

[40] Arthur D., Vassilvitskii S. *K-Means++: The Advantages of Careful Seeding* // Conference: Proceedings of the Eighteenth Annual ACM-SIAM Symposium on Discrete Algorithms, New Orleans, USA. – 2007. DOI: 10.1145/1283383.1283494.

[41] Шаталова О.М., Касаткина Е.В., Лившиц В.Н. *Кластерный анализ и классификация промышленно ориентированных регионов РФ по экономической специализации* // Экономика и математические методы. – 2022. – Т. 58, № 1. – С. 81–92.

[42] Ketova K.V., Kasatkina E.V., Vavilova D D. *Clustering Russian Federation regions according to the level of socio-economic development with the use of machine learning methods* // Economic and Social Changes: Facts, Trends, Forecast. – 2021. Vol. 14, No. 6. – P. 70–85. DOI: 10.15838/esc.2021.6.78.4

[43] Шалымов Д. С. *Алгоритмы устойчивой кластеризации на основе индексных функций и функций устойчивости* // Стохастическая оптимизация в информатике. СПб.: Изд-во С.-Петербургского университета. – 2008. № 4. – С. 236-248.

[44] Rousseeuw P.J. *Silhouettes: a Graphical Aid to the Interpretation and Validation of Cluster Analysis* // Computational and Applied Mathematics. – 1987. – No. 20, P. 53–65. DOI: 10.1016/0377-0427(87)90125-7.

[45] Davies D.L., Bouldin D.W. *A Cluster Separation Measure* // IEEE Transactions on Pattern Analysis and Machine Intelligence. – 1979. – P. 224–227. DOI:10.1109/TPAMI.1979.4766909.

[46] Calinski T., Harabasz J. *A dendrite method for cluster analysis* // Communications in Statistics. – 1974. – Vol. 3. – P. 1-27. DOI: 10.1080/03610927408827101.

Risk identification approach using artificial intelligence and big data analysis

N.N. Goglev, S.A. Migalin, E.V. Kasatkina

Abstract — **The use of artificial intelligence technologies and big data analysis in risk management makes it possible to reduce the burden on experts and reduce the influence of the human factor in risk assessment. These technologies are well studied and actively used to determine the probability of known risks and assess the magnitude of the consequences when they occur, but the approach to identifying new types of risks remains poorly developed. The authors have developed an innovative approach to identifying new types of risks based on the use of artificial intelligence methods and big data analysis.**

The developed approach involves the identification of new types of risk in three stages: 1) identification of anomalies in the historical data array; 2) division of the identified anomalies into homogeneous clusters; 3) profiling of clusters of anomalies as potentially new types of risks, description of the characteristic features of the identified clusters. To search for anomalous observations, the authors propose to use the technology of ensembling statistical methods and machine learning methods, such as the ellipsoidal data approximation method, the local outlier level method, and the isolation forest method. To form homogeneous clusters of anomalous observations, it is proposed to use one of the cluster analysis methods selected based on the values of internal clustering quality metrics. Correlation and statistical data analysis methods are used to profile anomalous clusters as potentially new types of risks. The proposed approach, in contrast to classical risk identification technologies, makes it possible to increase the efficiency and quality of identification. The developed approach can methodologically be integrated into standard risk management processes and used in various fields of activity for automated identification of new types of risks for the purpose of their subsequent analysis and processing.

***Keywords — Risk management, risk identification, big data analysis, artificial intelligence, machine learning, anomaly detection, clustering, anomaly profile*s**

References

[1] Committee of Sponsoring Organizations of the Treadway Commision. Enterprise Risk Management. Integrating with Strategy and Performance. Available: https://www.coso.org/documents/2017-coso-erm-integrating-with-strategy-and-performance-executive-summary.pdf.

[2] Artificial Intelligence (AI) Applied to Risk Management. Available: https://www.ferma.eu/publication/artificial-intelligence-ai-applied-to-risk-management.

[3] Aziz S., Dowling M. Machine Learning and AI for Risk Management // SSRN Electronic Journal. DOI: 10.2139/ssrn.3201337.

[4] Svistunova S. A., Muzalev S. V. Usage of Machine Learning in The Process of Risk-Management // Russian Journal of Management – 2021. – No 3. – P. 126–130, 2021. DOI: 10.29039/2409-6024-2021-9-3-126-130.

[5] IEC 31010:2019 «Risk management – Risk assessment techniques»

[6] GOST R 58771-2019. Nacional'nyj standart Rossijskoj Federacii. Menedzhment riska. Tehnologii ocenki riska.

[7] Deberdieva N.P., Voronin A.V. Identifikacija riskov promyshlennyh predprijatij v koncepcii risk-menedzhmenta // Jekonomika, predprinimatel'stvo i pravo. – 2020. – T. 10. – # 5. – S. 1425–1438. DOI: 10.18334/epp.10.5.100952.

[8] Shatalova O. M. O metodologicheskih podhodah k resheniju problemy neopredelennosti v upravlenii tehnologicheskimi innovacijami na predprijatii // Vestnik IzhGTU imeni M. T. Kalashnikova. – 2018 – T. 21. – # 3. – S. 120-126. DOI 10.22213/2413-1172-2018-3-120-126.

[9] Zimek A., Schubert E. Outlier Detection // Encyclopedia of Database Systems. Springer New York – 2017. DOI: 10.1007/978-1-4899-7993-3_80719-1.

[10] Beketnova Yu.M. Comparative Analysis of Machine learning Methods to Identify signs of suspicious Transactions of Credit Institutions and Their Clients. Finance: Theory and Practice. – 2021. No. 25(5). – P. 186–199. DOI: 10.26794/2587-5671-2020-25-5-186-199.

[11] Laimek R., Kaothanthong N., Supnithi T. ATM Fraud Detection Using Outlier Detection. // Intelligent Data Engineering and Automated Learning – IDEAL 2018. Lecture Notes in Computer Science. – Vol. 11314. Springer, Cham. DOI: 10.1007/978-3-030-03493-1_56.

[12] Ray S., Wright A. Detecting anomalies in alert firing within clinical decision support systems using Anomaly / Outlier Detection Techniques // Proc. 7th ACM Int. conf. on bioinformatics, computational biology, and health informatics. New York: Association for Computing Machinery. – 2016. – P. 185–190. DOI: 10.1145/2975167.2975186.

[13] Chesnokov A., Mikhailov V., Dolmatov I. Detection of Structural Deterioration in Hybrid Constructions // 3rd International Conference on Control Systems, Mathematical Modeling, Automation and Energy Efficiency (SUMMA). – 2021. – P. 479–484. DOI: 10.1109/SUMMA53307.2021.9632014.

[14] Hung D.V., Hung H.M., Anh P.H., Thang N.T. Structural damage detection using hybrid deep learning algorithm // Journal of Science and Technology in Civil Engineering (STCE) – HUCE. – 2020. – No. 14(2). – P. 53–64. DOI: 10.31814/stce.nuce2020-14(2)-05.

[15] Alos A., Dahrouj Z. Detecting Contextual Faults in Unmanned Aerial Vehicles Using Dynamic Linear Regression and K-Nearest Neighbour Classifier // Gyroscopy and Navigation. – 2020. – No. 28(1). – P. 66–80. DOI: 10.17285/0869-7035.0024.

[16] Maia P., Meira W. Jr., Barbosa B., Cruz G. Multicriteria Anomaly Detection in Government Purchases. In: Anais do VII Symposium on Knowledge Discovery, Mining and Learning, Fortaleza. – 2019. – P. 97–104. DOI: https://doi.org/10.5753/kdmile.2019.8794.

[17] Kaytaz U., Sivrikaya F., Albayrak S. Competitive Learning for Unsupervised Anomaly Detection in Intelligent Transportation Systems // Conference: IEEE International Conference on Communications, to be published.

[18] Rzaev B.T., Lebedev I.S. Primenenie bjegginga pri poiske anomalij setevogo trafika // Nauchno-tehnicheskij vestnik informacionnyh tehnologij, mehaniki i optiki. – 2021. – T. 21. # 2. – S. 234–240.

[19] Alshawabkeh M., Jang B., Kaeli D. Accelerating the local outlier factor algorithm on a GPU for intrusion detection systems // Conference: Proceedings of 3rd Workshop on General Purpose Processing on Graphics Processing Units, GPGPU. Pittsburgh, Pennsylvania, USA. – 2010. DOI: 10.1145/1735688.1735707.

[20] Campos G.O., Zimek A., Sander J., Campello R., Micenkova B., Schubert E., Assent I., Houle M.E. On the evaluation of unsupervised outlier detection: measures, datasets, and an empirical study // Data Mining and Knowledge Discovery. – 2016. – Vol. 30, No. 4. DOI: 10.1007/s10618-015-0444-8.

[21] Pukelsheim F. The Three Sigma Rule // The American Statistician. – 1994. – No. 48(2). – P. 88–91. DOI: 10.2307/2684253

[22] Rousseeuw P.J., Driessen V.K. A fast algorithm for the minimum covariance determinant estimator // Technometrics. – 1999. – Vol. 41(3). – P. 212–223.

[23] D'jakonov A.G., Golovina A.M. Vyjavlenie anomalij v rabote mehanizmov metodami mashinnogo obuchenija // Sbornik nauchnyh trudov XIX Mezhdunarodnoj konferencii DAMDID: Analitika i upravlenie dannymi v oblastjah s intensivnym ispol'zovaniem dannyh. – 2017. – S. 469–476.

[24] Ester M., Kriegel H.-P., Sander J., Xu X. A density-based algorithm for discovering clusters in large spatial databases with noise // Proceedings of the Second International Conference on Knowledge Discovery and Data Mining (KDD-96) / Evangelos Simoudis, Jiawei Han, Usama M. Fayyad. – AAAI Press. – 1996. – P. 226–231.

[25] Schubert E., Sander J., Ester M., Kriegel H. P., Xu X. DBSCAN revisited, revisited: why and how you should (still) use DBSCAN. // ACM Transactions on Database Systems. – 2017. – Vol. 42(3), No. 19.

[26] Kriegel H.-P., Kröger P., Sander J., Zimek A. Density-based clustering // Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery. – 2011. Vol. 1, No. 3. – P. 231–240. DOI: 10.1002/widm.30.

[27] Breunig M.M., Kriegel H.-P., Ng R.T., Sander J.R. OPTICS-OF: Identifying Local Outliers // Principles of Data Mining and Knowledge Discovery. – 1999. Vol. 1704. DOI: 10.1007/978-3-540-48247-5_28.

[28] Knorr E.M., Ng R.T., Tucakov V. Distance-based outliers: algorithms and applications // The VLDB Journal – The International Journal on Very Large Data Bases. – 2000. Vol. 8, No. 3-4. – P. 237–253.

[29] Breunig M. M., Kriegel H.-P., Ng R.T., Sander J. LOF: Identifying Density-based Local Outliers. Proceedings of the 2000 ACM SIGMOD International Conference on Management of Data. – 2000. – P. 93–104. DOI: 10.1145/335191.335388.

[30] Lazarevic A., Ozgur A., Ertoz L., Srivastava J., Kumar V. A comparative study of anomaly detection schemes in network intrusion detection // Proc. 3rd SIAM International Conference on Data Mining. – 2003.

[31] Vapnik V.N. The Support Vector method // Artificial Neural Networks – ICANN'97. LNCS. Springer, Berlin, Heidelberg. – 1997. – Vol. 1327. DOI: 10.1007/BFb0020166.

[32] Schölkopf B., Platt J. C., Shawe-Taylor J., Smola A. J., Williamson R. C. Estimating the Support of a High-Dimensional Distribution // Neural Computation. Bernhard. – 2001. – Vol. 13, No. 7. – P. 1443–1471. DOI: 10.1162/089976601750264965.

[33] Schölkopf B, Williamson RC, Smola A, Shawe-Taylor J, Platt J. Support vector method for novelty detection // Advances in neural information processing system. – 1999. – No. 12. – P. 582–588.

[34] Liu F.T., Ting K.M., Zhou Z.-H. Isolation forest // In Data Mining. ICDM'08. Eighth IEEE International Conference on. – 2008. – P. 413-422. DOI: 10.1109/ICDM.2008.17.

[35] Cheng-Yuan Liou, Wei-Chen Cheng, Jiun-Wei Liou, Daw-Ran Liou Autoencoder for words // Neurocomputing. – 2014. – Vol. 139. – P. 84-96.

[36] Zhisheng X., Qing Y., Yali A. Likelihood Regret: An Out-of-Distribution Detection Score For Variational Auto-encoder // Advances in Neural Information Processing Systems. – 2020.

[37] Aggarwal C.C., Sathe S. Outlier Ensembles: An Introduction. – Springer, 2017. – 276 r.

[38] Benkabou SE., Benabdeslem K., Canitia B. Unsupervised outlier detection for time series by entropy and dynamic time warping // Knowl Inf Syst. – 2018. – Vol. 54. – P. 463-486. DOI: 10.1007/s10115-017-1067-8

[39] Chesnokov M.Ju. Poisk anomalij vo vremennyh rjadah na osnove ansamblej algoritmov DBSCAN // Iskusstvennyj intellekt i prinjatie reshenij. – 2018. – # 1. – S. 99–107.

[40] Arthur D., Vassilvitskii S. K-Means++: The Advantages of Careful Seeding // Conference: Proceedings of the Eighteenth Annual ACM-SIAM Symposium on Discrete Algorithms, New Orleans, USA. – 2007. DOI: 10.1145/1283383.1283494.

[41] Shatalova O.M., Kasatkina E.V., Livshic V.N. Klasternyj analiz i klassifikacija promyshlenno orientirovannyh regionov RF po jekonomicheskoj specializacii // Jekonomika i matematicheskie metody. – 2022. – T. 58, # 1. – S. 81–92.

[42] Ketova K.V., Kasatkina E.V., Vavilova D D. Clustering Russian Federation regions according to the level of socio-economic development with the use of machine learning methods // Economic and Social Changes: Facts, Trends, Forecast. – 2021. Vol. 14, No. 6. – P. 70–85. DOI: 10.15838/esc.2021.6.78.4

[43] Shalymov D. S. Algoritmy ustojchivoj klasterizacii na osnove indeksnyh funkcij i funkcij ustojchivosti // Stohasticheskaja optimizacija v informatike. SPb.: Izd-vo S.-Peterburgskogo universiteta. – 2008. # 4. – S. 236-248.

[44] Rousseeuw P.J. Silhouettes: a Graphical Aid to the Interpretation and Validation of Cluster Analysis // Computational and Applied Mathematics. – 1987. – No. 20, P. 53–65. DOI: 10.1016/0377-0427(87)90125-7.

[45] Davies D.L., Bouldin D.W. A Cluster Separation Measure // IEEE Transactions on Pattern Analysis and Machine Intelligence. – 1979. – P. 224–227. DOI:10.1109/TPAMI.1979.4766909.

[46] Calinski T., Harabasz J. A dendrite method for cluster analysis // Communications in Statistics. – 1974. – Vol. 3. – P. 1-27. DOI: 10.1080/0361092.