DOI 10.37882/2223–2966.2021.03.14

МЕТОДЫ АНАЛИЗА И ПРЕДОТВРАЩЕНИЯ FRAUD-ОПЕРАЦИЙ В СИСТЕМАХ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ

METHODS OF ANALYSIS AND PREVENTION OF FRAUD OPERATIONS IN REMOTE BANKING SYSTEMS

V. Zinovev
O. Romashkova

Summary. The article is devoted to the study of methods of modeling and building analytical software systems to prevent FRAUD operations when conducting transactions in remote banking services. The analysis of information security requirements in Antifraud systems is performed. The architecture of the Antifraud system is described and an algorithm for its construction is developed. An innovative conceptual model of the Antifraud system concept has been developed.

Keywords: anti-fraud systems, remote banking services, banking systems, protection of bank transactions.

Зиновьев Владимир Иванович
Аспирант, ГАОУ ВО «Московский городской педагогический университет (МГПУ)» г. Москва
legrang@yandex.ru
Ромашкова Оксана Николаевна
Д.т.н., профессор, ГАОУ ВО «Московский городской педагогический университет (МГПУ)», г. Москва
ox-rom@yandex.ru

Аннотация. Статья посвящена исследованию методов моделирования и построения аналитических программных систем для предотвращения FRAUD-операций при проведении транзакций при дистанционном банковском обслуживании. Выполнен анализ требований защиты информации в Antifraud-системах. Представлено описание архитектуры Antifraud-системы и разработан алгоритм ее построения. Разработана инновационная концептуальная модель концепта Antifraud-системы.

Ключевые слова: антифрод-системы, дистанционное банковское обслуживание, банковские системы, защита банковских транзакций.

Введение

Стремительный рост количества банковских онлайн транзакций с каждым днем вызывает соответствующее увеличение количества мошенничества в области онлайн платежей и переводов (далее — fraud). Только за 2019 год на территории России кредитные организации в рамках борьбы с онлайн мошенничеством, по приблизительным подсчетам аналитических сводок, предотвратили хищение банковских средств со счетов граждан в размере более 48 миллиардов рублей. При этом, в результате fraud, с банковских счетов было выведено почти 6,5 миллиардов рублей (по выкладкам отчетов ФинЦЕРТ ЦБ РФ). В рамках статистики, усредненная сумма успешных fraud-транзакций составляла 10 тысяч рублей [1]. Это позволяет рассчитать приблизительное количество fraud операций, в которые входят как успешные (далее successful), так и предотвращенные (далее failed), а также рассчитать процентное соотношение successful fraud-транзакций (1).

$$\sum Fr = \frac{54{,}5\ \text{млрд.}}{10\ \text{тыс.}} = 5{,}45\ \text{млн} \quad (1)$$

где, $\sum Fr = Fs + Ff$ — сумма всех successful (Fs) и failed (Ff) транзакций.

Рассчитаем количество successful проведенных fraud-транзакций в количественном выражении (2).

$$\sum Fs = \frac{6{,}5\ \text{млрд.}}{10\ \text{тыс.}} = 650\ \text{тыс.} \quad (2)$$

А также к процентному соотношению (3).

$$Fs = \frac{650\ \text{тыс.} \times 100\%}{5{,}45\ \text{млн}} \approx 11{,}93\% \quad (3)$$

Таким образом, количество successful fraud-транзакций в процентном соотношении равно 11,93%.

В количественном выражении каждая восьмая fraud операция заканчивается потерей денег владельцами банковских счетов (4).

$$Fs = \frac{5{,}45\ \text{млн}}{650\ \text{тыс.}} \approx 8{,}4 \quad (4)$$

Как мы видим, самые элементарные расчеты показывают довольно низкий процент надежности Antifraud систем. Реальное же положение дел представляется несколько иным (в худшую сторону). Это связано с тем, что большинство кредитных организаций или не раскрывают статистику, или намеренно ее занижают, так как это чревато репутационными рисками, что в свою очередь снижает финансовую прибыль, из-за негативного отношения инвесторов, партнеров и клиентов.

1. Требования к стандартам безопасности Antifraud-системы ДБО «IntelSola»

Согласно стандарту безопасности PCI DSS (Payment Card Industry Data Security

Standard), логика разрабатываемой Antifraud-системы ДБО «IntelSola» соответствует основным группам критериев: защите безопасности сети и config-components модулей; построению многоуровневой защиты и шифрованию хранимых и передаваемых данных, а также настройке управления доступом к Cardholders; antivirus protection, сопровождению, физической защите, и контролю защищенности IT инфраструктуры; построению методов шифрования и защиты алгоритмов аутентификации; организации логирования внутренних процессов и сетевой активности; разработке системы управления безопасностью [2, 3].

Согласно протоколам стандарта PCI-DSS, система не хранит на своей стороне критичные аутентификационные данные (КАД): TRACK, CVV2, PIN, PIN-block карты (кроме исключения, когда производится хранение номера карты PAN (Primary Account Number) в зашифрованном виде эмитентом, для авторизации транзакции). Это означает, что в случае, если в antifraud-системе данные КАД были записаны в базу данных (БД), срабатывает сервисный job, который получая максимальный приоритет в очереди операций, удаляет все данные.

2. Архитектура Antifraud-системы ДБО «IntelSola»

Ярко выраженная модульно-компонентная структура разрабатываемой Antifraud-системы предполагает большое количество архитектурных паттернов. Это приводит к необходимости организации структуры системы, в виде гетерогенной микросервисной архитектуры, в основе которой лежит сервис-ориентированный подход (service-oriented architecture, SOA), с использованием компонентных элементов, а также различных технологий. Это позволяет: организовать максимальную автономность структурных компонентов; облегчить масштабируемость и развертываемость системы; неограниченное количество раз пере использовать методы разработанных сервисов в различных модулях и подсистемах; использовать различные технологии (несовместимые при интеграции в монолитной архитектуре). Помимо этого, формируется максимальная гибкость и устойчивость к сбоям, а также возможность изолированной отладки и рефакторингу.

При разработке системы используются несколько типов компонентов: сервисы, как микроприложения, функционирующие в собственных процессных компонентах, и масштабируемые изолированно; библиотеки, как компонентные конструкты в изолированных подсистемах. Каждый из компонентов формируется в виде отдельного микросервиса, изолированного от остальных, обладающего собственной структурой хранения данных (далее DB — Data Bases), и доступного для CRUD операций исключительно посредством интерфейсных компонентов.

В результате деления структур микросервисов на обособленные DB, формирование консистентности данных (далее consistency) строится на профильных сервисных службах, которые инициируют срабатывание процедур проверки данных по граничным триггерам типов after/before. Если триггеры не срабатывают, или отрабатывают с ошибкой, то транзакция отменяется.

Формирование frontend/backend связей на уровне пользовательского интерфейса (далее UI — user interface), предполагает отсутствие декомпозиции UI для дальнейшего взаимодействия с протоколами http и https. Так как отправка запросов в микросервисной архитектуре сопряжена со сложностями построения очереди, то для решения возможных коллизий возникновения таймаутов, http/https запросы формируются в виде небольших асинхронных пакетов [4].

3. Анализ построения Antifraud-системы ДБО «IntelSola»

Методы обнаружения подозрительной активности, а также предотвращения как потенциальных fraud-активностей, так и уже совершающихся FRAUD-транзакций, являются бесконечным циклом операций, содержащих огромное количество процессов и потоков процессов, необходимых для: мониторинга активностей; обнаружения на основании мониторинговых сигналов подозрительных активностей; принятия решения на основании корневых концептов (баз правил, инцидентов; алгоритмов; инструментария); интеллектуального обучения [5, 6].

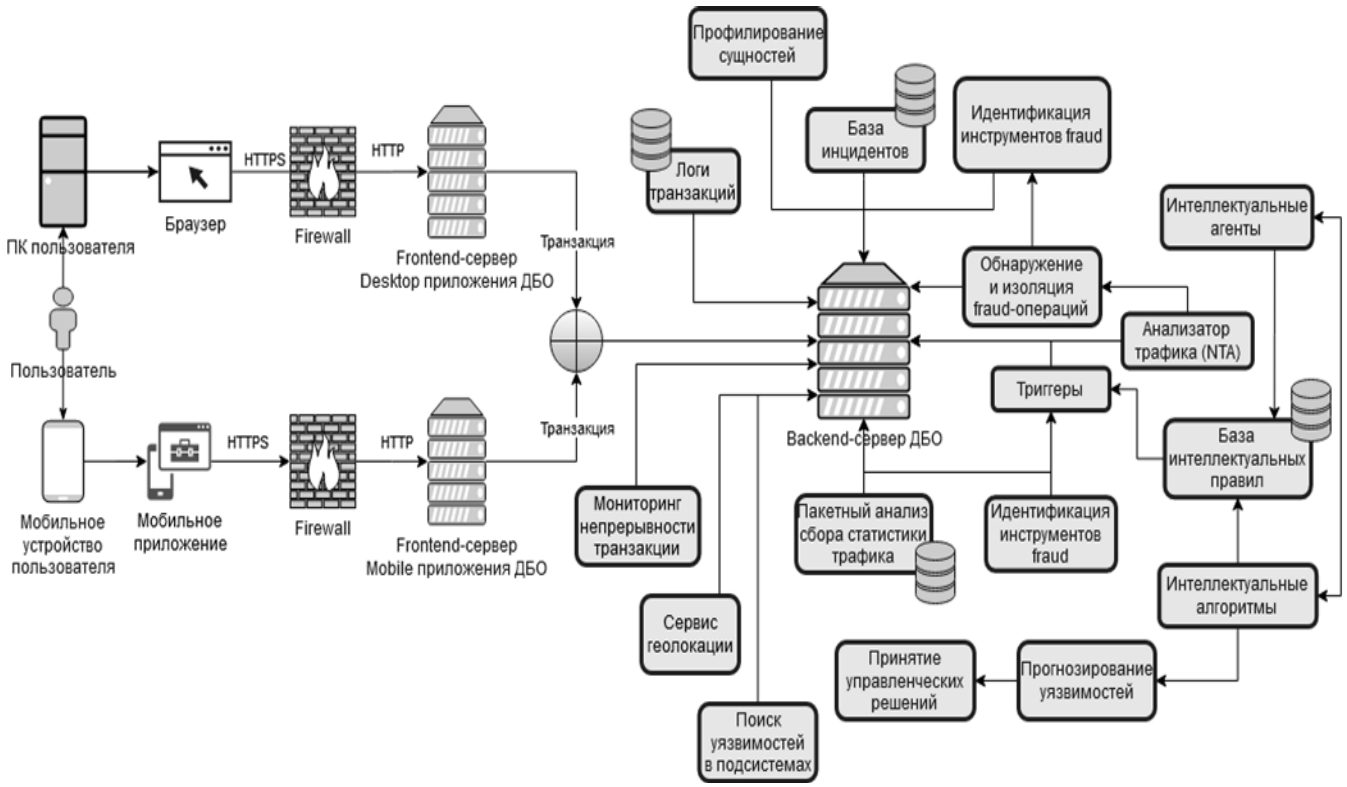

Рис. 1. Система ДБО «IntelSola»

Таким образом, на основании проведенного ранее функционального анализа, декомпозируем разрабатываемую модель antifraud-системы дистанционного банковского обслуживания (ДБО) «IntelSola», на следующие подсистемы (модули), необходимые для комплексного подхода в решении задачи (рисунок 1):

- Мониторинг непрерывности транзакции — модуль мониторинга и предотвращения прерывания транзакции между backend-сервером системы и банком-эмитентом;
- Сервис геолокации — модуль анализа геолокации проводимых транзакций;
- Предиктивный анализ сетевого трафика — модуль пакетного анализа для сбора статистики в разрезе заданных метрик, для предотвращения атак;
- Выявление аномалий, и установка маркеров обнаружения подозрительной сетевой активности — модуль анализа сетевого трафика (Network Traffic Analysis — далее NTA);
- Системный анализ смежных областей потенциальных направлений fraud-атак — аналитический модуль поиска уязвимостей в подсистемах;
- Обнаружение fraud-операций — модуль обнаружения и изоляции вредоносных процессов в подсистемах;
- Идентификация инструментов fraud — модуль идентификации вредоносных инструментов, их классификация, и декомпозиция для дальнейшего формирования базы правил;
- Формирование базы интеллектуальных правил — модуль формирования контуров интеллектуального отклика системы на соответствующее событие;
- Формирование базы инцидентов — модуль статистики всех инцидентов (как предотвращенных, так и совершившихся);
- Алгоритмы машинного обучения — модуль интеллектуальных алгоритмов;
- Когнитивные вычисления — модуль интеллектуальных агентов;
- Автоматизированная настройка и срабатывание триггеров — модуль автоматизированных настроек действий системы;
- Автоматизированное профилирование сущностей — модуль создания новых профилей, а также тонких настроек существующих;
- Выявление проблемных областей, и прогнозирование на основе уязвимостей потенциальных направлений FRAUD-атак — модуль прогнозирования уязвимостей;
- Принятие управленческих решений на основе типа fraud-атаки — модуль принятия соответ-

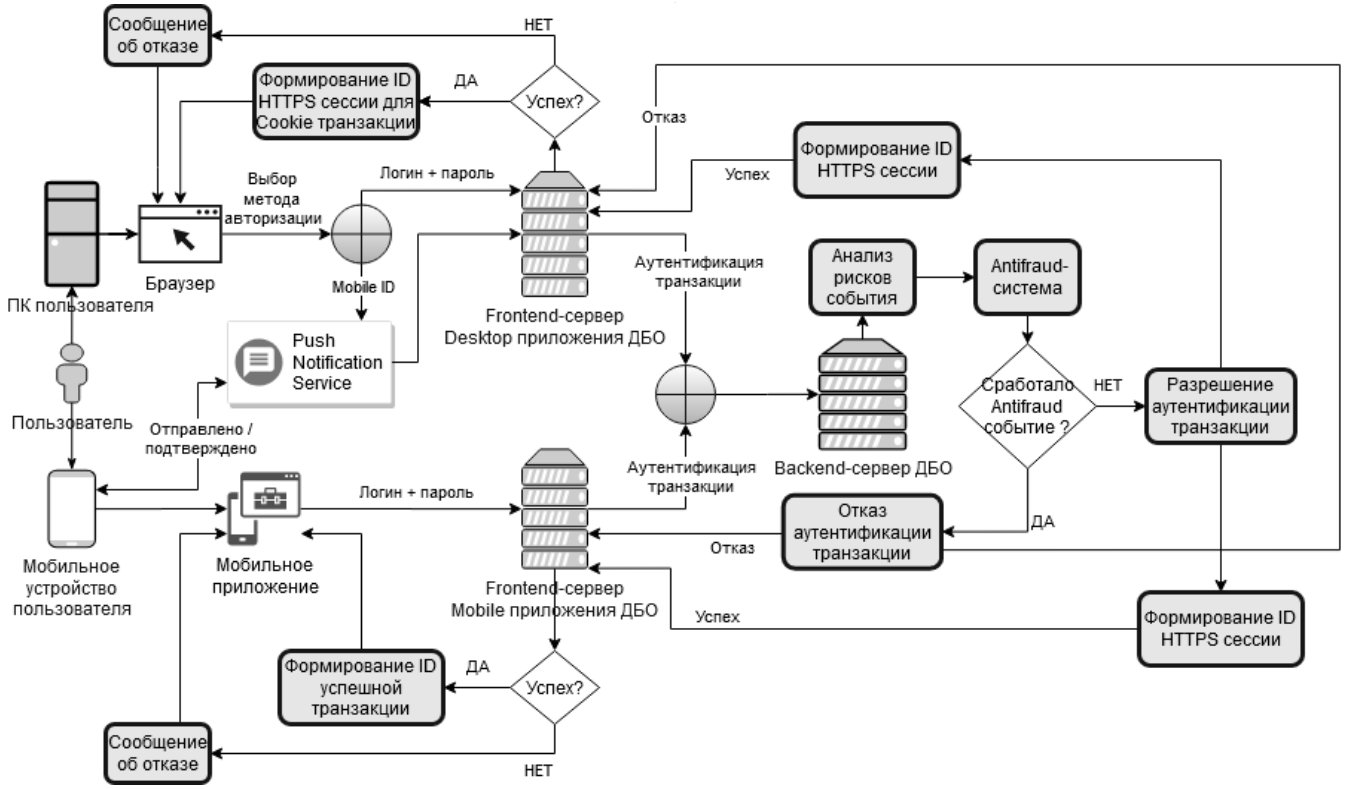

Рис. 2. Аутентификация транзакции

ствующего решения, как при потенциальной атаке, так и при совершившемся действии.

Аутентификация транзакции в общем виде представляет собой оценку рисков Antifraud-системой ее легитимности [7, 8], и на основании проведенного анализа или подтверждается, или отклоняется (рисунок 2).

Важную роль в структуре разрабатываемой системы имеет связь модулей: Интеллектуальные агенты; Интеллектуальные алгоритмы; База интеллектуальных правил. В общем виде концепт взаимодействия можно представить как адаптивные автономные алгоритмы, корректирующие свой математический аппарат итеративными шагами уменьшения дисперсии нестандартными методами гибридизации интеллектуальной системы, представляющими собой совокупность взаимодействующих между собой полиморфных структур: рекомбинантных агентов (структурных моделей); автономных интеллектуальных агентов интеграторов; интеллектуальных агентов принятия решений; базисных автономных интеллектуальных агентов; совокупной структуры интеллектуальной базы данных (рисунок 3).

Рассмотрим назначение основных агентов концепта гибридной модели мультиагентной подсистемы искусственного интеллекта Antifraud-системы:

1. Рекомбинантные агенты (модели): лингвистический агент — языковой модуль обработки и преобразования текстовых и графических массивов данных; логический агент — формализация нечеткой логики; аналитический агент — многомерный и многоуровневый анализ прогнозирования; стохастический агент — генератор вероятностных методов стохастической оптимизации и генетических алгоритмов; агент векторного квантования задач классификации — сети векторного квантования (минимизация искажения при кодировании), самоорганизующиеся карты Кохонена (аппроксимация данных); агент дискриминантного анализа нечетких систем — классификация обучающих выборок N совокупностей (групп); агент кластеризации эвристического нейросетевого алгоритма — решение задач отнесения образца к одному из нескольких попарно не пересекающихся множеств; алгоритм графового метода кластеризации — приближённый алгоритм поиска оптимума; агент адаптивных линейных сумматоров — нерекурсивный адаптивный фильтр для обработки сигналов и регулирования весовых коэффициентов. Совокупность вышеперечисленных рекомбинантных агентов позволяет создать мощную гибридную составляющую

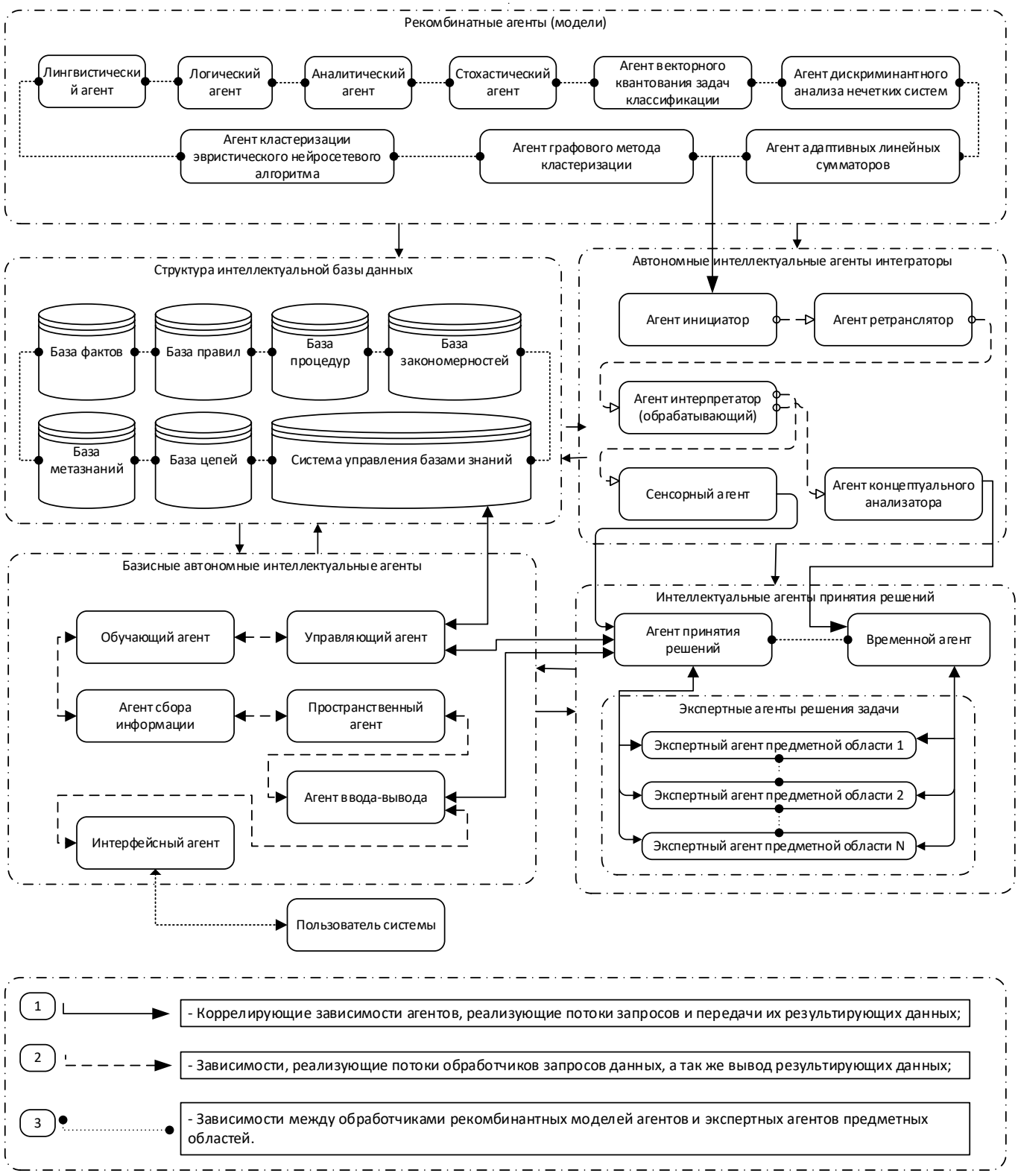

Рис. 3. Концепт гибридной модели мультиагентной подсистемы искусственного интеллекта Antifraud-системы

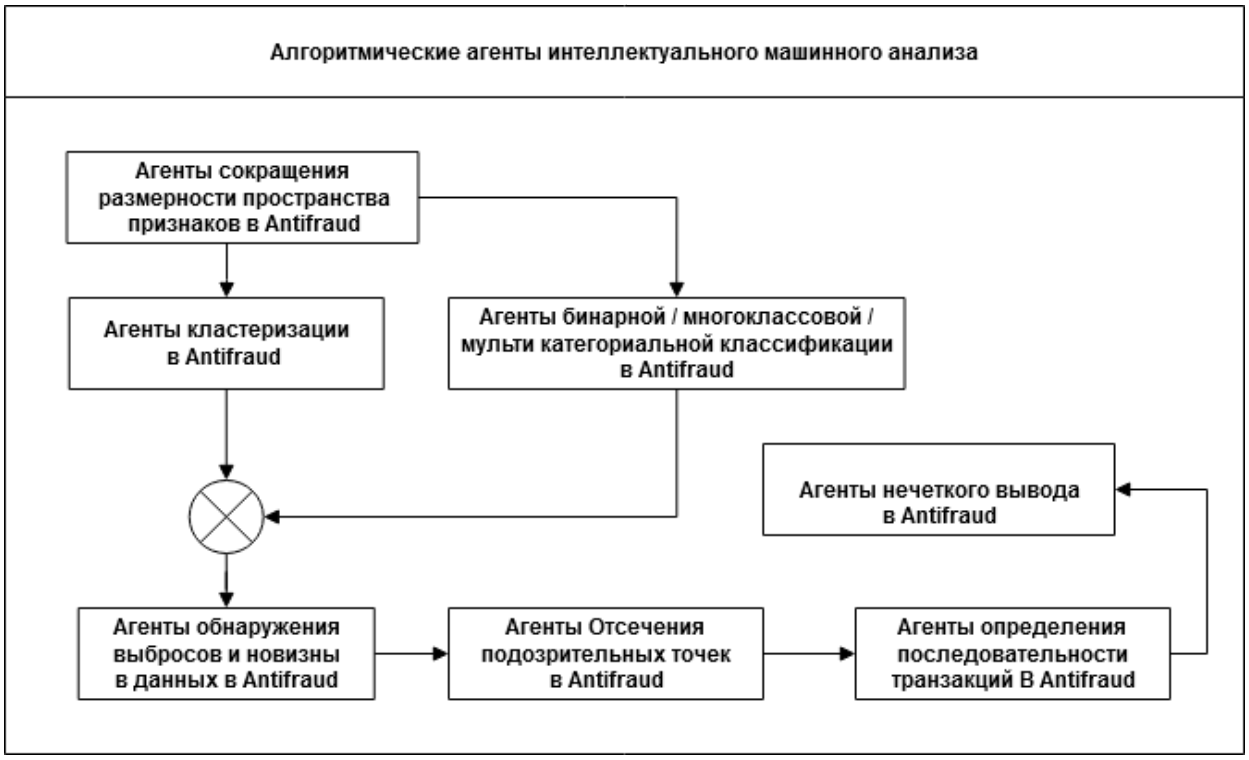

Рис. 4. Укрупненная модель алгоритмических агентов

будущей интеллектуальной системы принятия решений, отвечающую за первоначальную обработку, аналитику, а также инициацию пакетов предварительно обработанных алгоритмов, для дальнейших принятий интеллектуальных решений, с минимальным количеством степеней вероятностных отклонений.

2. Автономные интеллектуальные агенты интеграторы: агент инициатор — сбор и отправка систематизированных данных (буфер между рекомбинантными агентами и автономными интеллектуальными агентами); агент ретранслятор — обеспечение коммуникации (коммуникация между рекомбинантными агентами и автономными интеллектуальными агентами); обрабатывающий агент интерпретатор — решение типовых проблем распознавания речи; сенсорный агент — обработка сенсорных сигналов при помощи нейросетевых алгоритмов; агент концептуального анализатора — прогнозирование действий системы по оперативным данным, и создание рабочего сценария поиска решения. Таким образом автономные интеллектуальные агенты интеграторы позволяют обработать и систематизировать данные, с минимизацией временных интервалов, необходимых для системно-интеллектуальной аналитики.
3. Интеллектуальные агенты принятия решений: временной агент — принятие системой оперативных решений; агент принятия решений — непосредственное принятие взвешенных решений; экспертные агенты решения задачи N предметных областей.
4. Базисные автономные интеллектуальные агенты: обучающий агент — внесение усовершенствований, обучение; управляющий агент — управление структурами; агент сбора информации — сбор и предварительная обработка информационных структур; пространственный агент — моделирование информационно-имитационного пространства рабочей среды; агент ввода-вывода — система ввода-вывода информации; интерфейсный агент — адаптивный интерфейс пользователя.
5. Структура интеллектуальной базы данных — база фактов; база правил; база процедур; база закономерностей; база метазнаний; база цепей; система управления базами знаний (СУБД).

Вышеописанная модель гибридной интеллектуальной системы поддержки управленческих решений не просто соответствует общей концепции построения принятия решения, но и позволяет построить и адаптировать информационную модель проблемной предметной области исследования [7–9], координируя процесс организации вычислений такими значимыми преимуществами, как: минимизация временных и стоимостных

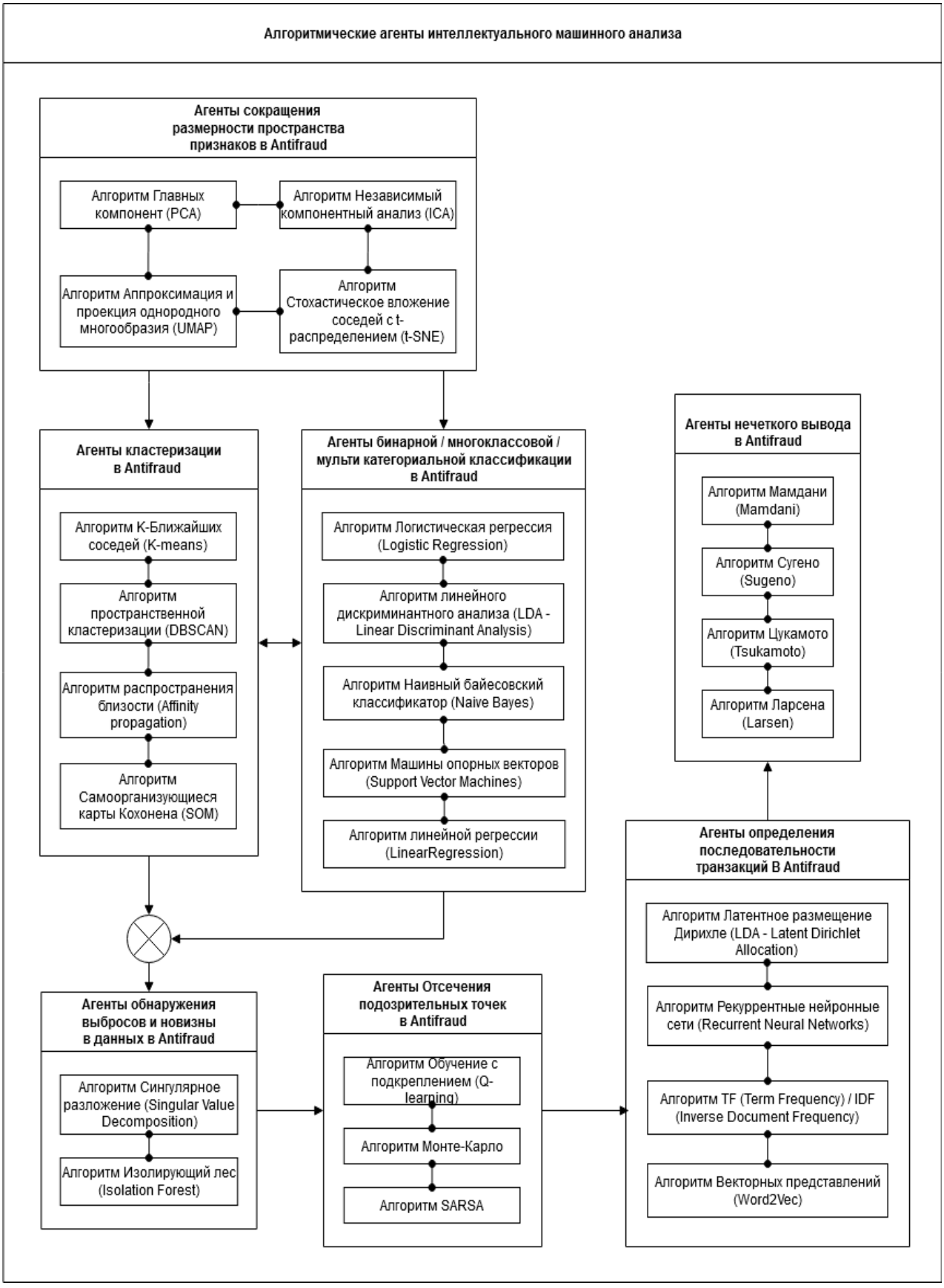

Рис. 5. Детализация модели алгоритмических агентов

показателей, повышение интегративных возможностей в процессе проведения асинхронных вычислений.

В общем виде структура алгоритмических агентов интеллектуального машинного анализа включает в себя следующие составляющие (рисунок 4):

1. Агенты сокращения размерности пространства признаков.
2. Агенты кластеризации.
3. Агенты бинарной / многоклассовой /мульти категориальной классификации.
4. Агенты обнаружения выбросов и новизны в данных.
5. Агенты отсечения подозрительных точек.
6. Агенты определения последовательности транзакций.
7. Агенты нечеткого вывода.

Агенты снижения размерности пространства позволяют моделям быстрее учиться, тратить гораздо меньше времени на переобучение. Признаки и факторы ранжируются в зависимости от значимости и приоритетов в той или иной логике, при срабатывании триггера, определяющего тип события в Antifraud.

Агенты кластеризации декомпозируют массивы данных на N количество групп, по категориальным и групповым признакам.

Агенты бинарной / многоклассовой / мультикатегориальной классификации производят обучение классификаторов, на основе декомпозированных данных, и дальнейшего их использования для прогнозирования меток.

Агенты обнаружения выбросов и новизны в данных позволяют идентифицировать экстремумы значений, которые выходят за пределы обучающих выборок. Таксономия методов идентификации выбросов в данном контексте агентов определяется: анализом экстремальных значений базисных распределений; построением вероятностных и статистических моделей; построением проекционных алгоритмов в линейных моделях; построением моделей на основе изолированных классов (на основе близости к кластеру); обнаружением экземпляров классов, удлиняющих совокупности наборов структурированных и упорядоченных данных; обнаружением выбросов в размерностях кластерных каналов, с декомпозицией на основе близости к экстремумам функций. Вышеописанная таксономия является критически важной совокупностью моделей определения и интерпретируемости выбросов, так как на основе принятого решения агентами, производится определение, является ли анализируемый экземпляр класса выбросом или нет.

Агенты отсечения подозрительных точек производят: балансировку данных, фильтрацию транзакций, доработка массивов выборки на предмет определения fraud-транзакций; обнаружение и формирование взаимосвязей, аномалий, и закономерностей в массивах данных.

Агенты определения последовательности транзакций формируют модель неявных групп, при помощи которой интерпретируются результаты наблюдений массивов данных, для определения степени нечеткости при построении иерархической потоковой последовательности операций.

Агенты нечеткого вывода позволяют получить и интерпретировать заключения в виде нечетких продукционных правил, на основе нечеткий условий или инфологических состояниях анализируемых массивов данных.

Детализация модели алгоритмических агентов представляет собой совокупность различных алгоритмов, комбинации которых позволяют достичь максимально релевантных результатов в разрабатываемой Antifraud-системе (рисунок 5).

Построение динамических моделей интеллектуального анализа на основе представленных комбинаций и последовательностей алгоритмов машинного анализа [10–12] позволяет:

- минимизировать: риски проведения мошеннических транзакций; риски отклонения валидных транзакций; риски принятия некорректных управленческих решений на основе полученных аналитических сводок и выкладок;
- максимизировать: скорость обработки транзакций; процесс декомпозиции транзакции на потоки; процент валидных транзакций; скорость и качество принятия управленческих решений.

Заключение

Таким образом, в рамках исследований проведен концептуальный анализ построения аналитических систем предотвращения FRAUD-операций при проведении банковских транзакций, результаты которого могут быть использованы для повышения качества и защищенности обрабатываемой информации в финансовых организациях. Описаны основные требования к стандартам безопасности Antifraud-системы и формирована ее архитектурная модель. Проведен анализ построения Antifraud-системы. Разработана концептуальная модель AntiFraud-системы, которая может быть рекомендована в качестве основы для реализации физической системы.

ЛИТЕРАТУРА

1. Ричардсон Крис, Микросервисы. Паттерны разработки и рефакторинга.— СПб.: Питер, 2019.— 544 с.: ил.— (Серия «Библиотека программиста»). ISBN978–5–4461–0996–8.
2. Ньюмен С. Создание микросервисов.— СПб.: Питер, 2016.— 304 с.: ил.— (Серия «Бест-селлеры O'Reilly»). ISBN978–5–496–02011–4.
3. Gaidamaka Y.V., Romashkova O.N., Ponomareva L.A., Vasilyuk I.P. Application of information technology for the analysis of the rating of university // CEUR Workshop Proceedings 8. Сер. "ITTMM 2018 — Proceedings of the Selected Papers of the 8th International Conference "Information and Telecommunication Technologies and Mathematical Modeling of High-Tech Systems"" 2018. С. 46–53.
4. Литвак Б.Г., Стефановский Д.В. Моделирование и построение глобального управленческого цикла // В книге: Управление развитием крупномасштабных систем (MLSD'2011). Материалы пятой международной конференции. 2011. С. 124–126.
5. Горелов Г.В., Ромашкова О.Н. Оценка качества обслуживания в сетях с пакетной передачей речи и данных // Вестник Российского университета дружбы народов. Серия: Прикладная и компьютерная математика. 2003. Т. 2. № 1. С. 23–31.
6. Dr. Anasse Bari, Mohamed Chaouchi, Tommy Jung. Predictive Analytics For Dummies // For Dummies; 2nd edition (October 31, 2016).— 464 pages. ISBN10 8126567937 (ISBN13 978–1119267003).
7. Ромашкова О.Н., Федин Ф.О., Фролов П.А. Применение нейросетевых технологий для проверки благонадежности контрагентов сетевой торговой компании // Современная наука: актуальные проблемы теории и практики. Серия: Экономика и право. 2018. № 7. С. 126.
8. Ian Goodfellow, Yoshua Bengio, Aaron Courville, Deep Learning. The MIT Press; Illustrated edition (November 18, 2016).— 800 pages. ISBN10 0262035618 (ISBN13 978–0262035613).
9. Ромашкова О.Н., Яковлев Р.И. Анализ моделей и методов для оценки живучести инфокоммуникационных сетей в условиях чрезвычайных ситуаций // T-Comm: Телекоммуникации и транспорт. 2012. Т. 6. № 7. С. 165–170.
10. Ромашкова О.Н., Федин Ф.О., Ермакова Т.Н. Нейросетевая компьютерная модель для поддержки принятия решений в образовательных комплексах // Вестник Рязанского государственного радиотехнического университета. 2017. № 61. С. 54–59.
11. Пономарева Л.А., Ромашкова О.Н., Василюк И.П. Алгоритм оценки эффективности работы кафедр университета для управления его рейтинговыми показателями // Вестник Рязанского государственного радиотехнического университета. 2018. № 64. С. 102–108.
12. Gorelov G.V., Kazanskii N.A., Lukova O.N. Communication quality assessment in speech packet transmission networks with random service interrupts // Automatic Control and Computer Sciences. 1993., vol.27., no.1., p.62.

Журнал «Современная наука: актуальные проблемы теории и практики»