УДК 338.24:004.8:343.97

МЕТОДОЛОГИЧЕСКИЕ АСПЕКТЫ ПРИМЕНЕНИЯ ИИ-ИНСТРУМЕНТАРИЯ В КИБЕРУЧЕТЕ КАК ФАКТОР ПРЕВЕНЦИИ ПРАВОНАРУШЕНИЙ

METHODOLOGICAL ASPECTS OF USING AI TOOLS IN CYBER-ACCOUNTING AS A FACTOR IN PREVENTING OFFENSES

В. В. Мякинькая
Белорусский государственный университет
пищевых и химических технологий,
декан инженерно-инновационного факультета,
кандидат экономических наук, доцент

Аннотация. *В статье обоснована методология киберучета как интеллектуальной системы, обладающей эмерджентным свойством самоочищения от криминогенных факторов в момент инициации данных и (или) бизнес-процесса.*

Ключевые слова: *киберучет, искусственный интеллект, превенция правонарушений, цифровая трансформация, экономическая безопасность.*

Annotation. *This article substantiates the methodology of cyber-accounting as an intelligent system with the emergent property of self-cleansing from criminogenic factors at the moment of data and/or business process initiation.*

Keywords: *cyber accounting, artificial intelligence, crime prevention, digital transformation, economic security.*

Современная практика бухгалтерского учета в Республике Беларусь опирается на развитое прикладное программное обеспечение (класса 1С и аналоги), обладающее инструментарием ретроспективного контроля. Однако существующий функционал ориентирован преимущественно на верификацию непреднамеренных ошибок. В условиях усложнения экономических отношений традиционный инструментарий демонстрирует свою неэффективность, что выражается в отсутствии возможности выявлять умышленное искажение данных, интегрированное в легитимные бизнес-процессы [1].

Согласно данным правоохранительных органов Республики Беларусь, ключевыми угрозами экономической безопасности остаются латентные схемы: дробление бизнеса, уход от налогов под видом «налоговой оптимизации», подмена трудовых отношений и незаконное использование преференциальных режимов. Статистика подтверждает, что традиционный «постфактум-контроль» не справляется с выявлением таких правонарушений ввиду высокого уровня их маскировки [2]. Решением данной проблемы выступает разрабатываемая нами концепция киберучета, который способен распознать сложные криминальные транзакции там, где классические программы видят обычную проводку.

Киберучет — это интеллектуализированная система непрерывного учета, обладающая «цифровой субъектностью»: она не просто фиксирует факты хозяйственной жизни, а в режиме реального времени анализирует правовую чистоту каждой транзакции. В данной модели за человеком сохраняются функции стратегического уровня (формирование допущений учетной политики), тогда как ИИ-инструментарий обеспечивает непрерывный превентивный мониторинг. В данной модели алгоритмы искусственного интеллекта (далее — ИИ) обеспечивают непрерывную обработку данных о фактах хозяйственной жизни, предиктивную верификацию, рискориентированный мониторинг качества информации и перспективные прогнозы. При этом за человеком закрепляются функции институционального уровня: формирование учетной политики, вынесение окончательного профессионального суждения и несение юридической ответственности за итоговые отчетные показатели.

Развитие киберучета предполагает имплементацию ИИ непосредственно в метод бухгалтерского учета. Интеграция позволяет реализовывать принцип преобладания экономической сущности над правовой формой в автоматическом режиме. Если бухгалтерский учет первичным учетным документом признает документ, то алгоритмы киберучета анализируют контекстуальный слой транзакции — целесообразность и реальность операции, идентифицируют «цифровую тень» преступления еще до момента формирования проводки.

Концептуально киберучет является закономерным развитием теории динамического баланса (И. Шер, Г. Дипи) и рискориентированных учетных систем [3; 4]. Если классический бухгалтерский баланс ориентирован на исчисление финансового результата, то киберучет дополняет эту модель вектором правовой легитимности.

Таким образом, предлагаемый нами киберучет следует рассматривать как адаптивную учетную систему, которая самостоятельно настраивается под меняющиеся паттерны криминогенных угроз. В такой модели двойная запись перестает быть просто математическим равенством. Она становится контрольным фильтром, когда каждое изменение состояния счетов проходит через когнитивный аудит алгоритмов.

В методологии киберучета достоверность становится динамической характеристикой, поддерживаемой непрерывно, в режиме реального времени.

Методологический инструментарий киберучета представлен в таблице 1.

Таблица 1

Технологический инструментарий киберучета в системе превенции правонарушений

Инструмент ИИ / Суть	Механизм работы в киберучете	Связь с экономической преступностью (на примерах практики судов Республики Беларусь)
Семантический анализ (NLP). Автоматизированная обработка текстов на естественном языке и неструктурированных данных	Сверка сути договора и назначения платежа с реальными кодами общегосударственного классификатора экономических видов деятельности, рыночными ценами и производственными мощностями субъекта	Дела о незаконном получении льгот и субсидий в сельской местности. ИИ сопоставляет объемы закупленного топлива и удобрений по данным учета с реальной площадью посевных площадей. Если данные противоречат физическим нормам расхода и мощностям производства, система маркирует это как попытку хищения бюджетных средств или умышленное завышение затрат
Анализ аномалий (Unsupervised Learning). Поиск отклонений от «нормального» поведения без заранее заданных условий	Алгоритмы ML выявляют «микропаттерны» (смурфинг), нетипичную частоту или структуру платежей, выпадающую из кластера обычного поведения субъекта	Схемы по «обналичиванию» через индивидуальных предпринимателей, где сотни мелких транзакций маскируют единый умысел. ИИ выявляет нетипичное снятие наличности сразу после зачисления, предупреждая легализацию доходов (ст. 235 Уголовного кодекса Республики Беларусь) [4; 5]
Графовая детекция (Network Analysis). Математический анализ связей между объектами	Визуализация сетей контрагентов. Поиск общих IP-адресов, телефонов и пересекающихся финансовых потоков. Вычисление коэффициентов аффилированности	Дела о дроблении бизнеса (например, в сфере ритейла или оказания услуг). ИИ выявляет скрытую взаимозависимость десятков «технических» обществ, созданных для искусственного распределения выручки и ухода от налогов (ст. 243 Уголовного кодекса Республики Беларусь) [4; 5]
Предиктивный скоринг (Risk-Scoring). Прогнозирование вероятности правонарушения	Система присваивает каждой операции «индекс криминогенности» на базе исторических данных о выявленных преступных схемах	Предотвращение незаконного возврата НДС. Система предсказывает риск фиктивного экспорта еще на этапе формирования накладных, анализируя нетипичные логистические маршруты и историю контрагента

Окончание табл. 1

Цифровая гигиена (Закон Бенфорда). Математический контроль достоверности данных	Анализ частоты появления цифр в бухгалтерских регистрах. Выявление искусственных манипуляций с отчетностью	Дела о хищениях путем злоупотребления полномочиями (ст. 210 Уголовного кодекса Республики Беларусь) [4; 5]. ИИ находит «подрисованные» цифры в авансовых отчетах или ведомостях, которые не соответствуют естественному математическому распределению цифр
Автоматизированный KYC (Know Your Customer). Интеллектуальная проверка личности	Интеграция с государственными базами данных («черные списки», реестры неблагонадежных субъектов)	Защита от схем с «ИП-менеджерами». При попытке завести в учетную систему договор с бывшим сотрудником, ставшим ИП, ИИ сигнализирует о признаках подмены трудовых отношений
Аудит смарт-контрактов (Blockchain + AI)	Проверка кода исполняемых контрактов на наличие уязвимостей для скрытого вывода активов	Сфера цифровых знаков (токенов) в рамках Декрета № 8 [6]. Предотвращение киберхищений и манипуляций с отчетностью организаций — резидентов Парка высоких технологий

Методологическая ценность описанного ИИ-инструментария заключается в его мультисубъектности. Трансформируясь из узкоспециализированного ИТ-решения в инклюзивный механизм институциональной защиты, киберучет конвертирует алгоритмы детекции в конкретные правовые гарантии. Это обеспечивает сбалансированную защиту интересов на всех уровнях социально-экономической системы (табл. 2).

Таблица 2

Матрица превентивного воздействия системы киберучета на криминогенные факторы

Уровни защиты интересов / Суть проблемы	Механизм реализации (ИИ-инструментарий)	Ожидаемый эффект (правовой и экономический результат)
Граждане и работники. Проблема: неосознанное вовлечение бухгалтеров и менеджеров в схемы «серых» закупок и «подставного» руководства	Использование NLP-анализа входящих договоров и электронных счет-фактур. Идентификация «фирм-пустышек» и блокировка подписания документов с признаками фиктивности в режиме «нулевой точки» (до совершения операции)	Защита добросовестных работников от репутационных рисков, исключение рисков привлечения к уголовной и субсидиарной ответственности за соучастие в преступлении
Субъекты хозяйствования. Проблема: внутреннее мошенничество (кикбэки, откаты), демпинг со стороны недобросовестных конкурентов и вывод активов	Применение графового анализа для обнаружения скрытых аффилированностей. Контроль неизменности учетных данных через цифровые следы, исключающий возможность «подкрутки» баланса	Создание экосистемы доверия. Повышение инвестиционной привлекательности бизнеса. Соблюдение закона становится технологически дешевле и безопаснее, чем поиск лазеек
Государство. Проблема: сложные схемы дробления бизнеса, незаконный возврат НДС, выплата «зарплат в конвертах», манипуляции со льготами	Использование Закона Бенфорда и нейросетевого анализа отклонений для верификации первичных документов. Переход от выездных проверок к дистанционному рискориентированному мониторингу	Формирование гарантированно «чистого» налогового поля. Снижение государственных расходов на содержание громоздкого ревизионного аппарата при одновременном росте собираемости налогов
Правовая среда. Проблема: высокая латентность (скрытость) экономических правонарушений и сложность их обнаружения в бумажных/архаичных массивах данных	Интеграция учета с обучаемыми моделями (ML), способными видеть «цифровую тень» преступления (аномалии транзакций) до момента подачи деклараций	Трансформация правовой культуры: переход от страха перед проверкой к архитектурной невозможности совершения правонарушения в силу прозрачности учетной среды

Синергия ИИ и бухгалтерского учета обеспечивает переход к непрерывному интеллектуальному надзору, позволяет трансформировать традиционный бухгалтерский учет из инструмента ретроспективного наблюдения в механизм активной защиты национальных экономических интересов. Внедрение киберучета лишает экономическую преступность ее главного условия — латентности. Формируемая цифровая среда «неизбежности» выявления следов экономических преступлений обеспечивает эволюцию правовой культуры, где технологическая невозможность нарушения закона становится фундаментом устойчивого развития государства и бизнеса.

1. Криминальный сдвиг: в Беларуси вдвое выросло число экономических правонарушений [Электронный ресурс] // Myfin : [сайт]. URL: https://myfin.by/article/zhizn/kriminalnyj-sdvig-v-belarusi-vdvoe-vyroslo-cislo-ekonomiceskikh-pravonarusenij-37564 (дата обращения: 15.01.2026). Перейти к источнику Вернуться к статье

2. От дроперов до криптовалют: названы главные финансовые махинации в Беларуси [Электронный ресурс] // Myfin : [сайт]. URL: https://myfin.by/article/biznes/ot-droperov-do-kriptovalut-nazvany-glavnye-finansovye-mahinacii-v-belarusi-38518 (дата обращения: 15.01.2026). Перейти к источнику Вернуться к статье

3. Дипи Г. В. Введение в теорию бухгалтерского учета. М. : Финансы и статистика, 1988. 208 с. Вернуться к статье

4. Шерр И. Ф. Бухгалтерия и баланс / пер. с нем. С. И. Цедербаума. М. : Экономика и жизнь, 1925. 575 с. Вернуться к статье

5. Уголовный кодекс Республики Беларусь [Электронный ресурс] : 9 июля 1999 г. № 275-З : принят Палатой представителей 2 июня 1999 г. : одобр. Советом Респ. 24 июня 1999 г. : в ред. Закона Респ. Беларусь от 20 окт. 2025 г. № 101-З. Доступ из информ.-поисковой системы «ЭТАЛОН». Вернуться к статье

6. О развитии цифровой экономики [Электронный ресурс] : Декрет Президента Респ. Беларусь от 21 дек. 2017 г. № 8 : в ред. от 18 марта 2021 г. № 1. Доступ из информ.-поисковой системы «ЭТАЛОН». Вернуться к статье