РАЗРАБОТКА МАТЕМАТИЧЕСКОЙ МОДЕЛИ АВТОМАТИЗИРОВАННОГО МОНИТОРИНГА ПОСЕЩАЕМОСТИ СОТРУДНИКОВ

Марышева Л.Т., Абдуллаев Д.Б.
Ташкентский университет информационных технологий имени Мухаммада ал-Хоразмий, Ташкент, Узбекистан
Марышева Л.Т. — доцент кафедры системного и прикладного программирования; Абдуллаев Д.Б. — магистрант
Электронная почта: loramarish@mail.ru; dilavar7517@gmail.com

Аннотация. *В статье рассматривается математическая модель автоматизированного мониторинга посещаемости сотрудников, объединяющая RFID-регистрацию, биометрическую идентификацию, событийную обработку и машинное обучение для прогнозирования отсутствий. Исходный материал содержит архитектуру системы, модуль адаптивного прогнозирования, оптимизацию распределения ресурсов и сравнительные метрики до и после адаптации. В переработанной версии модель формализована через поток событий присутствия, композитную вероятность верификации личности, расчет фактически отработанного времени, коэффициент использования рабочего времени, вероятностный прогноз отсутствия и задачу назначения персонала. Отдельно уточнено, что метод анализа иерархий должен включать матрицы попарных сравнений, получение весов и проверку согласованности, тогда как приведенная в исходном тексте функция максимизации является задачей назначения с весами, а не полной процедурой AHP. Анализ экспериментальной части выявил существенные ограничения: не указаны размер и состав выборки, период наблюдения, доля отсутствий, признаки модели, схема разделения данных, процедура валидации, порог классификации и доверительные интервалы. Кроме того, численные результаты внутри статьи частично расходятся: приводятся различные значения точности идентификации и полноты прогнозирования. Поэтому эти показатели сохранены как авторские результаты, но не трактуются как независимо подтвержденные. Для повышения воспроизводимости предложен временной train-validation-test протокол, анализ дисбаланса классов, оценка Precision, Recall, F1, ROC-AUC и PR-AUC, а также мониторинг дрейфа модели. Дополнительно рассмотрены требования к защите биометрических данных, презентационным атакам и законности мониторинга работников в Узбекистане. Сформулированы направления дальнейшей апробации на реальных данных предприятий. Практическая ценность подхода состоит в переходе от простого табельного учета к управляемой системе поддержки решений, однако применение прогнозов к конкретным работникам требует прозрачного назначения целей, ограничения доступа к данным, проверки качества по группам пользователей и обязательного участия ответственного специалиста при интерпретации автоматических сигналов и принятии кадровых решений.*

Ключевые слова: *мониторинг посещаемости, RFID, биометрия, машинное обучение, прогнозирование отсутствий, AHP, персональные данные, адаптация, верификация, рабочее время.*

ВВЕДЕНИЕ

Автоматизированный учет рабочего времени является частью цифровой инфраструктуры управления персоналом. Его задача состоит не только в

регистрации входов и выходов, но и в получении достоверной временной последовательности событий, пригодной для формирования табеля, анализа загрузки подразделений и оперативного планирования ресурсов. Исследования систем посещаемости показывают, что RFID снижает трудоемкость регистрации, однако самостоятельное использование карты не исключает передачи идентификатора другому сотруднику; поэтому в прикладных системах применяются комбинированные схемы RFID и биометрической аутентификации [1–6].

Исходная статья предлагает комплексную модель, включающую RFID, биометрию, фильтрацию событий, прогнозирование отсутствий методом машинного обучения и перераспределение задач с использованием метода анализа иерархий. Такая постановка расширяет традиционный табельный учет до интеллектуальной системы поддержки управленческих решений. Вместе с тем объединение биометрии, кадровых данных и прогнозной аналитики требует строгого разделения задач: идентификация сотрудника, вычисление рабочего времени, прогноз отсутствия и управленческое распределение персонала имеют разные целевые переменные, метрики качества и риски ошибок.

Научная проблема исследования заключается в построении воспроизводимой математической модели, которая связывает события посещаемости с прогнозом отсутствий и кадровым планированием, но не смешивает результаты разных модулей. Особенно важно обеспечить корректную экспериментальную проверку: в исходном материале заявлены показатели высокой идентификации и прогнозирования, однако отсутствуют сведения о размере выборки, периоде наблюдения, классовом балансе, наборе признаков, схеме train-test разделения, параметрах алгоритма и доверительных интервалах. Без этих данных невозможно определить, отражают ли показатели реальную обобщающую способность модели или свойства конкретной выборки.

Цель исследования — усовершенствовать математическую модель автоматизированного мониторинга посещаемости сотрудников путем формализации событийного потока, композитной верификации, прогнозирования отсутствий и задачи распределения ресурсов, а также разработать воспроизводимый протокол экспериментальной оценки. Для достижения цели поставлены задачи: определить структуру входных событий; формализовать расчет фактически отработанного времени; задать модель вероятностной идентификации; определить признаки и целевую переменную прогнозирования; сформировать cost-sensitive критерий ошибок; уточнить использование AHP; установить метрики качества; выделить требования к безопасности, защите персональных данных и мониторингу модели после внедрения.

Объектом исследования является процесс автоматизированного учета присутствия и использования рабочего времени сотрудников организации. Предметом исследования выступают математические методы обработки событий посещаемости, вероятностной верификации личности, прогнозной аналитики и оптимизации распределения кадровых ресурсов. Рабочая гипотеза состоит в том,

что объединение нескольких источников идентификации и адаптивной модели прогнозирования способно повысить надежность учета, однако практический эффект подтверждается только при независимой валидации каждого модуля и соблюдении требований к работе с биометрическими и трудовыми данными. Научная новизна уточненной постановки состоит в объединении модулей в единый формализованный контур с явным разграничением метрик и рисков.

ОБЗОР ЛИТЕРАТУРЫ

Системы RFID традиционно применяются для автоматической регистрации присутствия и сокращения ошибок ручного учета. Maramis и Rompas предложили RFID-систему учета сотрудников [1], Zaman и соавторы рассмотрели архитектуру RFID attendance [2], а Meghana и соавторы показали применение RFID для интеллектуального учета посещаемости [3]. В этих работах основной акцент сделан на автоматизации регистрации, а не на прогнозировании отсутствий. Поэтому перенос RFID-событий в интеллектуальную модель требует отдельного слоя очистки и верификации данных.

Для снижения риска регистрации по чужой карте используются комбинированные схемы. Kumar и соавторы исследовали сочетание биометрии и RFID [4], Srinidhi и Roy — защищенную web-enabled систему мониторинга и позиционирования [5], а Chen и Li — систему посещаемости на основе распознавания лица и RFID [6]. Эти исследования подтверждают практическую целесообразность многофакторной регистрации, но не снимают необходимости тестировать биометрический компонент по специализированным метрикам. ISO/IEC 19795-1:2021 требует оценивать биометрические системы через ошибки и пропускную способность по документированному протоколу [10].

В 2024 году опубликована работа по RFID-мониторингу с машинным обучением, где Random Forest использовался для анализа исторических тенденций посещаемости и поддержки планирования ресурсов [7]. Более новые исследования по прогнозированию отсутствий показывают, что задача существенно отличается от простой классификации событий присутствия. В пилотном исследовании 2025 года использовались Accuracy, AUC, Precision, Recall и F1, а авторы отдельно описывали характеристики выборки и обработку выбросов [8]. Исследования predictive workforce management также подчеркивают проблему дисбаланса классов и необходимость оценивать качество несколькими метриками [9].

Для биометрической части важны риски презентационных атак и различий в ошибках между группами пользователей. NIST FATE Part 10 показал, что программные PAD-алгоритмы демонстрируют различную результативность для разных типов атак [14]. NISTIR 8280 фиксирует демографические различия в ошибках ряда алгоритмов распознавания лиц и подчеркивает необходимость тестирования на репрезентативной популяции [15]. Следовательно, заявление о «высокой достоверности идентификации» требует не только общей доли правильных решений, но и анализа ложных допусков, ложных отказов, качества

входных изображений и устойчивости к spoofing.

С точки зрения управления рисками NIST AI RMF 1.0 и ISO/IEC 23894:2023 рекомендуют рассматривать надежность, безопасность, прозрачность, конфиденциальность и управление вредным смещением на протяжении жизненного цикла AI-системы [12, 13]. Для HR-сценариев это особенно важно, поскольку ошибочный прогноз отсутствия может стать основанием для управленческого воздействия на конкретного работника. Поэтому прогноз должен использоваться как сигнал поддержки решения, а не как автоматическое доказательство нарушения.

Правовые и этические ограничения также являются частью методологии. Закон Республики Узбекистан «О персональных данных» определяет биометрические сведения как персональные данные, характеризующие анатомические и физиологические особенности субъекта; при использовании биометрии для установления личности закон предусматривает требование согласия, если иное не установлено законодательством, а действующая редакция содержит особые требования к хранению биометрических данных [16]. Трудовой кодекс Республики Узбекистан возлагает на работодателя обязанность организовать учет рабочего времени [17]. При этом международные рекомендации ILO подчеркивают необходимость ограничения целей, безопасности, прозрачности и уважения частной жизни работников при электронном мониторинге [18].

Таблица 1.

Научно-методическая база автоматизированного мониторинга посещаемости

Источник / направление	Что подтверждает	Что необходимо учесть в данной модели
RFID attendance [1–3]	Автоматизация фиксации присутствия.	Ошибки считывания, дубликаты, потеря/передача карты.
RFID + биометрия [4–6]	Повышение надежности регистрации.	Раздельная оценка RFID и биометрического модулей.
ML для посещаемости [7–9]	Возможность прогнозной аналитики.	Дисбаланс классов, временное разделение данных, несколько метрик.
ISO/IEC 19795-1 [10]	Принципы испытаний биометрических систем.	FMR/FNMR, throughput, документированный протокол.
NIST / ISO AI risk [12–15]	Управление рисками, bias, PAD, мониторинг.	Проверка групп, spoofing, drift и контроль после внедрения.
Узбекистан / ILO [16–18]	Правовой и трудовой контекст.	Согласие, цель обработки, доступ, хранение и прозрачность.

МЕТОДОЛОГИЯ

Модель строится как последовательность независимых, но связанных модулей: регистрация события, очистка данных, верификация личности, расчет рабочего времени, прогнозирование отсутствия и распределение ресурсов. Такое разбиение необходимо, поскольку ошибка идентификации не должна автоматически интерпретироваться как отсутствие сотрудника, а прогноз

вероятности отсутствия не является подтвержденным фактом нарушения трудового графика.

Каждая фиксация терминала представляется кортежем, содержащим идентификатор сотрудника, временную метку, точку прохода, тип события и показатели уверенности используемых каналов. Формально событие можно представить следующим образом:

$$e_k = (id_k, t_k, g_k, r_k, qRFID_k, qBIO_k) \quad (1)$$

где id_k — идентификатор сотрудника; t_k — временная метка; g_k — точка прохода; $r_k \in \{IN, OUT\}$ — тип события; $qRFID_k$ и $qBIO_k$ — признаки качества или уверенности соответствующих каналов. На стадии предобработки удаляются технические дубликаты, проверяется допустимая последовательность IN/OUT и нормализуются временные метки.

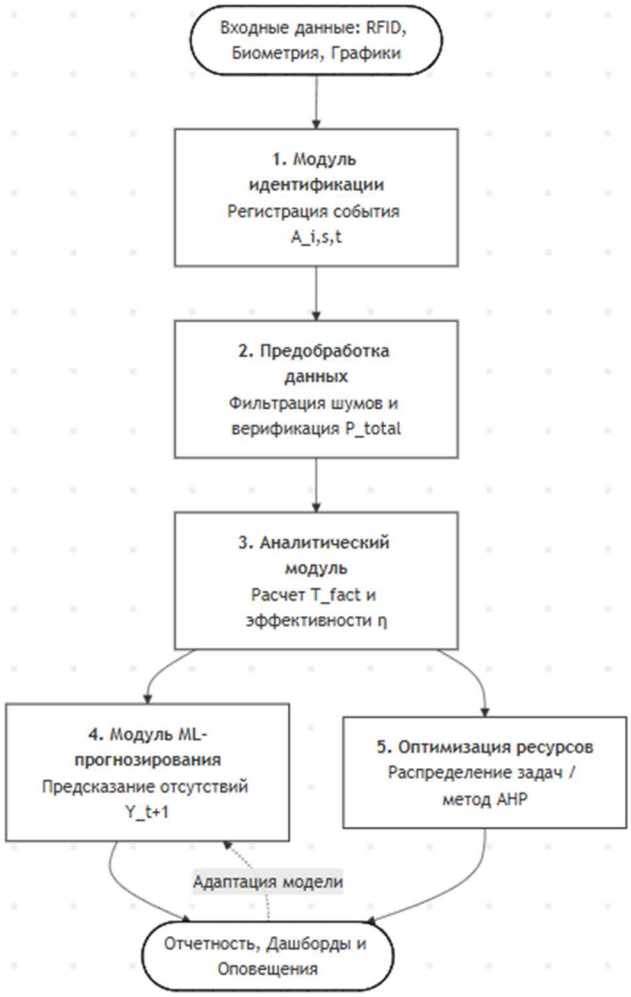

Рис. 1. Структурная схема математической модели мониторинга (по исходному материалу)

В исходной статье указано объединение RFID и биометрии через логистическую функцию, однако коэффициенты и правило калибровки не приведены. Для воспроизводимости композитный скор предлагается записывать как:

$$Ptotal = \sigma(\beta_0 + \beta_1 zRFID + \beta_2 zBIO + \beta_3 zCTX) \quad (2)$$

где $\sigma(z)=1/(1+e^{-z})$; zRFID — признак валидности карты; zBIO — нормированный биометрический score; zCTX — дополнительные контекстные признаки; β — параметры, оцениваемые на валидационной выборке. Решение о подтверждении личности принимается при $P_{total} \geq \tau_{id}$. Порог τ_{id} должен выбираться по допустимому соотношению ложного допуска и ложного отказа, а не по максимальной общей accuracy [10].

После очистки события объединяются в пары вход–выход внутри рабочего дня или смены. Фактически отработанное время сотрудника i определяется суммой валидных интервалов:

$$T_{fact,i} = \Sigma_k \, (t_{out,i,k} - t_{in,i,k}) \qquad (3)$$

Коэффициент использования рабочего времени определяется отношением фактического времени к нормативному:

$$\eta_i = T_{fact,i} / T_{norm,i} \qquad (4)$$

При этом η_i не следует интерпретировать как показатель индивидуальной производительности: он отражает только соотношение зарегистрированного и нормативного времени. Перерывы, командировки, дистанционная работа, отпуск, больничные и иные законные причины отсутствия должны кодироваться отдельно, чтобы не создавать ложные нарушения.

Для прогностического модуля формируется вектор признаков X_i,t на момент t, включающий только информацию, доступную до прогнозируемой даты. В исходной работе упомянуты окна 7 и 30 дней. Предлагаемая формализация имеет вид:

$$p_i,t+1 = f\theta(X_i,t), \quad y_i,t+1 \in \{0,1\} \qquad (5)$$

где $p_i,t+1$ — оценка вероятности отсутствия в следующем периоде, fθ — модель градиентного бустинга или другой классификатор, y — фактическая метка. Чтобы стоимость пропущенного реального отсутствия и ложной тревоги задавалась явно, используется взвешенная логистическая функция потерь:

$$L = -\Sigma \, [wFN \cdot y \cdot \ln(p) + wFP \cdot (1-y) \cdot \ln(1-p)] \qquad (6)$$

Весовые коэффициенты должны задаваться до тестирования и обосновываться бизнес-стоимостью ошибок. Критически важно не включать в признаки сведения, появляющиеся после прогнозируемого события, иначе возникает target leakage. Для временных данных рекомендуется хронологическое разделение train, validation и test, а не случайное перемешивание всех наблюдений.

Таблица 2.

Минимальный протокол воспроизводимой проверки модели

Компонент	Обязательные данные	Рекомендуемые метрики
Идентификация	Число сотрудников, число попыток, условия съемки, порог.	FMR/FNMR, TAR при заданном FMR, EER, latency.
Absenteeism ML	Период, N сотрудников, число событий, prevalence, признаки, split.	Precision, Recall, F1, ROC-AUC, PR-AUC, confusion matrix.
Адаптация	Правило переобучения, окно данных, baseline, контроль drift.	Изменение метрик во времени, PSI/другой drift indicator.
AHP/назначение	Критерии, эксперты, матрицы, CR, ограничения задачи.	CR, устойчивость решения, стоимость/покрытие задач.

Система	CPU/RAM, число терминалов, поток событий.	Latency, throughput, доступность, доля ошибок обработки.

В исходной статье приведена функция максимизации $\Sigma\omega_{ij}x_{ij}$. Такая запись соответствует задаче назначения, если веса ω_{ij} уже известны. Полная процедура AHP требует предварительно определить критерии, сформировать матрицы попарных сравнений, получить вектор приоритетов и проверить согласованность экспертных суждений [19–21]. После этого веса могут быть использованы в оптимизационной модели:

$$max\ \Sigma_i\Sigma_j\ \omega_{ij}\ x_{ij} \quad (7)$$

$$\Sigma_j\ x_{ij} \leq 1; \quad x_{ij} \in \{0,1\} \quad (8)$$

Если AHP используется для оценки компетенций или приоритетов, в статье необходимо привести число экспертов, шкалу сравнений, матрицы, метод агрегации и Consistency Ratio. При CR ≥ 0,10 обычно требуется повторная проверка сравнений [19–21]. Без этих данных воспроизводимость блока распределения ресурсов остается ограниченной.

АНАЛИЗ И РЕЗУЛЬТАТЫ

Исходная работа содержит сравнительные результаты прогностического модуля до и после адаптации. В таблице 3 эти значения сохранены как авторские данные. Они показывают улучшение Precision с 0,87 до 0,95 и Recall с 0,84 до 0,90. Для F1 указано увеличение с 0,85 до 0,93. Однако при вычислении F1 только из округленных Precision=0,95 и Recall=0,90 получается приблизительно 0,924, то есть 0,92 при округлении до двух знаков. Значение 0,93 возможно при использовании неокругленных исходных метрик, поэтому для проверки необходимы исходные predictions или confusion matrix.

Таблица 3.

Результаты, заявленные в исходной статье

Метрика	До адаптации	После адаптации	Комментарий
Precision	0,87	0,95	Приведено в исходной таблице.
Recall	0,84	0,90	Приведено в исходной таблице.
F1	0,85	0,93	Авторское значение; по округленным P/R ≈0,92.

В тексте присутствует также утверждение о точности идентификации более 98% и точности прогнозирования отсутствий 85–90%. В выводах приводятся другие значения: точность идентификации 95%, полнота прогнозирования 92% и F1=0,93. Эти показатели относятся к разным модулям, но границы между ними в исходной версии не обозначены, а часть чисел противоречит друг другу. Поэтому в научной интерпретации их нельзя объединять в единый показатель «эффективности модели». До предоставления протокола эксперимента они рассматриваются как предварительные авторские результаты.

Содержательно модель имеет три сильные стороны. Во-первых,

архитектура разделяет регистрацию событий, анализ посещаемости, прогноз и управленческое действие. Во-вторых, вводится асимметричная стоимость FP и FN, что соответствует практической природе absenteeism prediction. В-третьих, предусмотрено накопление истории и переобучение модели. Однако автоматическая адаптация может ухудшить качество при изменении состава данных или при попадании ошибок разметки в новый обучающий набор, поэтому обновление модели должно сопровождаться контролем drift, сравнением с предыдущей версией и возможностью rollback [12, 13].

Таблица 4.

Основные научно-методические недостатки и способы их устранения

Выявленный недостаток	Почему это важно	Как устранить
Нет размера и структуры выборки	Невозможно оценить статистическую надежность и переносимость.	Указать N работников, период, число смен/событий и prevalence отсутствий.
Нет описания train/validation/test split	Возможна утечка информации между прошлым и будущим.	Применить хронологический split и зафиксировать даты.
Противоречивые метрики	Неясно, какой модуль и на какой выборке оценен.	Разделить identification и absenteeism metrics; приложить confusion matrices.
AHP описан неполно	Невозможно воспроизвести веса.	Добавить критерии, экспертов, pairwise matrices и CR.
Нет PAD-протокола	Face recognition не защищает автоматически от spoofing.	Тестировать PAD отдельно по ISO/IEC 30107-3.
Нет анализа групп пользователей	Средняя метрика может скрывать неодинаковые ошибки.	Проверять FMR/FNMR/Recall по доступным группам при достаточной выборке.
Нет drift governance	Online learning может деградировать после внедрения.	Версионирование, мониторинг, контрольное тестирование, rollback.
Не описана работа с персональными данными	Биометрия и HR-данные требуют специальной защиты.	Указать правовое основание, согласие, цели, сроки хранения и доступ.

Для биометрического модуля исходная формулировка «устойчивость к фальсификациям» является недостаточно измеримой. Стандарт ISO/IEC 30107-3:2023 разделяет тестирование presentation attack detection и обычное биометрическое сопоставление [11]. NIST FATE Part 10 показал, что эффективность программных PAD-алгоритмов существенно зависит от вида presentation attack instrument [14]. Следовательно, для системы посещаемости необходим отдельный PAD-тест, включающий по меньшей мере фотографии, изображения на экране и иные релевантные для выбранного сенсора атаки.

ОБСУЖДЕНИЕ

Полученные результаты показывают, что предложенная архитектура имеет потенциал как система поддержки учета и планирования, но текущая

экспериментальная база недостаточна для утверждения о подтвержденной точности на уровне реального предприятия. Главный научный разрыв заключается не в отсутствии отдельных алгоритмов, а в отсутствии прослеживаемой связи «данные — протокол — модель — метрика — управленческое решение». Пока эта связь не описана, невозможно установить, насколько улучшение связано именно с адаптивным алгоритмом, а не с особенностями выборки или изменением порога классификации.

При прогнозировании отсутствий класс «отсутствие» часто встречается реже класса «присутствие», поэтому высокая Accuracy может быть малоинформативной. Современные исследования absenteeism используют одновременно Precision, Recall, F1 и AUC и отдельно описывают выборку [8, 9]. Для редких событий PR-AUC и Recall положительного класса особенно полезны. Выбор рабочей точки должен исходить из стоимости FN и FP: слишком низкий порог увеличит административную нагрузку ложными уведомлениями, а слишком высокий повысит вероятность пропуска реального кадрового дефицита.

Еще одно ограничение связано с причинной интерпретацией. Модель прогнозирует вероятность отсутствия на основе предыдущих данных, но это не означает, что отдельный признак является причиной отсутствия. Поэтому автоматизированные HR-решения не должны строиться на причинных выводах, которых модель не подтверждает. Целесообразно использовать прогноз для оперативного планирования смен и резервов, а любые дисциплинарные выводы основывать на верифицированных фактах, правилах организации и рассмотрении человеком.

Использование биометрии требует отдельного управления рисками. По Закону Республики Узбекистан «О персональных данных» биометрические данные, используемые для установления личности, имеют специальный режим обработки, а действующая редакция предусматривает обязательное хранение биометрических данных физических лиц на территории Республики Узбекистан [16]. Следовательно, архитектура должна включать разграничение доступа, журналирование, шифрование, минимизацию объема хранимых шаблонов, политику удаления, резервирование и документирование согласий или иных законных оснований. Для облачного развертывания это ограничение необходимо учитывать на стадии проектирования, а не после обучения модели.

Трудовой кодекс Республики Узбекистан требует от работодателя организовать учет рабочего времени [17], но выбор конкретной технологии учета не отменяет требований к корректности данных и правам работников. Рекомендации ILO подчеркивают, что электронный мониторинг должен быть связан с конкретной законной целью, а обработка данных — ограничена необходимым объемом [18]. Поэтому включение активности за компьютером, геолокации или иных дополнительных каналов, упомянутых в исходных рекомендациях, должно проходить отдельную оценку необходимости и пропорциональности; такие данные не следует автоматически добавлять в модель только ради повышения предсказательной точности.

Практически полезной модификацией является введение трех уровней

решения: технический уровень подтверждает валидность события; аналитический уровень оценивает риск отсутствия; управленческий уровень формирует предложение по перераспределению задач. Такой дизайн снижает риск того, что ошибка распознавания лица автоматически приведет к кадровому решению. Для каждого уровня должен существовать собственный журнал событий и возможность аудита.

ЗАКЛЮЧЕНИЕ

В работе усовершенствована математическая постановка автоматизированного мониторинга посещаемости сотрудников, объединяющая RFID, биометрическую верификацию, событийную обработку, прогнозирование отсутствий и распределение ресурсов. Предложено явно разделять четыре результата: подтверждение личности, расчет рабочего времени, прогноз вероятности отсутствия и рекомендацию по распределению задач. Это позволяет назначить каждому модулю собственные входные данные, ошибки и критерии качества.

Анализ исходной экспериментальной части выявил, что приведенные значения Precision, Recall и F1 свидетельствуют о заявленном улучшении после адаптации, однако статья не содержит достаточного описания выборки и протокола для независимого воспроизведения. Дополнительно обнаружено расхождение между показателями, приведенными в основной части и выводах, а также небольшая арифметическая несогласованность F1 с округленными Precision и Recall. До публикации рекомендуется унифицировать метрики и приложить confusion matrix или исходные агрегированные counts.

Методологически уточнено использование AHP: экспертные веса должны формироваться через pairwise comparisons и проверку Consistency Ratio, после чего они могут использоваться в задаче назначения. Для биометрии необходимо отдельно оценивать FMR/FNMR и presentation attack detection; для absenteeism prediction — использовать временное разделение данных, учитывать class imbalance, публиковать ROC-AUC/PR-AUC и контролировать drift после внедрения.

Практическое внедрение системы в Узбекистане должно быть согласовано с требованиями законодательства о персональных данных и рабочего времени. Биометрия, кадровые сведения и прогнозы поведения требуют минимизации данных, контроля доступа, прозрачности целей, регламентов хранения и участия ответственного специалиста при интерпретации сигналов. Дальнейшие исследования целесообразно направить на проспективную апробацию на нескольких предприятиях, проверку переносимости между подразделениями, расчет экономического эффекта и оценку качества системы в реальном эксплуатационном потоке.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Maramis G.D.P., Rompas P.T.D. Radio Frequency Identification (RFID) Based Employee Attendance Management System // IOP Conference Series: Materials

Science and Engineering. 2018. Vol. 306. 012045. DOI: 10.1088/1757-899X/306/1/012045.
2. Zaman H.U., Hossain J.S., Anika T.T., Choudhury D. RFID Based Attendance System // 2017 8th International Conference on Computing, Communication and Networking Technologies (ICCCNT). IEEE, 2017. DOI: 10.1109/ICCCNT.2017.8204180.
3. Meghana I., Meghana J.D.N.V.L., Jayaraman R. Smart Attendance Management System using Radio Frequency Identification // 2020 International Conference on Communication and Signal Processing (ICCSP). IEEE, 2020. DOI: 10.1109/ICCSP48568.2020.9182167.
4. Kumar A., Kumar S., Singh S. Attendance System Based on Biometrics and RFID // 2019 Fifth International Conference on Image Information Processing (ICIIP). IEEE, 2019. DOI: 10.1109/ICIIP47207.2019.8985745.
5. Srinidhi M.B., Roy R. A web enabled secured system for attendance monitoring and real time location tracking using Biometric and RFID technology // 2015 International Conference on Computer Communication and Informatics (ICCCI). IEEE, 2015. DOI: 10.1109/ICCCI.2015.7218103.
6. Chen Y., Li X. Research and Development of Attendance Management System Based on Face Recognition and RFID Technology // 2021 IEEE International Conference on Information Communication and Software Engineering (ICICSE). IEEE, 2021. DOI: 10.1109/ICICSE52190.2021.9404086.
7. RFID Monitoring System Using Machine Learning: A Design Thinking Approach for Smarter Attendance Solutions // 2024 10th International Conference on Advanced Computing and Communication Systems (ICACCS). IEEE, 2024. DOI: 10.1109/ICACCS60874.2024.10717244.
8. Predicting workplace absenteeism using machine learning: a pilot study in occupational health // Journal of Occupational Medicine and Toxicology. 2025. DOI: 10.1186/s12995-025-00482-5.
9. Supporting Sustainable Workforce Management for Worker Illness Absence Through Predictive Analytics // Engineering Proceedings. 2024. Vol. 84, No. 1, Art. 17.
10. ISO/IEC 19795-1:2021. Information technology — Biometric performance testing and reporting — Part 1: Principles and framework. ISO, 2021; corrected version 2024.
11. ISO/IEC 30107-3:2023. Information technology — Biometric presentation attack detection — Part 3: Testing and reporting. ISO, 2023.
12. ISO/IEC 23894:2023. Information technology — Artificial intelligence — Guidance on risk management. ISO, 2023.
13. Tabassi E. Artificial Intelligence Risk Management Framework (AI RMF 1.0). NIST AI 100-1. National Institute of Standards and Technology, 2023. DOI: 10.6028/NIST.AI.100-1.
14. Ngan M.L., Grother P.J., Hom A. Face Analysis Technology Evaluation (FATE) Part 10: Performance of Passive, Software-based Presentation Attack Detection Algorithms. NISTIR 8491. 2023. DOI: 10.6028/NIST.IR.8491.
15. Grother P., Ngan M., Hanaoka K. Face Recognition Vendor Test Part 3: Demographic Effects. NISTIR 8280. National Institute of Standards and Technology,

2019. DOI: 10.6028/NIST.IR.8280.
16. Закон Республики Узбекистан «О персональных данных» от 2 июля 2019 года. Актуальная редакция по состоянию на 2026 год. Национальная база данных законодательства LexUZ.
17. Трудовой кодекс Республики Узбекистан от 28 октября 2022 года. Актуальная редакция по состоянию на 2026 год. Национальная база данных законодательства LexUZ.
18. International Labour Organization. Protection of workers’ personal data: ILO code of practice. Geneva: ILO, 1997.
19. Saaty T.L. The Analytic Hierarchy Process. New York: McGraw-Hill, 1980.
20. Aguarón J., Moreno-Jiménez J.M. The geometric consistency index: Approximated thresholds // European Journal of Operational Research. 2003. Vol. 147, No. 1. P. 137–145.
21. Xu Z., Wei C. A consistency improving method in the analytic hierarchy process // European Journal of Operational Research. 1999. Vol. 116, No. 2. P. 443–449. DOI: 10.1016/S0377-2217(98)00109-X.