**УДК 004.932.72**

***Каракеян А.С.***

***студент***

***Елабужский институт Казанский федеральный университет***

***Россия, г. Елабуга***

# СИСТЕМА ИДЕНТИФИКАЦИИ И УЧЁТА СОТРУДНИКОВ НА ПРЕДПРИЯТИИ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИИ КОМПЬЮТЕРНОГО ЗРЕНИЯ

*Аннотация: в работе рассмотрены положительные и отрицательные аспекты цифровизации биометрии, проанализированы системы идентификации с использованием технологий компьютерного зрения, которые неразрывно связанны с механизмом витальности лица для обеспечения безопасности от мошеннических атак. Показано, что наилучшим решением в программном типе будет одновременное использование двух методов обнаружения, как активного, так и пассивного.*

*Ключевые слова: цифровая биометрия, система идентификации, методы и алгоритмы идентификации*

***Karakeyan A.S.***

***student***

***Yelabuga Institute, Kazan Federal University***

***Russia, Yelabuga***

# THE SYSTEM OF IDENTIFICATION AND ACCOUNTING OF EMPLOYEES AT THE ENTERPRISE USING COMPUTER VISION TECHNOLOGY

*Abstract: the paper examines the positive and negative aspects of the digitalization of biometrics, analyzes identification systems using computer vision technologies that are inextricably linked to the mechanism of facial*

*vitality to ensure security against fraudulent attacks. It is shown that the best solution in the software type would be the simultaneous use of two detection methods, both active and passive.*
*Keywords: digital biometrics, identification system, identification methods and algorithms*

С принятием федеральной программы «Информационное общество» в Российской Федерации [1] была поставлена цель полной цифровизации всех общественно-государственных услуг. В рамках этой программы произошла глобальная автоматизация всех процессов, охватывающих административные и социальные сферы деятельности человека, также она включила в себя и модернизацию системы идентификации и аутентификации личности гражданина. Переход этой системы на электронную платформу обеспечило высокую скорость обработки данных, предотвращение правонарушений, а значит, и повышение общественного порядка, облегчило процесс совершения мелких бытовых покупок. Однако внедрение автоматизированной системы биометрии привело и к появлению новых вызовов, связанных, в первую очередь, с попытками обмана системы.

Рассмотрим автоматизированные системы цифровой идентификации личности на предприятиях. Изучив научные статьи, мы выявили важные положения. Так, в своей работе «Биометрические данные: новые возможности и риски» И. Н. Карцан [2] акцентирует внимание на положительных аспектах автоматизированной цифровой биометрии. Он отмечает, что биометрические данные могут использоваться для создания индивидуальных профилей потребителей, что позволяет компаниям лучше понимать предпочтения и потребности клиентов. Это, в свою очередь, помогает выявлять потенциальные проблемы и принимать меры для их предотвращения. Другой исследователь М. В. Загинайло в статье «Преимущества и недостатки применения биометрических систем в

информационной безопасности» [3] отмечает следующее: биометрические технологии могут значительно улучшить контроль доступа как в физических, так и в цифровых системах. Данные исследования говорят нам, что тема является актуальной и востребованной для изучения. В современной обстановке автоматизированные системы идентификации личности не могут функционировать эффективно без интеграции систем живого обнаружения лица. Только синхронно работая, технологии могут обеспечить надежную защиту на предприятии и минимизировать риски, связанные с использованием биометрических данных. Для большей наглядности рассмотрим некоторые их них.

Face anti-spoofing (liveness detection) – это система, обеспечивающая распознавание настоящего лица от фальшивого, дающая возможность с помощью анализа изображения в видеопотоке определить, используется ли для аутентификации биометрический образец, взятый у живого объекта. На сегодняшний день выделяют в FAS два важных классификатора: аппаратный и программный метод.

Аппаратный метод опирается на необходимость использования дополнительного оборудования в процессе анализа: тепловизионные и 3D камеры. Рассмотрим термальную камеру и принцип её работы. С тепловизионной камеры поступает изображение, в котором каждый пиксель соответствует определенной температуре. Для передачи термограммы на систему liveness detection необходимо преобразовать температурные значения в 8 бит, произвести процесс нормализации, приведение значений пикселей к температурной шкале, где самая низкая температура в фотографии имеет значение 0, самая высокая - 255. Затем производится корректировка данного процесса по значениям температуры в биологически активных точках кожи здорового человека в состоянии покоя в зонах лица (от лобной зоны до области шеи) в пределах диапазона,

где нулевое значение до 28.28±0.71 и максимальное значение от 34.70±0.40 и выше [4].

Тепловизионные регистраторы производят в оптико-механическом конструкторском бюро «Астрон» [5]. Регистратор температуры тела АСТРОН-ПТР2020, компания оснастила дополнительным функционалом – биометрическим распознаванием людей по лицу с помощью технологии Id-Guard, разработанной компанией РекФэйсис.

Программный метод идентификации пользователя представляет собой способ, не требующий привлечения дополнительного оборудования, как правило, в этом случае используется стандартная камера, доступная на самом устройстве. Программный метод обладает удобством и доступностью, а потому он наиболее популярен. Однако программный метод наиболее уязвим к мошенническим атакам: некоторые пользователи начали использовать различные подходы мошенничества, такие как создание масок, видео и фотографий человека. Для того, чтобы с правиться с мошенническими действиями, в 2012 году был создан альянс FIDO (Fast Identify Online), который разрабатывает стандарты аутентификации. FIDO выделяет три основных уровня атак на системы биометрии: level A - использование фотографии лиц на экране электронного устройства или на бумажном носителе (presentation attack), level B - производство бумажных масок с изображение личности, в отношении которого совершается мошенничество, level C - создание 3D-масок из специального материала схожей с кожей человека (presentation attack instrument). Программный метод разделяется на два типа проверки, каждый из которых проходят разные уровни мошеннических атак по FIDO.

I. Первый тип - активный. Особенность его заключается в выполнении определённых действий [6]. Пользователь активно взаимодействует с системрй: воспроизводит голос, меняет мимику, показывает жесты и т.д. Примером такого типа является C2FIV [7].

II. Второй тип – пассивный. Идентификация происходит без активного участия проверяющего, система автоматически анализирует видеопоток и определяет витальность человека на основе предоставленных данных [6]. Одними из популярных анализов в пассивном типе проверки считаются отслеживания моргания глаз, движение губ, сравнение модели с лицом в видеопотоке, изменение эмоций и повороты головы.

Мы рассмотрели различные методы проверки на обнаружение фальсификации биометрического паспорта и теперь у нас есть представление и понимание об аппаратном и программном методе, их особенностях и различии. Согласно описанию, наилучшим общедоступным методом для проверки является программный. Для более высокой точности проверки и идентификации человека, рекомендуется использовать совместно два типа (активный и пассивный).

**Использованные источники:**

1. Постановление Правительства РФ от 15 апреля 2014 г. N 313 Об утверждении государственной программы Российской Федерации «Информационное общество» // СПС «КонсультантПлюс»: сайт. – URL: http://www.consultant.ru (дата обращения: 10.02.2025). – Текст: электронный.

2. Карцан И. Н. Биометрические данные: новые возможности и риски / И. Н. Карцан // Современные инновации, системы и технологии. –2023. – № 3. – С. 0201-0211.

3. Загинайло М. В. Преимущества и недостатки применения биометрических систем в информационной безопасности / М. В. Загинайло, В. В. Каплун. // Молодой ученый. — 2016. — № 30 (134). — С. 73-75.

4. Салимов А. А. Распознавание лиц с помощью тепловизионной камеры / А.А. Салимов, З.А. Алдамова, Л.А. Кромина // Модернизационный потенциал образования и науки как социальных

институтов: сборник научных трудов по материалам Международной научно-практической конференции 11 ноября 2020 г. Белгород: / ООО Агентство перспективных научных исследований (АПНИ). – Белгород, 2020. – С. 17-20.

5. Астрон. Тепловизионные системы: сайт. – Москва, 2022 – URL: https://astrohn.ru (дата обращения: 10.02.2025). – Текст: электронный.

6. Кучер М.Ю. Подходы к распознаванию лиц и их методы / М.Ю. Кучер, Ю.С. Белов // В сборнике: Технические и естественные науки. Сборник избранных статей по материалам Международной научной конференции. – Санкт Петербург, 2020. – С. 38-40.

7. Zheng Sun Concurrent Two-Factor Identify Verification Using Facial Identify and Facial Actions / Sun Zheng, Lee Dah-Jye, Zhang Dong, Li Xiao // in Proc. IS&T Int'l. Symp. on Electronic Imaging: Intelligent Robotics and Industrial Applications using Computer Vision. – 2021. – P. 318-1 - 318-7.