**УДК 004.03**

# МЕТОДЫ И ПРОБЛЕМАТИКА СОВЕРШЕНСТВОВАНИЯ МЕТОДОВ ПОВЫШЕНИЯ БЕЗОПАСНОСТИ СИСТЕМ РАСПОЗНАНИЯ ЛИЦ

**Золотарев К.О.** (Университет ИТМО), **Селин Н.В.** (Университет ИТМО), **Роговой В.** (Университет ИТМО)
**Научный руководитель – к.т.н. Попов И.Ю.** (Университет ИТМО)

В данной работе была исследована и рассмотрена проблематика, появившаяся в связи с бурным развитием мошеннической деятельности в отношении банковского сектора и сектора государственной безопасности с применением новейших технологий подмены лиц и манипуляций с изображением. Были изучены и рассмотрены основные препятствия на пути к получению качественного результата в сфере распознавания подделки лиц, дипфейков и подмены лиц.

**Введение.** В последние годы системы распознавания лиц становятся все более популярной технологией, используемой в различных приложениях, как элемент повышения безопасности, например, аутентификация и идентификация. Однако, как и любая технология, системы распознавания лиц уязвимы для угроз безопасности и атак. Это привело к растущей потребности в методах повышения безопасности систем распознавания лиц.

Одной из ключевых областей, которая была определена как критически важная для безопасности систем распознавания лиц, является распознавание жизненности лиц на изображении. Распознавание жизненности означает способность системы определять, является ли лицо на изображении живым человеком или поддельным изображением лица, например фотографией или маской.

**Основная часть.** Системы биометрии лица превзошли возможности человека в распознавании других людей, это можно объяснить наличием больших наборов данных с метками, которые можно легко получить из Интернета.

Однако изображения попыток подделки обучающих систем для определения живости не находятся в свободном доступе и могут быть получены только вручную. Что создает огромную проблему на пути к развитию технологии [1].

Ручной сбор таких наборов данных — это трудоемкий процесс, который требует от исследовательских групп работы с приглашенными участниками в контролируемых лабораторных условиях, что приводит к ограниченному количеству и разнообразию данных. Это ограничение уменьшает преимущества моделей глубокого обучения, которые эффективны при использовании с большими размеченными наборами данных. Следовательно, необходимы новые подходы для улучшения возможностей обнаружения живости систем распознавания лиц[2].

Одним из таких подходов является использование специальных датчиков, таких как инфракрасные (ИК) камеры и камеры глубины, которые обеспечивают дополнительные возможности для анализа. ИК-камеры могут обнаруживать тепловую энергию, излучаемую живой кожей, что затрудняет копирование лица мошенниками. Кроме того, камеры глубины обеспечивают трехмерное изображение объекта, что упрощает обнаружение поддельных лиц, которым не хватает глубины. Однако, такие технологии требуют специфического оборудования и материального обеспечения, что изначально ограничивает их доступность [3].

Несмотря на огромный прогресс, достигнутый в технологии распознавания лиц, она по-прежнему сталкивается с серьезными проблемами, особенно с точки зрения точности и конфиденциальности. Недавние исследования выявили ограничения систем

распознавания лиц при идентификации людей с более темной кожей по сравнению с людьми со светлой кожей, подчеркнув необходимость повышения производительности при обнаружении разных людей.

**Выводы.** В результате проделанной работы были рассмотрены существующие методы распознавания подделки лиц и проблемы, стоящие на пути получения качественного результата. Рассмотрение основополагающих проблем данных методов позволяет улучшить технологии распознавания подделки биометрических данных (лиц). Также данные проблемы обозначают крайнюю актуальность и востребованность темы и, что она требует дальнейшего углубленного изучения.

**Список использованных источников:**


1. Гринчук О.В., Методы определения подлинности изображения лиц, дис. канд. тех. наук, 05.13.17, защищена 24.12.20, утв. 29.12.20 - М. 2020 113 с.: Библиогр.: с. 107-113 002.073.05
2. Facetec - Liveness detection security report -Q2 2022 [Электронный ресурс] https://www.facetec.com/FaceTec_Liveness_Security_Report_Q2_2022.pdf (Дата обращения 25.02.23)
3. Face Flashing: a Secure Liveness Detection Protocol based on Light Reflections [Электронный ресурс] https://arxiv.org/pdf/1801.01949.pdf (Дата обращения 25.02.23)