

Для цитирования

Николаев Д.Е., Снежкина О.С., Мамаев В.Ю., Кураева Л.Х. Расширенная классификация инструментов атаки на биометрическое предъявление для обеспечения оценки качества и подтверждения соответствия подсистем обнаружения атаки на биометрическое предъявление для модальности лицо / III Научно-практическая конференция «Стандартизация: траектория науки», приуроченная ко Всемирному дню стандартов, Москва, 15 октября 2025 г. // Информационно-экономические аспекты стандартизации и технического регулирования. 2025. № 6(87). С. 721–729.

УДК 57.087.1

**РАСШИРЕННАЯ КЛАССИФИКАЦИЯ ИНСТРУМЕНТОВ АТАКИ
НА БИОМЕТРИЧЕСКОЕ ПРЕДЪЯВЛЕНИЕ ДЛЯ ОБЕСПЕЧЕНИЯ ОЦЕНКИ
КАЧЕСТВА И ПОДТВЕРЖДЕНИЯ СООТВЕТСТВИЯ ПОДСИСТЕМ
ОБНАРУЖЕНИЯ АТАКИ НА БИОМЕТРИЧЕСКОЕ ПРЕДЪЯВЛЕНИЕ ДЛЯ
МОДАЛЬНОСТИ ЛИЦО**

Николаев Д.Е., директор, некоммерческое партнерство «Русское биометрическое общество»; председатель ТК 098 «Биометрия и биомониторинг»; начальник сектора, МГТУ им. Н.Э. Баумана, Москва

Снежкина О.С., руководитель направления по исследованиям и испытаниям перспективных биометрических технологий, Некоммерческое партнерство «Русское биометрическое общество»; инженер, МГТУ им. Н.Э. Баумана, Москва

Мамаев В.Ю., заместитель директора, некоммерческое партнерство «Русское биометрическое общество»; заместитель председателя ТК 098 «Биометрия и биомониторинг»; инженер, МГТУ им. Н.Э. Баумана, Москва

Кураева Л.Х., инженер, МГТУ им. Н.Э. Баумана, Москва

В статье предлагается расширенная классификация инструментов атак на биометрическое предъявление (ИАБП) для обеспечения оценки качества и подтверждения соответствия подсистем обнаружения атак на биометрическое предъявление для модальности лицо. Уровень навыка (компетентность специалиста), а также временных и материальных затрат, требуемых для реализации ИАБП, представленных в данной статье, варьируется в широком диапазоне. Для физических ИАБП предлагаемая классификация учитывает возможные вариации материалов, модификации и способы изготовления. В статье приведены примеры различных видов ИАБП, существующие и успешно реализуемые на сегодняшний день, которые доказали свою эффективность при атаках на действующие биометрические системы, а также мало изученные ИАБП, которые представляют потенциальную угрозу для систем безопасности.

Ключевые слова: информационные технологии, биометрия, атака на биометрическое предъявление, инструменты атак на биометрическое предъявление.

**EXTENDED CLASSIFICATION OF PRESENTATION ATTACK INSTRUMENTS FOR
FACIAL MODALITY TO PROVIDE QUALITY ASSESSMENT AND CONFORMITY
VALIDATION OF BIOMETRIC PRESENTATION ATTACK DETECTION SUBSYSTEMS**

Nikolaev D.E., director, Non-Commercial Partnership «Russian Biometric Society»; chairman of TC 098 «Biometrics and Biomonitoring»; Head of department, Bauman Moscow State Technical University, Moscow
Snezhkina O.S., head of the department for research and testing of promising biometric technologies, Non-Commercial Partnership «Russian Biometric Society»; engineer, Bauman Moscow State Technical University, Moscow

Мамаев В.Ю., deputy director, Non-Commercial Partnership «Russian Biometric Society»; deputy chairman of TC 098 «Biometrics and Biomonitoring»; engineer, Bauman Moscow State Technical University, Moscow
Kuraeva L.Kh., engineer, Bauman Moscow State Technical University, Moscow

The article proposes an extended classification of facial biometric presentation attack instruments (PAI) to provide quality assessment and conformity validation of biometric presentation attack detection (PAD) subsystems. The skill level, as well as the time and material costs required to implement the PAIs presented in this article, vary widely. For physical PAIs, the proposed classification takes into account possible variations in materials, modifications, and creating methods. The article provides an overview of various types of PAIs that exist and are successfully implemented today, which have proven their effectiveness in attacks on existing biometric systems, as well as little-studied PAIs that pose a potential threat to security systems.

Keywords: information technology, biometrics, biometric presentation attack, biometric presentation attack instruments.

Введение

Биометрическое распознавание личности в последнее время получило широкое применение во многих системах обеспечения безопасности: в системах видеонаблюдения, контроля доступа, электронной коммерции, в судебной экспертизе, пограничном контроле, медицине и других областях. Например, современная технология FIDO (Fast Identity Online), которую поддерживает большинство устройств Google, Apple, Microsoft, Huawei и т.д., позволяет аутентифицировать пользователя онлайн с помощью смартфона, что существенно упрощает многие процессы, в которых необходимо подтверждение личности. Главными преимуществами FIDO считаются удобство, защита конфиденциальности и безопасность. Однако несмотря на то, что FIDO, как способ беспарольной аутентификации, действительно решает массовую проблему кражи паролей, он по-прежнему остается уязвимым к атакам на биометрическое предъявление, что повышает риски взлома конкретных устройств.

Биометрические системы, как правило, оснащены подсистемой обнаружения атак на биометрическое предъявление (ОАБП). Главная проблема большинства подсистем ОАБП заключается в том, что испытания этих подсистем проводят на базах данных с простыми, наиболее известными и распространенными видами инструментов атак на биометрическое предъявление (ВИАБП). Так, в аккредитованных NIST лабораториях iBeta и Vixelab при испытаниях используют инструменты атак только 2 уровней (например, в iBeta уровень 1 соответствует стоимости 30\$, уровень 2 – 300\$); соответственно системы, прошедшие испытания в таких лабораториях, с высокой вероятностью уязвимы при использовании злоумышленником более высокотехнологичных ИАБП. Таким образом, количество существующих сегодня ВИАБП значительно больше количества ВИАБП, используемых в испытательных лабораториях. Необходимо учитывать вариации материалов, которые могут быть использованы при подготовке ИАБП (например, различные виды бумаги в случае распечатанных фотографий), способы изготовления и механизацию.

Основная проблематика статьи

В данной работе предлагается расширенная классификация ИАБП для модальности лицо, для создания которых требуется разный уровень навыка (компетентность специалиста), временные и материальные затраты. Предложенная классификация учитывает возможные вариации для наиболее известных ИАБП, а также ИАБП, которые обычно не используются при испытаниях подсистем ОАБП и, как следствие, могут представлять угрозу для современных биометрических систем.

1. Виды ИАБП для модальности лицо

1.1 Распечатанная фотография

Распечатанная фотография является самым распространенным ВИАБП благодаря тому, что он не требует много времени, усилий и материальных затрат для его изготовления. Большинство подсистем обнаружения витальности лица тестируют на базах данных, включающих распечатанные фотографии и различные их модификации (например, распечатанная фотография с вырезанными отверстиями под глаза и/или нос и/или рот,

вырезанное из фотографии изображение очков с глазами, завернутая распечатанная фотография, 2D маска из картона и т. д.). Примеры таких ВИАБП показаны на рис. 1–3.



Рис. 1. Примеры атаки на биометрическое предъявление с применением распечатанной фотографии и модификаций распечатанной фотографии из базы данных WMCA [1]



Рис. 2. Примеры атаки на биометрическое предъявление с применением распечатанной фотографии и модификаций распечатанной фотографии из базы данных ROSE-YouTu [2]



Рис. 3. Пример атаки на биометрическое предъявление с применением 2D маски [3]

Тем не менее при изготовлении данных ВИАБП возможны вариации в материале (картон, разные виды бумаги) и в способе печати (печать на струйном или лазерном принтере, термопринтере), которые редко учитываются при создании базы данных для испытания. В известных публичных базах данных в качестве ИАБП часто представлены распечатанные фотографии, при изготовлении которых были использованы один или два вида бумаги – классическая офсетная офисная бумага А4 и глянцевая фотобумага [4-6]. Однако качество печати и отражательные свойства отличаются для разных видов бумаги: например, для офисной бумаги А4 качество печати скорее всего будет хуже, чем для других видов бумаги, а глянцевой фотобумаге свойственно наличие бликов (рис. 4). Также важно учитывать способ печати, поскольку разрешение печати фотографий на струйном принтере превышает разрешение печати фотографий на лазерном принтере. Таким образом, в рамках ВИАБП распечатанная фотография и 2D маска качество, и соответственно стоимость изготовления могут варьироваться.



Рис. 4. Пример атаки на биометрическое предъявление с применением распечатанной фотографии на разных видах бумаги [4]

Потенциальную угрозу для подсистем ОАБП может также представлять такой подход к изготовлению ИАБП, при котором для печати одной и той же фотографии используют несколько материалов с разным уровнем прозрачности и отражения. В результате совмещения распечатанных изображений получается «многослойное» изображение, которое в сравнении с обычной распечатанной на бумаге фотографией обладает определенным эффектом глубины.

1.2 Фотография/видеозапись на экране внешнего устройства

В современном мире получить цифровое изображение или видеозапись с лицом определенного человека не составляет труда, что делает предъявление фотографии/видеозаписи на экране внешнего устройства второй наиболее распространенной атакой на биометрическое предъявление наряду с распечатанной фотографией и 2D маской. Вместе с тем по сравнению с распечатанной фотографией и 2D маской для реализации данного ВИАБП достаточно только иметь внешнее устройство для демонстрации цифрового изображения без необходимости дополнительных затрат на подготовку.

Фотография/видеозапись на экране внешнего устройства активно применяется в качестве ВИАБП при испытаниях различных подсистем ОАБП. Примеры данного ВИАБП показаны на рис. 5.

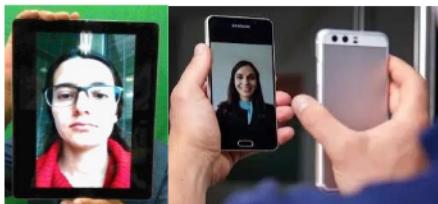


Рис. 5. Примеры атаки на биометрическое предъявление с применением фотографии/видеозаписи на экране внешнего устройства [1, 7]

1.3 Воспроизведение фотографии/видеозаписи с помощью проектора

Для воспроизведения фотографии может быть использован проектор. При этом возможно как воспроизведение фото в пространстве, так и проекция фотографии жертвы на лицо злоумышленника (рис. 6).



Рис. 6. Пример атаки на биометрическое предъявление с применением портативного проектора [8]

1.4 Профессиональный и пластический грим

Для реализации профессионального грима необходимы навыки художника-гримера, особые материалы, а также время на подготовку и нанесение грима, от нескольких часов до нескольких суток. Создание репрезентативной базы данных с высококачественным профессиональным, в том числе пластическим, гримом требует высоких материальных затрат, в связи с чем, несмотря на широкую известность, эти ВИАБП почти не используются при испытаниях современных подсистем ОАБП, а следовательно, могут представлять существенную угрозу для биометрических систем распознавания лица.

Примеры профессионального и пластического грима показаны на рис. 7 и 8.



Рис. 7. Пример профессионального грима, имитирующего разный возраст человека, из базы данных WMCA [1]

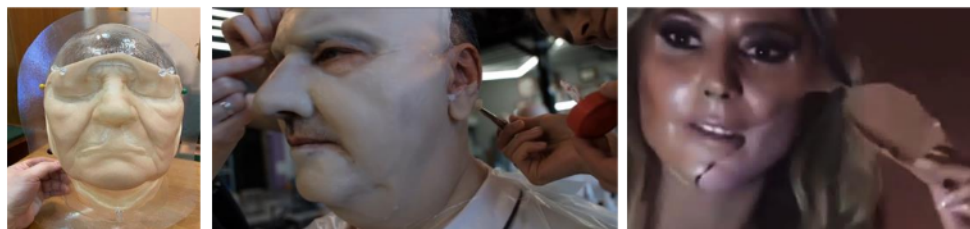


Рис. 8. Пример маски, используемой для пластического грима [9–13] и снятие маски, используемой для пластического грима

1.5 3D маска

Качественно выполненные 3D маски могут с высокой точностью воспроизводить изображение подлинного лица человека, повторяя его форму, текстуру и цвет, из-за чего подсистема ОАБП может принимать такие маски за живого человека.

Стоимость исполнения и уровень детализации для 3D масок могут варьироваться в широком диапазоне. 3D маска может быть изготовлена из бумаги, картона, ткани, латекса, пластика, гипса, силикона. В зависимости от материала изготовления маска может быть жесткой, каркасной или мягкой.

Примеры 3D масок из разных материалов показаны на рис. 9–11.

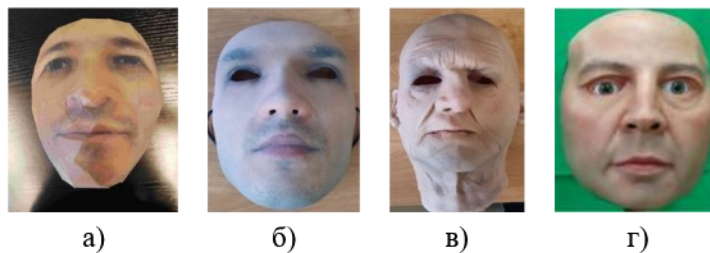


Рис. 9. Примеры 3D маски из разных материалов: а) жесткая из бумаги [1], б) жесткая из пластика [14], в) мягкая из латекса [14], г) мягкая из силикона [15]



Рис. 10. Примеры жесткой 3D маски [16-18]



Рис. 11. Примеры мягких 3D масок с отверстиями для глаз [19]

Изготовление качественной 3D маски требует навыков высокого уровня, большого количества времени и материальных затрат. К показателям качества 3D маски можно отнести эластичный материал и текстуру поверхности, максимально приближенные к человеческой коже, а также отверстия для глаз.

На практике при испытаниях обычно отдают предпочтение простым вариациям 3D масок из недорогих материалов, а более реалистичные и высококачественные 3D маски почти не используют, а значит, подсистемы ОАБП остаются к ним уязвимы.

1.6 3D прототип

3D прототип является одним из наиболее дорогостоящих ИАБП. Несмотря на то, что из-за невозможности надеть ИАБП на себя перечень потенциальных сценариев реализации такой атаки меньше, чем для 3D маски или профессионального грима, в 3D прототипе могут быть реализованы различные варианты механизации, нагрева и т.д., которые позволят обмануть определенные биометрические системы (например, оснащенные датчиком движения или тепловизором).

Для изготовления 3D прототипа может быть использован как один материал, например гипс или пластик, так и комбинация материалов, например с применением силикона для реалистичной имитации человеческой кожи. Примеры 3D прототипа показаны на рис. 12.

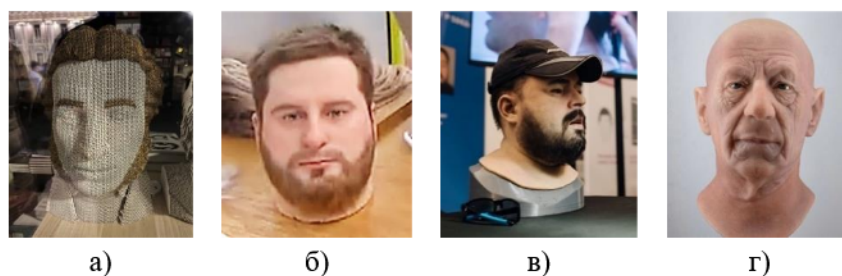


Рис. 12. Примеры 3D прототипа: а) 3D голова, изготовленная из картона, б) 3D голова, изготовленная из силикона [17], в) механизированная 3D голова [9-13], г) 3D голова, изготовленная из воска [20]

1.7 Принуждение

Подсистемы ОАБП в биометрических системах стали стандартным методом противодействия атакам с подменой лица (спуфинг-атакам), и такой сценарий, как принудительное предъявление подлинного лица (например, в состоянии алкогольного/наркотического опьянения, в состоянии седации и т.д.), обычно даже не

рассматривается при проектировании и испытаниях биометрических систем. Как следствие, если злоумышленник принудит законного пользователя пройти аутентификацию в защищенной системе, то он скорее всего обойдет все имеющиеся в системе средства обнаружения атак на биометрическое предъявление.

1.8 Близнецы

Близнецов можно рассматривать как особый случай атаки на биометрическое предъявление. Возможная угроза заключается в том, что один из близнецов может атаковать биометрическую систему, чтобы получить доступ и выдать себя за другого близнеца. Кроме того, близнецы могут легко преодолеть методы ОАБП, поскольку их атака основана на предъявлении лица живого человека. Исследования в этой области показывают, что точное различение однояйцевых близнецов, особенно в неконтролируемых условиях, остается очень сложной задачей [21–23].

1.9 Голова мертвого человека

В определенных сценариях злоумышленник может попытаться получить доступ к системе, предъявив для распознавания биометрические данные мертвого человека. В литературе встречаются упоминания о подобной атаке для таких модальностей, как отпечаток пальца и радужная оболочка глаза [24, 25], однако нельзя исключать потенциальную угрозу применения такого подхода при атаке биометрической системы. ГОСТ Р 58624.1–2019 устанавливает, что биометрические характеристики, полученные от мертвого индивида, относятся к инструментам атаки. Тем не менее более подробно этот ВИАБП в стандарте не рассматривается.

1.10 Пластическая операция

Пластическая хирургия способна в значительной степени изменить исходную биометрическую информацию о лице. На сегодняшний день существуют исследования в данной области, которые подтверждают сложность задачи распознавания лиц, измененных вследствие пластической операции [26, 27].

Таким образом, пластическую операцию можно рассматривать как способ атаки на биометрическое предъявление, которая так же, как и в случае с близнецами, может обойти методы ОАБП, поскольку основана на предъявлении лица живого человека.

1.11 Дипфейк

Предлагаемая классификация не учитывает дипфейки в качестве ИАБП, так как дипфейки относятся к атакам типа «data injection» (инъекционная атака) и будут подробнее рассмотрены в дальнейших исследованиях..

2. Классификация ИАБП для модальности лицо

В данной статье предлагается следующая структура обозначения кода ИАБП:



В структуре обозначения кода ИАБП для модальности лицо используют следующие возможные варианты:

- для кода вида биометрической модальности: Л – лицо;
- кода типа ИАБП: 01 – искусственно созданный; 02 – на основе характеристик человека.

Примечание – Классификация типов приведена с учетом требований ГОСТ Р 58624.1–2019;

- кода вида ИАБП:

- для искусственно созданных ИАБП: 01 – распечатанная фотография, 02 – воспроизведение фотографии/видеозаписи, 03 – 3D;

- для ИАБП на основе характеристик человека: 01 – близнецы, 02 – грим, 03 – принуждение, 04 – пластическая операция, 05 – труп;

- кода группы ИАБП: порядковый номер группы ИАБП определенного вида ИАБП;

- номера ИАБП: порядковый номер ИАБП в группе ИАБП;

- кода общего затрачиваемого времени: 01 – не более одних суток; 02 – от 1 до 7 сут; 03 – от 7 до 14 сут, 04 – от 14 сут до 1 мес, 05 – более 1 мес.

- кода компетентности специалиста: 01 – непрофессионал; 02 – профессионал; 03 – эксперт; 04 – эксперт в нескольких областях знаний/группа экспертов.

Примечание – Классификация кода общего затрачиваемого времени и кода компетентности специалиста приведена с учетом требований ГОСТ Р ИСО/МЭК 18045;

- кода себестоимости изготовления: 01 – очень низкая (менее 1 тыс. руб.); 02 – низкая (от 1 тыс. руб. до 10 тыс. руб.); 03 – средняя (от 100 тыс. руб. до 1 млн руб.); 04 – высокая (более 1 млн руб.).

Заключение

В данной работе предложена расширенная классификация инструментов атак на биометрическое предъявление для обеспечения оценки качества и подтверждения соответствия подсистем ОАБП для модальности лицо, учитывающая ИАБП, для создания которых требуется разный уровень навыка (компетентности специалиста), материальных и временных затрат. Предложенная классификация учитывает возможные вариации для наиболее известных ИАБП, а также ИАБП, которые обычно не используются при испытаниях подсистем ОАБП и, как следствие, представляют угрозу для биометрических систем.

Список литературы / References

1. George A. et al. Biometric face presentation attack detection with multi-channel convolutional neural network // IEEE transactions on information forensics and security. – 2019. – Т. 15. – С. 42–55.
2. Li H. et al. Unsupervised domain adaptation for face anti-spoofing // IEEE Transactions on Information Forensics and Security. – 2018. – Т. 13. – №. 7. – С. 1794–1809.
3. [Электронный ресурс]. URL: <https://www.idrnd.ai/what-is-passive-facial-liveness-and-why-you-shouldnt-use-face-biometrics-without-it/>
4. Tan X. et al. Face liveness detection from a single image with sparse low rank bilinear discriminative model // Computer Vision–ECCV 2010: 11th European Conference on Computer Vision, Heraklion, Crete, Greece, September 5–11, 2010, Proceedings, Part VI 11. – Springer Berlin Heidelberg, 2010. – С. 504–517.
5. Anjos A., Marcel S. Counter-measures to photo attacks in face recognition: a public database and a baseline // 2011 international joint conference on Biometrics (IJCB). – IEEE, 2011. – С. 1–7.
6. Zhang Z. et al. A face antispoofing database with diverse attacks // 2012 5th IAPR international conference on Biometrics (ICB). – IEEE, 2012. – С. 26–31.
7. [Электронный ресурс]. URL: <https://www.bioid.com/2019/07/24/presentation-attack-detection/>.
8. [Электронный ресурс]. URL: <http://jingcailiu.com/wearable-face-projector/>.
9. Николаев. Д.Е. О вопросах безопасности биометрических систем идентификации. Форум «Безопасность информационных технологий в цифровой экономике» (БИТЦЭ–2022). 27 сентября 2022 г. / Nikolaev. Д.Е. "Operations of biometric identification systems." Forum «Improvement of technological information in encryption экономике» (БИТЦЭ–2022). 27 sentiabr 2022 г.
10. Николаев. Д.Е. «Вопросы защиты биометрических систем идентификации от атак на предъявление биометрического образа». Конференция «Доверенный искусственный интеллект–2022». 6 декабря 2022 г. / Nikolaev. Д.Е. «Prosys to use biometric identification systems other than atak na "biometric prediction". Conference «Doverennyy iskusstvennyy intellekt–2022». 6 December 2022

11. Николаев. Д.Е. О вопросах безопасности биометрических систем идентификации. Форум «Цифровая экономика: Технологии доверенного искусственного интеллекта». г. Москва, технологическая долина МГУ «Воробьевы горы». 25 мая 2023 г./
Nikolaev. Д.Е. "Operations of biometric identification systems." Forum «Cypher economics: Технологии доверенного искусственного intellect». г. Moscow, технологическая долина МГУ «Воробьевы горы». May 25, 2023
12. Николаев. Д.Е. Атаки на биометрическое предъявление в биометрических системах идентификации. Конференция «Биометрическое распознавание личности. Перспективы развития в правоохранительной сфере». г. Москва, ГИАЦ МВД РФ. 17 мая 2024 г./
Nikolaev. Д.Е. «Attaki in biometric prediction in biometric systems "identification". Conference «Biometric распознавание личности. Perspektive division into "private sphere". г. Москва, ГИАЦ МВД РФ. May 17, 2024
13. Николаев. Д.Е. Вопросы защиты биометрических систем идентификации от атак на предъявление биометрического образца. Форум «Технологии доверенного искусственного интеллекта». г. Москва, Кластер «Ломоносов». 27 мая 2024 г./
Nikolaev. Д.Е. «Prosys to use biometric identification systems other than atak на «biometric «prediction». Forum «Technology of ancient and intellectual intellect». г. Moscow, Class "Lomonosov". May 27, 2024
14. Kowalski M. A study on presentation attack detection in thermal infrared //Sensors. – 2020. – Т. 20. – №. 14. – С. 3988.
15. Bhattacharjee S., Mohammadi A., Marcel S. Spoofing deep face recognition with custom silicone masks // 2018 IEEE 9th international conference on biometrics theory, applications and systems (BTAS). – IEEE, 2018. – С. 1–7.
16. Цифровой двойник. Какие риски и перспективы существуют у биометрии в России. <https://smotrim.ru/video/2808798/>
Cypher two-way. What risks and perspectives depend on biometrics in Russia. <https://smotrim.ru/video/2808798>.
17. Сбep. <https://smotrim.ru/video/2844859?ysclid=lzh09jliye125652662>.
18. Shuhei Okawara. Фото: Issei Kato. Reuters.
19. [Электронный ресурс] Crea Fx. URL: <https://www.creafox.com/en/>.
20. [Электронный ресурс]. URL: <https://ru.pinterest.com/pin/754915956276469033/>.
21. Phillips P. J. et al. Distinguishing identical twins by face recognition //2011 IEEE International Conference on Automatic Face & Gesture Recognition (FG). – IEEE, 2011. – С. 185–192.
22. Vijayan V. et al. Twins 3D face recognition challenge //2011 international joint conference on biometrics (IJCB). – IEEE, 2011. – С. 1–7.
23. Le T. H. N. et al. Facial aging and asymmetry decomposition based approaches to identification of twins //Pattern Recognition. – 2015. – Т. 48. – №. 12. – С. 3843–3856.
24. Amit Chatterjee, Vimal Bhatia, Shashi Prakash, Anti-spoof touchless 3D fingerprint recognition system using single shot fringe projection and biospeckle analysis, Optics and Lasers in Engineering, Volume 95, 2017, Pages 1–7.
25. Pacut A., Czajka A. Aliveness detection for iris biometrics //Proceedings 40th annual 2006 international carnahan conference on security technology. – IEEE, 2006. – С. 122–129.
26. Singh R. et al. Plastic surgery: A new dimension to face recognition //IEEE Transactions on Information Forensics and Security. – 2010. – Т. 5. – №. 3. – С. 441–448.
27. Singh R. et al. On the robustness of face recognition algorithms against attacks and bias //Proceedings of the AAAI Conference on Artificial Intelligence. – 2020. – Т. 34. – №. 09. – С. 13583–13589.