8. **Zhiting Hu, Xuezhe Ma, Zhengzhong Liu, Eduard Hovy, Eric Xing.** Harnessing Deep Neural Networks with Logic Rules, *Computer Science Learning*. 2016. P. 2410—2420. arXiv: 1603.06318.

9. **Alex Graves, Greg Wayne, Malcolm Reynolds, Tim Harley, Ivo Danihelka, Agnieszka GrabskaBarwinska, Sergio Gómez Colmenarejo, Edward Grefenstette, Tiago Ramalho, John Agapiou** et al. Hybrid computing using a neural network with dynamic external memory, *Nature*, 2016, no. 538 (7626), pp. 471—476.

10. **Shibzuhov Z. M.** O potochechno korrektnyh operacijah nad algoritmami raspoznavanija i prognozirovanija, *Doklady RAN*, 2013, vol. 450, no. 1, pp. 24—27 (in Russian).

11. **Shibzukhov Z. M.** Correct Aggregation Operations with Algorithms, *Pattern Recognition and Image Analysis*, 2014, vol. 24, no. 3, pp. 377—382.

12. **Shibzuhov Z. M.** O nekotoryh konstruktivnyh i korrektnyh klassah algebraicheskih ΣΠ-algoritmov, *Doklady RAN*, 2010, vol. 432, no. 4, pp. 465—468 (in Russian).

13. **Timofeev A. V., Pshibihov V. H.** Algoritmy obuchenija i minimizacii slozhnosti polinomial'nyh raspoznajushhih sistem, *Izvestija AN SSSR. Tehnicheskaja kibernetika*, 1974, no. 7, pp. 214—217 (in Russian).

14. **Timofeev A. V., Ljutikova L. A.** Razvitie i primenenie mnogoznachnyh logik i setevyh potokov v intellektual'nyh sistemah, *Trudy SPII RAN*, 2005, vyp. 2, pp. 114—126 (in Russian).

15. **Ljutikova L. A., Shmatova E. V.** Analiz i sintez algoritmov raspoznavanija obrazov s ispol'zovaniem peremenno-znachnoj logiki, *Informacionnye tehnologii*, 2016, vol. 22, no. 4, pp. 292—297 (in Russian).

16. **Ljutikova L. A.** Ispol'zovanie matematicheskoj logiki s peremennoj znachnost' pri modelirovanii sistem znanij, *Vestnik Samarskogo gosudarstvennogo universiteta. Estestvennonauchnaja serija*, 2008, no. 6 (65), pp. 20—27 (in Russian).

УДК 004.93

С. В. Куликов, науч. сотр., e-mail: kulikov@deepmark.ru,
О. С. Захаров, науч. сотр., e-mail: zakharov@deepmark.ru,
Д. Ю. Андреев, ген. директор, e-mail: andreev@deepmark.ru,
ООО "Лаборатория умных технологий", г. Пенза

Исследование возможности совместного применения нейросетевого преобразователя биометрия—код и глубокой сверточной нейронной сети в распознавании лиц[1]

Проводится анализ возможности использования нейросетевых преобразователей биометрия—код (НПБК), отвечающих требованиям серии стандартов ГОСТ Р 52633, в задаче извлечения стабильного ключа из изображения лица. НПБК используется в качестве последнего слоя заранее обученной глубокой сверточной нейросетевой модели. По методике, соответствующей ГОСТ Р 52633.1—2009, проводится оценка показателей стабильности, уникальности и качества параметров, получаемых на выходе глубокой нейросетевой модели, для анализа возможности обучения НПБК на выходных параметрах глубокой нейросетевой модели. Проведено тестирование ряда конфигураций НПБК (соотношение числа нейронов и числа входов каждого нейрона), выбранных согласно ГОСТ Р 52633.5—2011, и сравнение полученных ROC-кривых с аналогичными кривыми, полученными для шаблонов на базе Евклидова расстояния и машин опорных векторов.

Ключевые слова: *распознавание лиц, криптографический ключ, глубокая сверточная нейронная сеть, нейросетевой преобразователь биометрия-код, НПБК, машина опорных векторов, Евклидово расстояние, показатель уникальности, показатель стабильности, показатель качества, ROC-кривая*

Введение

Глубокие сверточные нейронные сети в настоящий момент не имеют конкурентов в области распознавания лиц. Тем не менее, проблема извлечения стабильного ключа с высокой энтропией из изображения лица остается открытой, хотя необходимость использования глубокой нейронной сети в этой задаче и не вызывает сомнений.

Глубокие сверточные нейронные сети — специальный класс многослойных нейронных сетей, который наиболее широко применяется для распознавания изображений. Такие сети состоят из большого числа слоев, обычно — несколько десятков, и содержат среди прочих слои, применяющие к входным данным операцию свертки.

Существует класс задач, в которых требуется преобразовывать биометрический образ в код, обладающий свойствами криптографического ключа (*biometric encryption*). Возможность получения криптографического ключа из биометрических данных позволяет обеспечивать дополнительную безопасность и обезличенность при организации биометрических систем. В частности, в такой системе база персональных данных, в том числе биометрических, может быть орга-

[1] Работа выполнена при финансовой поддержке Фонда содействия инновациям (договор № 1554ГС1/24419).

низована таким образом, чтобы обеспечить обезличенность путем шифрования всех данных на извлекаемом из биометрических данных ключе. Утечки из такой базы менее опасны, чем из базы с открытым хранением персональных данных (или с шифрованием на мастер-ключе).

Биометрические данные лица человека не исключение, и их тоже используют для получения подобных ключей [1]. Само собой, технология преобразования изображения лица в код более других подвержена атакам с использованием муляжей (фотографий и видеозаписей) [2]. Имея фотографию атакуемого пользователя и зашифрованные персональные данные, злоумышленник имеет возможность расшифровать их, если технология не предусматривает защиту от фотографии на уровне преобразования в код. Теоретическая возможность такой защиты существует, но выходит за рамки этой статьи. В любом случае технология преобразования биометрических данных лиц в код имеет право на существование как минимум в виде составной части мультибиометрических систем.

В России технология преобразования биометрических данных в код попадает под определение "средства высоконадежной биометрической аутентификации" и регламентируется серией стандартов ГОСТ Р 52633. Задачей данной работы является анализ возможности совместного применения глубокой сверточной нейронной сети — де-факто стандарта для распознавания лица, и нейросетевого преобразователя биометрия—код по ГОСТ Р 52633.0—2006 [3]. Критерием возможности совместного применения является снижение/увеличение дифференцирующей способности модели при использовании НПБК, определяемое по *ROC*-кривой (*receiver operating characteristic*), в сравнении с машиной опорных векторов и шаблонами на базе Евклидова расстояния. Для построения *ROC*-кривых проводится численное моделирование работы всех трех вышеупомянутых технологий на тестовой базе лиц объемом 454736 примеров для 10575 субъектов.

1. Архитектура сетей

В качестве глубокой сверточной нейронной сети была выбрана относительно компактная модель со слоями "Max Feature Map" [4]. Архитектура сети была выбрана с тем расчетом, чтобы производительность сети позволяла использовать ее для работы на встраиваемых контроллерах низкой производительности (что является одним из основных применений схем *biometric encryption*) и чтобы получить наиболее практически значимые результаты.

Сеть имеет пять групп слоев, по пять слоев в каждой группе, слой регуляризации *dropout* и слой классификации *softmax* на выходе. Сеть принимает на вход черно-белое изображение лица размером 128×128 пикселей. Перед подачей на глубокую сверточную нейронную сеть лицо проходит процедуру выравнивания по особым точкам (два угла рта, кончик носа, два центра глаз). Для обнаружения лиц на кадрах/фотографиях как в рамках обучения глубокой модели, так и в рамках исследований, описываемых в этой работе, использовали каскадный нейросетевой детектор, аналогичный MtCNN [5]. Выравнивание лица осуществляли по горизонтальной линии глаз, масштаб выбирали пропорционально расстоянию между горизонтальной линией глаз и центром рта (рис. 1, см. третью сторону обложки), положение точки, соответствующей центру рта, не было ограничено вертикальной линией центра изображения.

Для обучения модели была использована собственная база лиц объемом 1,5 млн изображений для 30 тысяч субъектов. Для регуляризации модели при обучении выровненное изображение лица произвольно смещали на ± 8 пикселей по обеим осям и была установлена вероятность выключения нейрона на слое *dropout*, равная 70 %. Полученная за ~ 2 млн итераций сеть имеет показатель EER (вероятность верной классификации при одинаковой вероятности ошибок), равный 98,8 % на базе LFW [6].

Нейросетевые преобразователи биометрия—код в соответствии с ГОСТ Р 52633.0—2006 в качестве входных данных используют "частично случайный вектор входных биометрических параметров", в концепцию которого отлично вписывается дескриптор, получаемый на выходе (точнее, на слое, предыдущем по отношению к слою *softmax*) глубокой нейронной сети. Таким образом, НПБК представляет собой некий аналог шаблона машины опорных векторов, применяемой к выходному дескриптору глубокой нейросетевой модели. НПБК обучается на нескольких примерах образа "Свой" и заданном коде, после чего теоретически должен выдавать максимально случайные выходные коды для образов "Чужой" и заданный код для образов "Свой". Обучение НПБК, а именно — соотношение числа нейронов и числа входов каждого нейрона, процедуру вычисления весов нейронной сети регламентирует ГОСТ Р 52633.5—2011.

В приложении А ГОСТ Р 52633.0—2006 рекомендуется для технологии распознавания лица выбирать длину выходного кода НПБК, равной 7...14 бит. То есть распознавание лица считается слабой технологией, не способной обеспечить достаточно низкую вероятность ошибок второго рода (FPR, *false positive rate*) при приемлемом уровне ошибок первого рода (FNR, *false negative rate*). Это объясняется тем, что ГОСТ Р 52633.0—2006 был написан в 2006 г., когда технологии распознавания лиц были на несколько порядков сла-

бее современных, и с тех пор это приложение стандарта не актуализировалось. Для проведения исследований число нейронов и соответственно длина выходного кода НПБК была выбрана равной 32 и 128 бит. По мнению авторов статьи, современные технологии распознавания лица по вероятностям ошибок находятся на уровне технологий распознавания отпечатка пальца, поэтому целесообразно отойти от устаревших требований стандарта и использовать длину ключа в 32 бита, которая согласно приложению А ГОСТ Р 52633.0—2006 может быть использована для технологии распознавания отпечатка пальца. Длина кода в 128 бит согласно стандарту может применяться только для технологий, содержащих тайный образ (секретную фразу или подпись), и была выбрана для анализа поведения НПБК в условиях, не соответствующих требованиям стандарта, но имеющих определенное практическое применение (криптографические ключи 128 бит могут считаться надежными в определенных условиях, а ключи 7, 14 или 32 бит — определенно нет).

2. Исследование НПБК

Тестирование НПБК проводили на дескрипторах, полученных из выровненных лиц базы CASIA-WebFace. Использовалась очищенная база, содержащая 454736 лиц 10575 субъектов. Зависимость типа *ROC* вероятности действительного положительного решения (TPR, *True Positive Rate*) от ложно-положительного решения (FPR, *False Positive Rate*) для тестовой базы CASIA-WebFace показана на рис. 2.

Согласно приведенной в ГОСТ Р 52633.1—2009 [8] методике расчета для используемой базы был проведен анализ стабильности, уникальности и качества биометрических параметров, используемых в качестве входных параметров НПБК. Гистограммы распределения образов по классам средней стабильности, уникальности и качеству параметров представлены на рис. 3.

Согласно проведенному анализу входных биометрических параметров, показатель среднего качества является низким, однако согласно ГОСТ Р 52633.5—2011 [2], НПБК способен обучаться на низкокачественных входных параметрах при использовании достаточного числа входов у каждого нейрона. Изменяя число входов

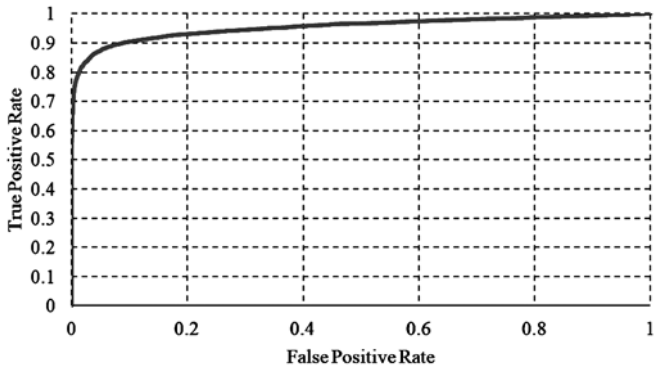

Рис. 2. ROC-кривая для используемой глубокой нейронной сети на базе LFW

у нейрона, можно регулировать значение выходного качества данного нейрона и, следовательно, регулировать вероятность появления ошибок первого (*P*1) и второго рода (*P*2). Чем выше выходное качество нейрона, тем ниже вероятность появления ошибок *P*1 и *P*2.

Согласно ГОСТ Р 52633.5—2011 НПБК может использовать однослойную, либо двухслойную нейронную сеть. Для проведения исследования была выбрана однослойная нейронная сеть с 32 и 128 нейронами. Число входов у нейронов изменялось от 6 до 48. Изменением числа входов у нейронов осуществляется выбор рабочей точки на *ROC*-кривой для НПБК в целом.

Для выбора оптимальной конфигурации сети и исследования зависимости появления ошибок первого и второго рода была проведена серия экспериментов по обучению и тестированию обученной нейронной сети. На каждом шаге задавали число входов у нейрона, генерировалась таблица связей и выполнялось обучение однослойной нейронной сети из 32 или 128 нейронов. Обучение выполнялось для 100 первых субъектов в базе CASIA-WebFace; таким образом, на каждом шаге выполнялось обучение 100 однослойных нейронных сетей. Во время тестирования вычисляли чувствительность алгоритма (TPR) и специфичность алгоритма (FPR). В терминах ГОСТ Р 52633.5—2011 TPR соответствует (1-*P*1), FPR соответствует *P*2. Для вычисления TPR использовали примеры образа "Свой", не участвующие в обучении. Вычисление FPR выполняли на всех образах базы за исключением обучающе-

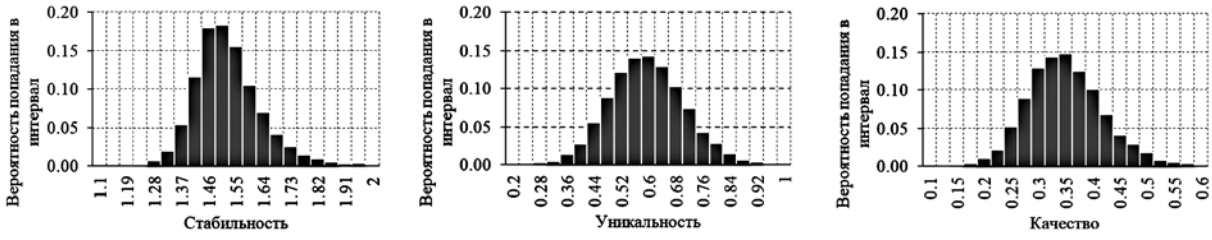

Рис. 3. Распределение образов "Свой" по классам средней стабильности, уникальности, качества параметров

го образа. Зависимость TPR от FPR для разных конфигураций сети (числа входов нейронов) показана на рис. 4 (см. третью сторону обложки).

На рис. 4 показаны четыре группы точек, каждая группа показывает значения TPR и FPR для 100 обучающих образов. Из рис. 4 видно, что при увеличении числа входов нейронов от 12 до 48 происходит увеличение значений TPR и FPR.

На рис. 5 приведена кривая изменения средних значений TPR и FPR для различных конфигураций сети. Точками показаны значения TPR и FPR для различных однослойных нейронных сетей при увеличении числа входов нейронов сети от 12 до 48.

Проведенные эксперименты показали, что для распознавания лиц предпочтительнее использовать сеть, содержащую не 32, а 128 нейронов: сеть с такой конфигурацией показывает лучшую дифференцирующую способность.

Для оценки точности работы НПБК в качестве шаблона аналогичная кривая была построена для машин опорных векторов (SVM) и шаблона, основанного на использовании Евклидова расстояния.

НПБК принимает решение о принадлежности примера образу "Свой", если выходной код совпадает с исходным кодом. Для обучения SVM в качестве негативов (термин "Все Чужие" по ГОСТ Р 52633.0—2006) использовалась база LFW [6]. Использовался не бинарный выход SVM,

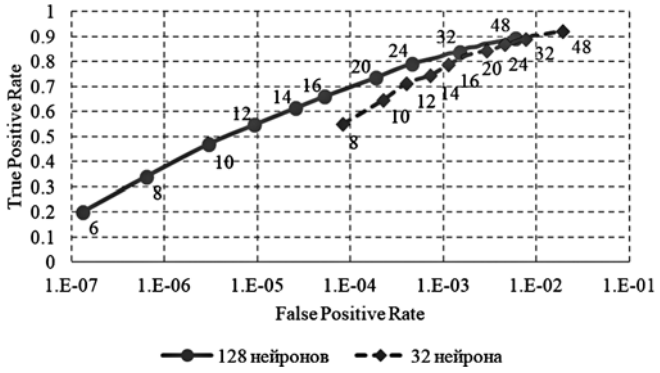

Рис. 5. *ROC*-кривая изменения средних значений TPR и FPR для различных конфигураций сети

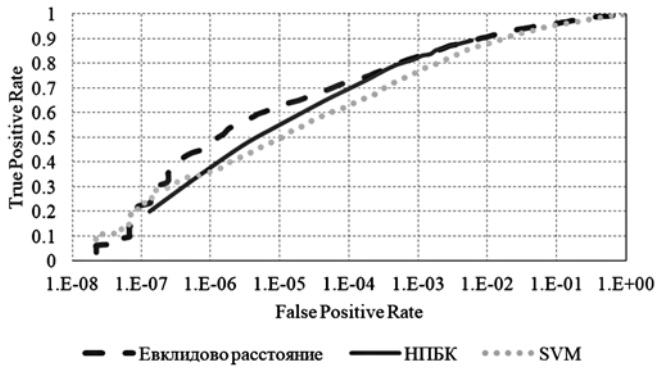

Рис. 6. *ROC*-кривые для трех технологий распознавания лиц

а вероятность принадлежности классу "Свой", решение о принадлежности принималось сравнением вероятности с порогом. Шаблон на базе Евклидова расстояния использовал последнее для определения расстояния между дескриптором рассматриваемого тестового примера и всеми обучающими примерами образа "Свой". Решение о принадлежности к образу "Свой" принималось в зависимости от числа обучающих примеров, расстояние до которых было меньше заданного. Для получения *ROC*-кривой для SVM и шаблонов на базе Евклидова расстояния изменяли порог принятия решения, при этом использовались те же обучающие примеры и те же образы (субъекты базы), что и для тестирования различных конфигураций НПБК. Сравнение *ROC*-кривых НПБК со 128 нейронами с аналогичными кривыми для шаблонов на базе Евклидова расстояния и SVM выполнено на рис. 6.

Заключение

Разрешающая способность НПБК применительно к задаче распознавания лиц в целом оказалась на уровне шаблонов и SVM. Если быть точнее, НПБК показывает несколько большее качество распознавания, чем SVM, при обучении на той же базе негативов. SVM специфична к обучающей базе негативов, при наличии смещения в этой базе относительно условий тестирования разрешающая способность снижается. Этим объясняется лучшее качество распознавания для простых шаблонов на базе Евклидова расстояния относительно и SVM, и НПБК. В то же время НПБК по сути является модифицированной SVM, отличающейся дополнительной регуляризацией — правилом обучения, которое гарантирует равновероятность бинарных значений на выходах нейронов. Дополнительная регуляризация снижает эффект переобучения на базе негативов, что и дает некоторое улучшение качества распознавания по сравнению с обычной SVM.

Что касается длины выходного кода, было установлено что НПБК с кодом длиной 128 бит имеет лучшее качество распознавания, чем с кодом 32 бита. При этом выходной код длиной 128 бит соответствует требованиям ГОСТ Р 52633.0—2006 к качеству выходного "белого шума" НПБК: соблюдается требование к равновероятности состояний и корреляции разрядов выходного кода, это легко объясняется тем, что средний модуль корреляции 256 входных биометрических параметров НПБК, полученных на выходе глубокой сверточной сети, находится на уровне 0,1. Следовательно, положение ГОСТ Р 52633.0—2006, регламентирующее длину ключа для технологии распознавания лица на уровне 7—14 бит как минимум нуждается в пояснении, а более вероятно — в уточнении.

Список литературы

1. **Lu Haiping, Martin Karl, Francis Bui, Plataniotis K. N., Hatzinakos D.** Face recognition with biometric encryption for privacy-enhancing self-exclusion // Digital Signal Processing, 2009 16th International Conference (5—7 July 2009), Santorini-Hellas, Greece. P. 440—450.

2. **Toli C.-A.** Provoking Security: Spoofing Attacks against Crypto-Biometric Systems // World Congress on Internet Security (October 2015), Dublin, Ireland. URL: https://lirias.kuleuven.be/bitstream/123456789/506050/1/Provoking + Security + Spoofing + Attacks + against + Crypto-Biometric + Systems.pdf.

3. **ГОСТ Р 52633.0—2006.** Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации. М.: Гос. стандарт, 2007. 26 с.

4. **Wu Xiang, He Ran, Sun Zhenan, Tan Tieniu.** A Light CNN for Deep Face Representation with Noisy Labels // Chinese Academy of Sciences, Beijing, P. R. China. URL: https://arxiv.org/abs/1511.02683 (дата обращения: 12.08.2017).

5. **Zhang Kaipeng, Zhang Zhanpeng, Li Zhifeng, Qiao Yu.** Joint Face Detection and Alignment using Multi-task Cascaded Convolutional Networks. URL: https://arxiv.org/abs/1604.02878 (дата обращения: 12.08.2017).

6. **Learned-Miller E., Huang B. G., RoyChowdhury A., Li Haoxiang, Hua Gang.** Labeled Faces in the Wild: A Survey. // Advances in Face Detection and Facial Image Analysis, Springer Publishing Company, Incorporated, 2016. P. 189—248.

7. **ГОСТ Р 52633.5—2011.** Защита информации. Техника защиты информации. Автоматическое обучение нейросетевых преобразователей биометрия—код доступа. М.: Гос. стандарт, 2012. 20 с.

8. **ГОСТ Р 52633.1—2009.** Защита информации. Техника защиты информации. Требования к формированию баз естественных биометрических образов, предназначенных для тестирования средств высоконадежной биометрической аутентификации. М.: Гос. стандарт, 2010. 24 с.

S. V. Kulikov, Researcher, e-mail: kulikov@deepmark.ru,
O. S. Zakharov, Researcher, e-mail: zakharov@deepmark.ru,
D. Yu. Andreev, Director, e-mail: andreev@deepmark.ru,
LLC "Laboratoriya umnykh tekhnologiy", Penza, Russia

Exploring the Possibility of Using Deep Convolutional Neural Network Paired with Neural "Biometric Image to Code" Converter in Face Recognition

The article focuses on the possibility of using neural "biometric image to code" converter (NBCC) according to standards GOST R 52633.X in face-based biometric encryption. NBCC is used as last layer in pretrained deep convolutional neural network. The article describes the evaluation of indexes defined in GOST R 52633.1—2009 such as stability, uniqueness and quality of features extracted with deep convolutional neural network to analyze the possibility of training NBCC on features mentioned above. A number of NBCC configurations selected in accordance to GOST R 52633.5—2011 are evaluated and compared by ROC-curves to Euclidian distance based templates and SVMs.

Keywords: *face recognition, biometric encryption, deep convolutional neural network, features, stability index, uniqueness index, quality index, support vector machine, Euclidian distance, ROC-curve*

References

1. **Lu Haiping, Martin Karl, Francis Bui, Plataniotis K. N., Hatzinakos Dimitris.** Face recognition with biometric encryption for privacy-enhancing self-exclusion, *Digital Signal Processing, 2009 16th International Conference, 5—7 July 2009, Santorini-Hellas, Greece*, 2009, pp. 440—450.

2. **Toli C.-A.** Provoking Security: Spoofing Attacks against Crypto-Biometric Systems, *World Congress on Internet Security, October 2015, Dublin, Ireland*, available at: https://lirias.kuleuven.be/bitstream/123456789/506050/1/Provoking + Security + Spoofing + Attacks + against + Crypto-Biometric + Systems.pdf.

3. **GOST R 52633.0—2006.** *Zashhita informacii. Tehnika zashhity informacii. Trebovanija k sredstvam vysokonadezhnoj biometricheskoj autentifikacii* (Information security. Information security technologies. Requirements for highly reliable biometric authentication instruments), Moscow: State standart, 2007, 26 p. (in Russian).

4. **Wu Xiang, He Ran, Sun Zhenan, Tan Tieniu.** *A Light CNN for Deep Face Representation with Noisy Labels*, Chinese Academy of Sciences, Beijing, P. R. China, available at: https://arxiv.org/abs/1511.02683 (date of access: 12.08.2017).

5. **Zhang Kaipeng, Zhang Zhanpeng, Li Zhifeng, Qiao Yu.** *Joint Face Detection and Alignment using Multi-task Cascaded Convolutional Networks*, available at: https://arxiv.org/abs/1604.02878 (date of access: 12.08.2017).

6. **Learned-Miller E., Huang B. G., RoyChowdhury A., Li Haoxiang, Hua Gang.** Labeled Faces in the Wild: A Survey, *Advances in Face Detection and Facial Image Analysis,* Springer Publishing Company, Incorporated, 2016, pp. 189—248.

7. **GOST R 52633.5—2011.** *Zashhita informacii. Tehnika zashhity informacii. Trebovanija k sredstvam vysokonadezhnoj biometricheskoj autentifikacii. Avtomaticheskoe obuchenie nejrosetevyh preobrazovatelej biometrija-kod dostupa* (Information security. Information security technologies. Automating training of neural "biometric image to code" converter), Moscow: State standart, 2012, 20 p. (in Russian).

8. **GOST R 52633.1—2009.** *Zashhita informacii. Tehnika zashhity informacii.* Trebovanija k formirovaniju baz estestvennyh biometricheskih obrazov, prednaznachennyh dlja testirovanija sredstv vysokonadezhnoj biometricheskoj autentifikacii. (Information security. Information security technologies. Requirements for gathering of inartificial biometric datasets, designed for highly reliable biometric authentication instruments evaluation), Moscow: State standart, 2010, 24 p. (in Russian).