УДК 004.056.53 Вестник УрФО № 3(37) / 2020, с. 34–41

Ручай А. Н.

DOI: 10.14529/secur200304

РАЗРАБОТКА ИЗБИРАТЕЛЬНОЙ МУЛЬТИБИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ

Данная работа посвящена разработке избирательной мультибиометрической аутентификации. Новизна работы заключается в разработке нового подхода к мультибиометрической аутентификации. В зависимости от доступности и удобства использования датчиков, от устойчивости к атакам, от болезней или травм пользователей могут быть выбраны любые биометрические характеристики, такие как ритм пароля, голос, динамическая подпись, графический пароль и т.д. В работе представлены результаты разработки избирательной мультибиометрической аутентификации на основе нового подхода.

Ключевые слова: *биометрия, мультибиометрия, мультибиометрическая аутентификация, биометрические технологии, управление доступом, информационная безопасность.*

Ruchay A. N.

DEVELOPMENT OF NEW ELECTIVE MULTIBIOMETRIC AUTHENTICATION

The purpose of this work is the development of elective multibiometric authentication. The novelty of the work is to develop a new approach to multibiometric authentication. Depending on the availability and usability of sensors, from resistance to attacks, from diseases or injuries of users, any biometric characteristics can be selected, such as password rhythm, voice, dynamic signature, graphic password, etc. The paper presents the results of the development of elective multibiometric authentication based on a new approach.

Keywords: *biometrics, multibiometrics, multibiometric authentication, biometric technologies, access control, managing permissions.*

1. Введение

В биометрических системах аутентификации на основе одной биометрической характеристике существуют следующие проблемы [1]:

• Шум в считываемых данных (скопление грязи на датчике, деформированные и зашумленные данные, изменившийся под влиянием холода голос, возможное изменение радужной оболочки глаза под влиянием очков, изменившиеся под влиянием освещенности характеристики лица).

• Не уникальность (внутриклассовые вариации и межклассовое сходство).

• Не универсальность (невозможность использования биометрических характеристик, низкое качество и непротиворечивость полученных биометрических данных, взаимодействие пользователя с датчиком).

• Атаки с обманом.

Разработчики и исследователи обычно предлагают системы аутентификации, использующие одну биометрическую характеристику и один датчик [2], что создает проблемы в использовании и угрозы в безопасности [3]. Однако современные тенденции заставляют использовать другой подход – мультибиометрическую аутентификацию [4], основное преимущество которой состоит в повышении безопасности [5].

Мультибиометрическая аутентификация позволяет использовать несколько биометрических характеристик и датчиков, которые могут быть интегрированы на разных уровнях и могут использоваться в различных сочетаниях [6]. Биометрические характеристики могут обрабатываться различными методами или комбинироваться для мультибиометрической аутентификации. Решение может быть принято на основе объединенного решающего правила, что повышает надежность.

Мультибиометрическая аутентификация имеет высокую безопасность, надежность и защиту от атак [4], для чего используются множество биометрических данных, множество биометрических образцов, множество правил принятия решений, множество методов нормализации или методов извлечения признаков. Однако повышение безопасности и надежности с помощью мультибиометрической аутентификации приводит к дополнительным требованиям к скорости обработки, к неудобствам пользователей и к проблемам с конфиденциальностью. Поэтому при разработке мультибиометрической аутентификации необходимо найти разумный компромисс между надежностью, безопасностью, вычислительными затратами и удобством пользователя. Этот компромисс можно достичь с помощью динамического управления безопасностью и надежностью на основе автоматических или полуавтоматических методов. Однако в работах очень мало внимания уделяется архитектуре, разработке, оценке надежности, безопасности и производительности в подходах динамического изменения безопасности. В разделе 2 данной статьи представлены различные подходы мультибиометрической аутентификации.

В этой статье был разработан подход избирательной мультибиометрической аутентификации, в котором динамически изменяется уровень безопасности путем выбора различных параметров и биометрических характеристик. Предлагаемый подход к избирательной мультибиометрической аутентификации подробно описан в Разделе 3 данной статьи. В рамках предложенного подхода для управления доступом в помещении можно использовать аутентификацию на основе голоса, ритма пароля, клавиатурного подчерка или графического пароля [7, 8]. В другом случае аутентификация может быть выполнена на основе ритма пароля или подписи. Для аутентификации в мобильных устройствах можно применять ритм пароля, подпись или графический пароль. На контрольно-пропускных пунктах может использоваться аутентификация только на основе подписи.

2. Мультибиометрическая аутентификация

Мультибиометрическая аутентификация может использоваться для решения различных аспектов управления безопасностью, основная цель которой является повышение безопасности [4, 5].

Ниже приведены различные подходы к созданию мультибиометрических систем [1]:

• мультимодальность (для идентификации пользователя используется более одной биометрической характеристики).

• мультиалгоритмичность (к одному биометрической характеристики применяется несколько различных подходов для извлечения признаков и алгоритмов сопоставления).

• многоэкземплярность (используется несколько экземпляров одной биометрической характеристики).

• мультисенсорность (информация одной и той же биометрии, полученной с разных сенсоров, объединяется в одну).

• мультивыборность (для регистрации и распознавания используются несколько образцов одной и той же биометрической характеристики).

Мультимодальность может быть реализовано в трех разных режимах [1]:

• Последовательный режим (каскадный режим) – каждая модальность проверяется перед исследованием следующей.

• Параллельный режим – считанные / захваченные данные из нескольких модальностей используются одновременно, а затем результаты объединяются для принятия окончательного решения.

• Иерархический режим – отдельные классификаторы объединяются в иерархию или древовидную структуру.

В мультибиометрической аутентификации существуют следующие различные уровни слияния: на уровне решения, итоговой оценки, характеристик и образцов. Для универсальности должны учитываться всевозможные подходы к реализации мультибиометрии с помощью слияния.

Существует три стратегии мультибиометрического слияния [9]:

• Пользовательская нормализация для мультибиометрического слияния. Например, в зависимости от качества входных образцов предлагаемый алгоритм разумно выбирает подходящий способ слияния для оптимальной эффективности [10].

• Критерий устойчивости для ранжирования пользователей по их эффективности. Он обеспечивает стабильно хорошую эффективность на разных базах данных, несмотря на отсутствие обучающих образцов. Коэффициент Фишера, коэффициент F и d-prime приведены в качестве примеров критериев в [9].

• Избирательная стратегия слияния. Поскольку не все биометрические характеристики должны быть работоспособными для каждой попытки, или необходимо выполнять аутентификацию независимо от устройств или попыток, в этом случае мы должны динамически выбирать соответствующий метод слияния.

В работе [11] была исследована схема динамического слияния динамических оценок для мультиалгоритмического распознавания путем включения качества данных.

В работе [12] авторы предлагают метод последовательного слияния, который использует тест-статистику отношения правдоподобия в сочетании с классификатором машина опорных векторов для учета ошибок. В зависимости от качества входных биометрических данных предлагаемый алгоритм динамически выбирает между различными классификаторами и правилами слияния для распознавания человека по выбранной биометрии.

В статье [13] представлены методы мультибиометрического слияния на ранговом уровне. Предлагаемые методы предлагаются для повышения эффективности схем слияния на уровне рангов при наличии слабых классификаторов или входных изображений низкого качества.

Мультибиометрическая аутентификация должна быть очень гибкой, чтобы учитывать различные требования и ограничения пользователей. При этом она должна решать проблему отсутствия биометрических характеристик в результате низкого качества данных или невозможности предъявления, которая может быть решена с помощью использования других доступных биометрических характеристик. Кроме того, важно соблюдать требование необходимого уровня безопасности, что требует разработки различных динамических избирательных правил и методов мультибиометрического слияния.

В статье [14] описан эксперимент с несколькими простыми методами мультибиометрического слияния. Авторы [15] предложили интересный подход, который включает проведение непрерывной аутентификации. Этот подход требует длительного физического присутствия пользователя и поэтому не подходит для некоторых приложений и ситуаций.

В статье [16] предлагается использовать несколько уровней безопасности для мультибиометрической аутентификации с тремя биометрическими характеристиками (лицо, движение губ, голос). Когда требуемый уровень безопасности низкий, тогда достаточно принять решение на основании двух из трех биометрических характеристик. С другой стороны, для приложений с высоким уровнем безопасности требуется использования всех трех биометрических характеристик. Однако этот подход не позволяет изменять динамически уровень безопасности. Вместо этого администратор принимает решение, в котором должны использоваться конкретные зафиксированные биометрические характеристики.

В работе [17] предлагается сценарий динамического управления доступом в здании с разделением на разные зоны (это могут быть разные этажи или номера комнат) и определенные права доступа для каждого пользователя. Решение доступа в конкретной зоне также могут зависеть от решений, уже принятых в других зонах. Кроме того, количество биометрических характеристик, требуемых в каждой зоне, и различные правила могут варьироваться.

Другим аспектом разработки избирательной мультибиометрической аутентификации является обеспечение желаемой надежности и эффективности, а также выполнения пользовательских предпочтений, ограничений, удобства пользователей и возрастных изменений [18]. Уровень безопасности мультибио-

метрической аутентификации также должен быть скорректирован в зависимости от возможных атак, что требует динамических подходов изменения уровня безопасности.

В работе [19] представлен новый подход к адаптивному комбинированию нескольких биометрических характеристик для динамического обеспечения желаемого уровня безопасности. Работа [19] ориентирована на повышение эффективности и безопасности, хотя одна из ключевых проблем данного подхода связана с правильным выбором биометрических характеристик.

Таким образом, эта данная статья направлена на разработку подхода, в котором адаптивно выбирается набор биометрических характеристик из доступных для обеспечения желаемого уровня безопасности.

3. Избирательная мультибиометрическая аутентификация

В этой статье, в отличие от всех предыдущих работ [20], предлагается новый подход к разработке избирательной мультибиометрической аутентификации, где используется различные критерии выбора параметров и способов мультибиометрической аутентификации. Схема предлагаемой избирательной мультибиометрической аутентификации представлена на рис. 1, на котором показаны основные этапы избирательной мультибиометрической аутентификации, основанной на ритме пароля, голоса, динамической подписи и графического пароля. Этот подход можно использовать и с другими биометрическими характеристиками.

Самым важным блоком для данной схемы является блок полуавтоматических настроек, который выполняет перевод всех настроек и параметров, заданных администратором и пользователем на этапе обучения. В качестве параметров выступает полуавтоматический выбор: последовательности предоставления биометрической характеристики, сам набор биометрических характеристик, устройства ввода (сенсора), метода параметризации, метода сравнения, метода комбинации решения. Здесь под полуавтоматическим выбором понимается выбор метода слияния в виде заранее заданных жестких правил и критериев.

Перечислим базовые критерии и правила [20]:

1. Наличие необходимых устройств ввода (сенсоров);

2. Уровень безопасности (количество необходимых биометрических характеристик);

3. Выбор очередности предоставления биометрических характеристик;

4. Результат предыдущих попыток аутентификации;

5. Особенности данной зоны (комнаты, устройств);

6. Особенности пользователей и их предпочтения, возрастные ограничения;

7. Время прохождения аутентификации;

8. Степень угроз и вероятности атак на устройства ввода (сенсор);

9. Качество предоставляемых биометрических образцов.

Блок полуавтоматических настроек после задания всех настроек и параметров полуавтоматическим способ может выбрать необходимую решающую функцию в блоке комбинация решения $f_1(m1, m2, m3), \ldots, f_k(m1, \ldots, m4)$, где $m1, m2, m3, m4$ – результат сравнения каждой биометрической характеристики в отдельности, и выбрать необходимый порог принятия решения. В предлагаемом подходе параметры для гарантирования определенного уровня безопасности автоматически не подбираются, эта задача стоит для дальнейших исследований.

В предлагаемой нами избирательной мультибиометрической аутентификации есть 4 биометрических характеристики (голос, динамическая подпись, ритм пароля, графическое распознавание). Всевозможные подмножества из этих биометрий могут быть: $\{1,2,3,4\}\{\cdot\}$, $\{1\},\{2\},\{3\}$, $\{4\},\{1,2\}$, $\{1,3\},\{1,4\}$, $\{2,3\},\{2,4\},\{3,4\},\{1,2,3\},\{1,2,4\}$, $\{1,3,4\},\{2,3,4\}$, $\{1,2,3,4\}$.

Каждый из 16 подмножеств описывает один из вариантов выбора биометрических характеристик в избирательной мультибиометрической аутентификации. Опишем алгоритм выбора комбинации биометрических характеристик в зависимости от уровня безопасности.

Пусть набор используемых биометрических характеристик определяется как $\{p_1, p_2, p_3, p_4\}$, , где p_i – индекс использования биометрической характеристики i. Мы предполагаем, что критерии, влияющие на p_i, независимы, поэтому

$$p_i = \prod_{j=1}^{k} p_i^j,$$

где p_i^j – оценка фактора использования биометрической характеристики i с критерием j.

В данной работе были предложены следующие критерии j для каждой биометриче-

ской характеристики i для предлагаемой избирательной мультибиометрической аутентификации:

1. $p^1 = \{0,1\}$ – коэффициент наличия необходимых входных датчиков, когда входной датчик доступен $p^1 = 1$, и когда входной датчик недоступен $p^1 = 0$.

2. $p^2 = [1,10]$ – коэффициент необходимого уровня безопасности. Администратор устанавливает этот коэффициент для каждой биометрической характеристики i. Например, для голосовой аутентификации $p^2 = 10$, для других биометрических характеристик (динамическая подпись, ритм пароля, графическое распознавание) соответственно $p^2 = 3,9,6$.

3. $p^3 = [1,10]$ – коэффициент использования атак на датчик. Администратор устанавливает эту вероятность для каждой биометрической характеристики i. Например, для голоса $p^3 = 3$ из-за высокого риска атак подделки, для других биометрических характеристик (динамическая подпись, ритм пароля, графическое распознавание) соответственно $p^3 = 9,7,6$.

4. $p^4 = [0,1]$ – коэффициент качества биометрических образцов. В зависимости от качества входных выборок предлагаемый алгоритм динамически выбирает подходящий алгоритм слияния для оптимальной эффективности [10, 11, 13].

5. $p^5 = [3,10]$ – коэффициент результата предыдущих попыток аутентификации. Этот коэффициент динамически оценивается. Например, $p^5 = d$, если последние d попытки не прошли аутентификацию.

6. $p^6 = [1,10]$ – коэффициент защищенности помещения (оборудования). Администратор устанавливает этот коэффициент для каждой биометрической характеристики i.

7. $p^7 = [0,1]$ – коэффициент предпочтений пользователя. Администратор устанавливает этот коэффициент для каждого пользователя. Например $p^7 = 0$, из-за возрастных ограничений или отсутствия биометрической характеристики, иначе $p^7 = 1$.

8. $p^8 = [0,10]$ – коэффициент времени на аутентификацию. Например $p^8 = 3$, для голоса из-за длительного процесса, для других биометрических характеристик (динамическая подпись, ритм пароля, графическое распознавание) соответственно $p^8 = 9,7,6$.

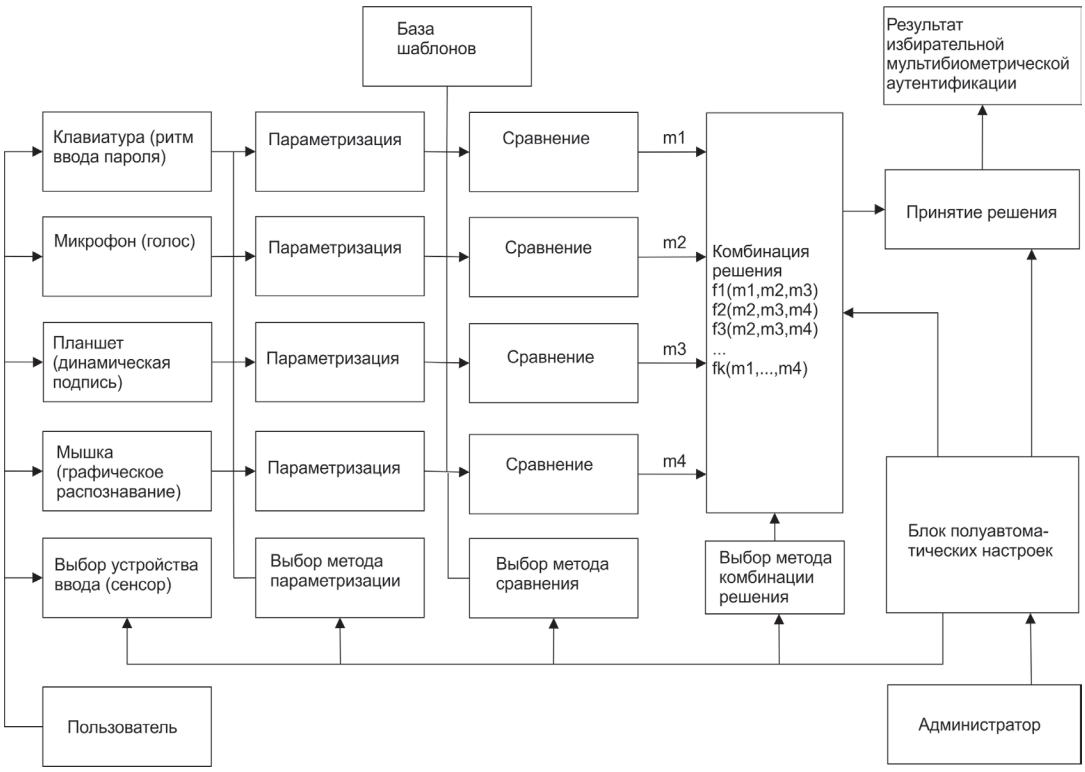

Рис. 1. Схема избирательной мультибиометрической аутентификации

Опишем алгоритм выбора подмножества элементов для предложенной избирательной мультибиометрической аутентификации:

1. Оценим все значения $\{p_1, p_2, p_3, p_4\}$ для всех критериев p^J.

2. Сравним p_i с порогом $\alpha > 0$. Если

$p_i < \alpha$, то исключаем биометрию p_i. Администратор устанавливает порог α.

3. После того, как значения были оценены $\{p_1, p_2, p_3, p_4\}$, мы сортируем p_i.

4. Выбираем первые t, которые соответствуют высоким показателям p_i выбранной биометрической характеристики. Администратор устанавливает параметр t.

В предлагаемой нами избирательной мультибиометрической аутентификации в зависимости от доступности и удобства использования датчиков, от устойчивости к атакам, от болезней или травм пользователей могут быть выбраны любые биометрические характеристики, такие как ритм пароля, голос, динамическая подпись, графический пароль и т.д.

4. Заключение

В работе был разработан новый подход для избирательной мультибиометрической аутентификации. В этом подходе в отличии всех предыдущих работ предлагается различные критерии полуавтоматического выбора метода слияния и параметров мультибиометрической аутентификации. Однако существуют направления для дальнейшего развития избирательного подхода мультибиометрической аутентификации: применение других биометрических характеристик, обеспечение большей универсальности, увеличение эффективности и производительности, реализация динамического выбора параметров системы, в частности, метода слияния для гарантированного уровня безопасности.

Литература

1. Gad, R., El-Fishawy, N., El-Sayed, A., Zorkany, M.: Multi-Biometric Systems: A State of the Art Survey and Research Directions. International Journal of Advanced Computer Science and Applications, 2015, 6(6), P. 128–138.

2. Bolle, R. M., Connell, J. H., Pankanti, S., Ratha, N. K., Senior, A. W.: Guide to biometrics. Springer-Verlag, New-York, 2003.

3. Dunstone, T., Yager, N.: Biometric system and data analysis: design, evaluation, and data mining. Springer, Boston, Ma, 2009.

4. Ross, A. A., Nandakumar, K., Jain A. K.: Handbook of multibiometrics. Springer, New York, 2006.

5. Bhanu, B., Govindaraju, V.: Multibiometrics for Human Identification. Cambridge University Press, Cambridge, 2011.

6. Sesin, E. M., Belov, V. M.: Personal identification system based on integration organization of several biometric characteristics of the person. Proceedings of Tomsk State University of Control Systems and Radioelectronics 2012, 2(25), 2, P. 175–179.

7. Асяев Г.Д., Рагозин А.Н. Определение минимального набора входных данных для корректной аутентификации по клавиатурному почерку с использованием нейронной сети // Вестник УрФО. Безопасность в информационной сфере. 2017. № 3(25). С. 19-23.

8. Иванов А.И., Сомкин С.А., Андреев Д.Ю., Малыгина Е.А. О многообразии метрик, позволяющих наблюдать реальные статистики распределения биометрических данных «нечетких экстракторов» при их защите наложением гаммы // Вестник УрФО. Безопасность в информационной сфере. 2014. № 2 (12). С. 16-23.

9. Poh, N., Ross, A., Lee, W., Kittler, J.: A user-specific and selective multimodal biometric fusion strategy by ranking subjects. Pattern Recognition 2013, 46, P. 3341-3357.

10. Vatsa, M., Singh, R., Noore, A.: Context Switching Algorithm for Selective Multibiometric Fusion. Pattern Recognition and Machine Intelligence 5909, Springer, 2009. P. 452–457.

11. Fathima, A., Vasuhi, S., Treesa, T., Babu, N.T., Vaidehi, V.: Person Authentication System with Quality Analysis of Multimodal Biometrics. WSEAS transactions on information science and applications.

12. Vatsa, M., Singh, R., Noore, A., Ross, A.: On the Dynamic Selection of Biometric Fusion Algorithms. IEEE transactions on information forensics and security 2010, 5(3). P. 470–479.

13. Abaza, A., Ross, A.: Quality Based Rank-Level Fusion in Multibiometric Systems. Proc. of 3rd IEEE International Conference on Biometrics: Theory, Applications and Systems (BTAS), 2009.

14. Kittler, J., Hatef, M., Duin, R. P. W., Matas, J.: On combining classifiers. IEEE Trans. Patt. Anal. Machine Intell. 1998, 20. P. 226–239.

15. Sim, T., Zhang, S., Janakiraman, R., Kumar, S.: Continuous verification using multimodal biometrics. IEEE Trans. Patt. Anal. Machine Intell. 2007, 29(4), P. 687–700.

16. Frischholz, R. W., Deickmann, U.: BioID: a multimodal biometric identification system. IEEE Comput. 2000, 33(2).

17. Bradlow, E. T., Everson, P. J.: Bayesian inference for the beta-binomial distribution via polynomial expansions. J. Comput. Graphical Statistics, 2002, 11(1). P. 200–207.

18. Poh, N., Wong, R., Kittler, J., Roli, F.: Challenges and research directions for adaptive biometric recognition systems. Proc. ICB, Alghero, Italy. 2009.

19. Kumar, A., Kanhangad, V. Zhang, D.: A new framework for adaptive multimodal biometrics management. IEEE Transactions on Information Forensics and Security. 2010, (5). P. 92–102.

20. Ручай А.Н., Кузнецов В.В., Мельников А.В., Вохминцев А.В. Разработка централизованной системы избирательной мультибиометрической аутентификации // Информационные технологии и вычислительные системы. №1. 2016. С. 106-116.

21. Ruchay A. An elective multibiometric authentication // CEUR Workshop Proceedings, vol. 1710, 2016. P. 292-302.

References

1. Gad, R., El-Fishawy, N., El-Sayed, A., Zorkany, M.: Multi-Biometric Systems: A State of the Art Survey and Research Directions. International Journal of Advanced Computer Science and Applications, 2015, 6(6), P. 128–138.

2. Bolle, R. M., Connell, J. H., Pankanti, S., Ratha, N. K., Senior, A. W.: Guide to biometrics. Springer-Verlag, New-York, 2003.

3. Dunstone, T., Yager, N.: Biometric system and data analysis: design, evaluation, and data mining. Springer, Boston, Ma, 2009.

4. Ross, A. A., Nandakumar, K., Jain A. K.: Handbook of multibiometrics. Springer, New York, 2006.

5. Bhanu, B., Govindaraju, V.: Multibiometrics for Human Identification. Cambridge University Press, Cambridge, 2011.

6. Sesin, E. M., Belov, V. M.: Personal identification system based on integration organization of several biometric characteristics of the person. Proceedings of Tomsk State University of Control Systems and Radioelectronics 2012, 2(25), 2, P. 175–179.

7. Asyayev G.D.. Ragozin A.N. Opredeleniye minimalnogo nabora vkhodnykh dannykh dlya korrektnoy autentifikatsii po klaviaturnomu pocherku s ispolzovaniyem neyronnoy seti // Vestnik UrFO. Bezopasnost v informatsionnoy sfere. 2017. № 3(25). S. 19-23.

8. Ivanov A.I.. Somkin S.A.. Andreyev D.Yu.. Malygina E.A. O mnogoobrazii metrik. pozvolyayushchikh nablyudat realnyye statistikiraspredeleniya biometricheskikh dannykh “nechetkikh ekstraktorov”pri ikh zashchite nalozheniyem gammy // Vestnik UrFO. Bezopasnost v informatsionnoy sfere. 2014. № 2 (12). S. 16-23.

9. Poh, N., Ross, A., Lee, W., Kittler, J.: A user-specific and selective multimodal biometric fusion strategy by ranking subjects. Pattern Recognition 2013, 46, P. 3341-3357.

10. Vatsa, M., Singh, R., Noore, A.: Context Switching Algorithm for Selective Multibiometric Fusion. Pattern Recognition and Machine Intelligence 5909, Springer, 2009. P. 452–457.

11. Fathima, A., Vasuhi, S., Treesa, T., Babu, N.T., Vaidehi, V.: Person Authentication System with Quality Analysis of Multimodal Biometrics. WSEAS transactions on information science and applications.

12. Vatsa, M., Singh, R., Noore, A., Ross, A.: On the Dynamic Selection of Biometric Fusion Algorithms. IEEE transactions on information forensics and security 2010, 5(3). P. 470–479.

13. Abaza, A., Ross, A.: Quality Based Rank-Level Fusion in Multibiometric Systems. Proc. of 3rd IEEE International Conference on Biometrics: Theory, Applications and Systems (BTAS), 2009.

14. Kittler, J., Hatef, M., Duin, R. P. W., Matas, J.: On combining classifiers. IEEE Trans. Patt. Anal. Machine Intell. 1998, 20. P. 226–239.

15. Sim, T., Zhang, S., Janakiraman, R., Kumar, S.: Continuous verification using multimodal biometrics. IEEE Trans. Patt. Anal. Machine Intell. 2007, 29(4), P. 687–700.

16. Frischholz, R. W., Deickmann, U.: BioID: a multimodal biometric identification system. IEEE Comput. 2000, 33(2).

17. Bradlow, E. T., Everson, P. J.: Bayesian inference for the beta-binomial distribution via polynomial expansions. J. Comput. Graphical Statistics, 2002, 11(1). P. 200–207.

18. Poh, N., Wong, R., Kittler, J., Roli, F.: Challenges and research directions for adaptive biometric recognition systems. Proc. ICB, Alghero, Italy. 2009.

19. Kumar, A., Kanhangad, V. Zhang, D.: A new framework for adaptive multimodal biometrics management. IEEE Transactions on Information Forensics and Security. 2010, (5). P. 92–102.

20. Ruchay A.N.. Kuznetsov V.V.. Melnikov A.V.. Vokhmintsev A.V. Razrabotka tsentralizovannoy sistemy

izbiratelnoy multibiometricheskoy autentifikatsii // Informatsionnyye tekhnologii i vychislitelnyye sistemy. №1. 2016. S. 106-116.

21. Ruchay A. An elective multibiometric authentication // CEUR Workshop Proceedings, vol. 1710, 2016. P. 292-302.

РУЧАЙ Алексей Николаевич, кандидат физико-математических наук, доцент, заведующий кафедрой компьютерной безопасности и прикладной алгебры, Челябинский государственный университет. 454001, Челябинск, ул. Братьев Кашириных, 129.; доцент кафедры защиты информации, Южно-Уральский государственный университет (национальный исследовательский университет). 454080, г. Челябинск, пр. им. В.И. Ленина, 76. E-mail: ran@csu.ru.

RUCHAY Alexey Nikolaevich, PhD in Physics and Mathematics, Associate Professor, Head of the Department of Computer Security and Applied Algebr, Chelyabinsk State University. 454001, Chelyabinsk, st. Kashirin Brothers, 129.; Associate Professor, Department of Information Security, South Ural State University (National Research University). 454080, Chelyabinsk, etc. them. IN AND. Lenin, 76. E-mail: ran@csu.ru.