УДК 004.93:57.087.1

БИОМЕТРИЧЕСКИЕ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: КЛАССИФИКАЦИЯ И АКТУАЛЬНЫЕ НАПРАВЛЕНИЯ РАЗВИТИЯ

Т.А. Ткалич[1], К.А. Забродская[2], В.В. Шишко[3], В.И. Рымжа[4]
[1-4] Белорусский государственный экономический университет,
г. Минск, Республика Беларусь

В статье определены сущность, особенности и критерии классификации биометрических систем информационной безопасности, представлена характеристика основных способов биометрической идентификации, выявлены актуальные направления их развития.
Ключевые слова: *защита; информация; безопасность; биометрическая система; идентификация, развитие.*

В современных условиях развития глобального информационного общества и цифровой экономики одной из важнейших проблем, связанных с внедрением инфокоммуникационных технологий в различных областях деятельности, является надежная защита информационных ресурсов (ИР) и информационно-коммуникационной инфраструктуры, обеспечение информационной безопасности (ИБ) конфиденциальных данных. Существующие в настоящее время системы защиты все чаще оказываются бессильными перед множеством потенциальных угроз ИБ, что актуализирует поиск новых и более надежных решений в области управления доступом к информации.

Перспективным инструментом защиты данных является ***биометрическая система*** (БС) информационной безопасности[1-7], которая позволяет автоматизировать сбор биометрических образцов, обработать, сравнить и определить вероятность совпадения биометрических данных с биометрическими шаблонами и определить успешность идентификации личности или проверки подлинности по уникальным индивидуальным физическим признакам (характеристикам), которые должны быть характерными, повторяющимися, доступными для устройств записи, приемлемыми, универсальными [4].

Любая биометрическая система выполняет следующие функции: *регистрация* – сбор биометрических образцов от конечного пользователя, подготовка и хранение биометрических контрольных шаблонов и других данных, связанных с личностью пользователя; *верификация* – сравнение биометрического образца с биометрическим шаблоном в режиме «один-к-одному» и возврат результата в виде решения о совпадении; *идентификация* – поиск «один-ко-многим» для получения списка

кандидатов и *аутентификация* – подтверждение подлинности пользователя БС [4, 6]. Точность биометрической верификации и идентификации характеризуется такими показателями как *коэффициент ложного доступа* (False Acceptance Rate, FAR, ошибка первого рода – вероятность ошибочного принятия заявленной личности мошенника за истинную), *коэффициент ложного отказа доступа* (False Reject Rate, FRR, ошибка второго рода – вероятность ошибочного отказа подлинной личности) [1, 2].

Биометрическая система состоит из двух частей: аппаратных средств и специального прикладного программного обеспечения. ***Архитектура типовой биометрической системы*** включает подсистемы сбора, передачи, обработки, хранения и сопоставления данных, принятия решений, управления (администрирования), аппаратный и программный интерфейс приложений. Назначение составных компонент БС описано в стандарте [4].

Анализ публикаций и стандартов по теме исследования [1-7] позволил систематизировать ***критерии классификации БС:***

- ***по категории конечных пользователей*:** БС для частных и корпоративных потребителей [1-4];
- ***по решаемым задачам*:** БС регистрации, верификации, идентификации и аутентификации [4];
- ***по способу управления:*** автономные, централизованные, универсальные [1];
- ***по функциональным характеристикам:*** БС с ограниченными функциями, БС с расширенными функциями, многофункциональные системы [1];
- ***по количеству одновременно анализируемых биометрических признаков и биометрическому объединению*** данных от различных источников: монобиометрические системы и мультибиометрические системы (мультимодальные, мультиэкземлярные, мультиалгоритмические, мультипредставление, мультидатчиковые БС) [5];
- ***по алгоритмам обработки биометрических образцов:*** моноалгоритмические и мультиалгоритмические БС;
- ***по принципу действия:*** статические БС, основанные на анализе биологических характеристик, данных человеку при рождении, и динамические БС, основанные на характеристиках, которые могут изменяться со временем и зависят от особенностей поведения [1-6];
- ***по типам биометрических признаков*:**
  - *на основе отпечатков пальцев (дактилоскопия)* – преобразование изображения пальца в цифровой код и сравнение с эталонным шаблоном базы данных; преимущества: легкий ввод идентификационных данных, наличие большого количества идентификаторов (10 пальцев рук),

компактное сканирующее оборудование, высокое соотношение цена/надежность; недостатки: возможность отсутствия пригодных для идентификации отпечатков, повреждения или потери пальца, изготовление муляжа [2-4];

- *на основе геометрии руки* – сравнение трехмерного рисунка информационных знаков кисти с рисунками базы данных; преимущества: простота технологии идентификации, отсутствие требований к чистоте, температуре и влаге ладони; недостатки: контактный способ считывания биометрических характеристик, высокий уровень ошибок, отсутствие у некоторых людей пальцев или ладони [2-4];
- *на основе радужной оболочки глаз* – цифровое преобразование и сравнение видеоизображения радужки глаза с базой данных; преимущества: независимость от внешних факторов, высокая точность, отсутствие негативных ассоциаций у населения, бесконтактный способ идентификации; недостатки: малочисленность баз данных, дорогостоящее оборудование [2-4];
- *на основе формы лица* – цифровое преобразование 3D-изображения лица, контуров глаз, губ, носа и других характеристик; преимущества: бесконтактный и незаметный способ идентификации, быстрая обработка данных; недостатки: большая зависимость от внешних факторов (освещенность, ракурс, возраст), высокий процент ошибок, изменение лица с течением времени, сложность реализации системы [2-4];
- *голосовая биометрия* – применение частотных методов или линейных предсказателей речевого сигнала; преимущества: возможность дистанционной идентификации, низкая стоимость реализации, привычный для населения способ; недостатки: проблема сохранения парольной фразы в тайне, влияние множества факторов (интонация, скорость речи, болезни, психологическое состояние клиента) на качество распознавания и высокий уровень ошибок [2-4];
- *на основе динамического ввода подписи* – построение цифрового кода по динамическим характеристикам подписи (силе натиска на поверхность, графическим параметрам, скорости нанесения подписи); преимущества: простота и доступность использования, сложность подделки, доступность процедуры; недостатки: зависимость параметров от психофизиологического состояния людей и стабильности их почерка [2-4];

- ***по биометрической модальности*:** традиционные, нетрадиционные, мультимодальные БС [2, 5];
- ***по аппаратным средствам:*** БС с применением сканеров и применением терминалов [1-7];
- ***по технологиям считывания и записи биометрических характеристик:*** оптоэлектронные, полупроводниковые, ультразвуковые, пироэлектрические, электрооптические, телевизионные, тепловизионные, мультидатчиковые [1, 3];

- ***по сфере применения:***
  - *БС в области охраны правопорядка* – автоматическая мультибиометрическая идентификация, основанная на применении специализированных сканеров отпечатков пальцев, мобильных терминалов; контроль доступа [2, 3, 7];
  - *БС в финансовой и банковской сфере* – биометрическая идентификация, основанная на применении встраиваемых оптических сканеров отпечатков пальцев для интеграции с банкоматами, платежными терминалами; банковскими информационными системами [2, 3, 7];
  - *БС в сфере образования* – комплекс прикладных биометрических решений для интеграции функций биометрической идентификации в прикладные программные продукты, используемые в кафетериях, столовых, библиотеках; применение биометрической идентификации для защиты данных в компьютерных сетях образовательных учреждений, повышения эффективности всех ключевых процессов деятельности образовательных учреждений (регистрация прихода-ухода учащихся, удостоверение личности сдающих экзамены и зачеты, мультибиометрическая идентификация удостоверения абитуриентов и студентов вузов) [2, 3, 7].
  - *БС в сфере торговли и сервиса* – учет рабочего времени и контроля доступа; применение автоматической мультибиометрической идентификации в программах лояльности клиентов и ключевых процессах обслуживания покупателей, интеграция функций БС в прикладные программные продукты, используемые в деятельности предприятий торговли и сервиса [2, 3, 7].
  - *БС медицины* – защита медицинских информационных систем от несанкционированного доступа, обеспечение целостности медицинских документов, аутентификация, протоколирование и аудит действий пользователей медицинской биометрической системы [2, 3, 7].

Следует отметить, что способы биометрической идентификации постоянно развиваются: разрабатывается не только новое оборудование, способствующее снижению ошибок, но и новые методы определения личности. Спектр технологий, которые могут использоваться в системах ИБ, постоянно расширяется. По мнению экспертов [2] перспективными биометрическими технологиями идентификации личности являются:

- термограммы лица в инфракрасном диапазоне излучения;
- анализ формы ушной раковины;
- анализ характеристик ДНК;
- спектроскопия кожи;
- анализ отпечатков ладоней;
- анализ характеристик походки человека;
- распознавание по уровню солености кожи;

- анализ индивидуальных запахов человека;
- распознавание по расположению вен [2].

Анализ рынка БС показал, что наибольший интерес для конечного пользователя представляют биометрические технологии идентификации и управления доступом на основе отпечатков пальцев, голоса и подписей. В ближайшем будущем индивидуальным биометрическим удостоверением личности будет обеспечен каждый пользователь. Сравнение идентификаторов будет происходить в режиме реального времени посредством сети Интернет [7]. Специалисты считают, что актуальным направлением развития биометрических систем является мультибиометрия [5], позволяющая увеличить скорость, повысить производительность БС и уменьшить число ошибок идентификации личности в сравнение с одним биометрическим идентификатором.

Таким образом, внедрение биометрических систем в настоящее время становится достойной альтернативой классическим методам защиты информации и является фактором, значительно влияющим на конкурентоспособность организации.

Список литературы

1. Болл Руд М. Руководство по биометрии / Болл Руд М., Коннел Джонотан Х, Панканти Шарат, Ратха Налина К., Сеньор Эндрю У. – Москва: Техносфера, 2007. – 368 с.
2. Традиционные методы биометрической аутентификации и идентификации: учеб. электрон. издан. / В.М. Колешко, Е.А. Воробей, П.М. Азизов, А.А. Худницкий, С.А. Снигирев. – Минск: БНТУ, 2009. – 107 с.
3. Досжанова А.А. Модели и алгоритмы обработки информации в биометрико-нейросетевых системах обезличивания электронных историй болезней: дис. … докт. Философии. – Алматы: Казахск. нац. техн. ун-т им. К.И. Сатпаева, 2014. – 115 с.
4. Информационные технологии. Биометрия. Обучающая программа по биометрии: ГОСТ ISO/IEC 54412-2011/ISO/IEC/TR24741:2007. – Введ. 21.09.2011. – М: Стандартинформ, 2012. – 56 с.
5. Информационные технологии. Биометрия. Мультимодальные и другие мультибиометрические технологии. 54411-2011/ISO/IEC/TR 24722:2007. – Введ. 21.09.2011. – М: Стандартинформ, 2014. – 32 с.
6. Информационные технологии. Биометрические профили для взаимодействия и обмена данными. Часть 1. Общая архитектура биометрической системы и биометрические профили: Межгосударственный стандарт ГОСТ ISO/IEC 24713-1–2013. Введ. 21.09.2013. – М: Стандартинформ, 2014. – 24 с.
7. Отрасли, сегменты, сектора [Электронный ресурс]. - ООО «Биолинк Солюшенс», 2015. – Режим доступа: http://www.biolink.ru/solutions/markets/ (дата обращения 07.05.2016).

BIOMETRIC INFORMATION SECURITY SYSTEMS: CLASSIFICATION AND ACTUAL DIRECTIONS OF DEVELOPMENT

T.A. Tkalich[1], K.A. Zabrodskaya[2], V.V. Shishko[3], V.I. Rymzha[4]
[1-4] UO "Belarusian State Economic University", Minsk, Belarus

The article defines the nature, characteristics and classification features of biometric information security systems, with the characteristics of the main methods of biometric identification, identified current trends of their development.
Keywords: *protection; information; security; biometric system; identification.*

Об авторах:
ТКАЛИЧ Татьяна Алексеевна – доктор экономических наук, доцент, профессор кафедры информационных технологий, УО «Белорусский государственный экономический университет» (220070, Минск, пр-т Партизанский, 26), e-mail: informatika@tut.by
ЗАБРОДСКАЯ Кристина Адамовна – ассистент кафедры информационных технологий, УО «Белорусский государственный экономический университет» (220070, Минск, пр-т Партизанский, 26), e-mail: z_k@tut.by
ШИШКО Виктория Витальевна – студентка факультета международных экономических отношений, УО «Белорусский государственный экономический университет» (220070, Минск, пр-т Партизанский, 26), e-mail: vic-shic96@mail.ru
РЫМЖА Вероника Игоревна – студентка факультета международных экономических отношений, УО «Белорусский государственный экономический университет» (220070, Минск, пр-т Партизанский, 26), e-mail: veranika.rymzha@gmail.com

About authors:
TKALICH Tatyana Alekseevna is the Doctor of Economics, the associate professor, professor of department of information technologies, UO "Belarusian State Economic University" (220070, Minsk, Partizansky Ave, 26), e-mail: informatika@tut.by
ZABRODSKAYA Kristina Adamovna is the assistant to department of information technologies, UO "Belarusian State Economic University" (220070, Minsk, Partizansky Ave, 26), e-mail: z_k@tut.by
SHISHKO Victoria Vitalyevna is the student of faculty of the international economic relations, UO "Belarusian State Economic University" (220070, Minsk, Partizansky Ave, 26), e-mail: vic-shic96@mail.ru
RYMZHA Veronika Igorevna is the student of faculty of the international economic relations, UO "Belarusian State Economic University" (220070, Minsk, Partizansky Ave, 26), e-mail: veranika.rymzha@gmail.com