

РАЗРАБОТКА И АНАЛИЗ КОНЦЕПТУАЛЬНОЙ МОДЕЛИ БИОМЕТРИЧЕСКОЙ ИНФОРМАЦИИ С ТОЧКИ ЗРЕНИЯ ДЕЙСТВУЮЩЕЙ НОРМАТИВНО-ПРАВОВОЙ БАЗЫ

Сергей Владимирович Шуругин

Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, магистрант кафедры фотоники и приборостроения, тел. (953)776-94-51, e-mail: sshurugin97@mail.ru

Ариф Уратович Матвеев

Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, магистрант кафедры фотоники и приборостроения, тел. (999)463-43-96, e-mail: arifan.matveev@mail.ru

Евгений Владимирович Грицкевич

Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, кандидат технических наук, доцент кафедры информационной безопасности, тел. (383)343-91-11, e-mail: gricew@mail.ru

Предлагаемая работа посвящена классификации биометрических систем распознавания субъектов, играющих в современных системах защиты информации большую роль, поскольку они являются в настоящее время одним из основных средств идентификации и аутентификации личности. Приведенные в работе классификационные схемы позволяют применить системный подход при разработке новых методов биометрии.

Ключевые слова: идентификация, аутентификация, биометрия, биометрическая система защиты информации

DEVELOPMENT AND ANALYSIS OF A CONCEPTUAL MODEL OF BIOMETRIC INFORMATION FROM THE POINT OF VIEW OF THE EXISTING LEGISLATIVE AND REGULATORY FRAMEWORKS

Sergei V. Shurugin

Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Graduate, Department of Photonics and Device Engineering, phone: (953)776-94-51, e-mail: sshurugin97@mail.ru

Arif U. Matveev

Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Graduate, Department of Photonics and Device Engineering, phone: (999)463-43-96, e-mail: arifan.matveev@mail.ru

Evgeny V. Gritskevich

Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Ph. D., Associate Professor, Department of Information Security, phone: (383)343-91-11, e-mail: gricew@mail.ru

The proposed work is devoted to the classification of biometric systems for recognizing subjects, which play an important role in modern information security systems, since they are currently one of the main means of identification and authentication of an individual. The classification schemes presented in this paper allow us to apply a systematic approach to the development of new methods of biometrics.

Keywords: identification, authentication, biometrics, biometric information security system

Введение

Целью данной работы является анализ методов и средств идентификации и аутентификации субъектов с использованием биометрических данных с точки зрения извлечения максимально возможной полезной информации, содержащейся в получаемых цифровых изображениях.

Данная цель может быть достигнута путем проведения качественного и количественного анализа биометрических систем для прогнозирования эффективности их применения в различных условиях, а также выбора наиболее оптимальных методов обработки получаемых цифровых изображений по критерию минимизации потерь извлекаемой полезной информации.

Объектом исследования будут являться системы идентификации и аутентификации субъектов с использованием биометрической информации. Предметом исследования являются автоматизированные методы и средства, применяемые для получения цифровых изображений и эффективного извлечения полезной идентифицирующей и аутентифицирующей информации, содержащейся в этих изображениях.

Качественный анализ состояния вопросов использования биометрической информации для решения задач идентификации и аутентификации субъектов

Биометрия как способ решения задач опознавания личности использовалась практически в течение всей истории существования человеческого общества. При этом отдельный индивид, участвующий в процессах, связанных с распознаванием других индивидов, не всегда отдавал или отдает себе отчет в том, что он решает задачи идентификации и аутентификации субъектов, то есть данные процессы, как правило, осуществляются конкретным лицом на подсознательном уровне. Причем это относится не только к разумным существам, но и к высокоорганизованным животным. Известно, что скорпионы, обитающие в подъездах домов городов Средней Азии, не реагируют на жильцов подъезда, тогда как могут укусить незнакомца. Ядовитые змеи, постоянно проживающие с одним человеком (хозяином, который их кормит) не нападают на него. Даже некоторые аквариумные рыбы спокойно реагируют на появление их владельца, но начинают метаться по аквариуму с приближением чужого человека.

Осознанное применение биометрических технологий с целью выявления признаков, присущих конкретному субъекту, стало интенсивно развиваться

в девятнадцатом столетии. Именно тогда дактилоскопические методы пришли на помощь криминалистам, значительно повысив достоверность получаемой информации.

В конце двадцатого века развитие программно-технических средств позволило приступить к созданию автоматизированных систем, обеспечивающих процедуры распознавания конкретного человека по его внешним признакам, включая не только статические характеристики, но и динамику поведения, чему в немалой степени способствовала формализация алгоритмической базы применяемых методов за счет обобщения накопленных частных случаев, реализующих конкретные процедуры идентификации и аутентификации личности по конкретным признакам [1].

Еще не так давно в обществе наблюдалось недопонимание, а, иногда, и скептическое отношение к использованию биометрических технологий в повседневной человеческой деятельности, исключая, пожалуй, только криминалистические лаборатории. Сейчас такое использование практически не встречает заметного противодействия, тем более, резкого отторжения, за редким исключением наиболее консервативной части населения.

Изменению общественных настроений в этой области способствовало несколько весьма серьезных причин, из которых можно было бы выделить две наиболее важных: прагматическую и экономическую. К первой относятся вопросы повышения безопасности существования людей и с точки зрения физического выживания (например, противодействие терроризму), и с точки зрения финансовой стабильности отдельно взятого индивида (защита денежных средств от посягательств мошенников), и с точки зрения безопасности окружающей информационной среды (тайна частной жизни и блокировка нежелательной, то есть вредной информации).

С экономической же точки зрения развитие биометрических технологий несет в себе несомненную выгоду тем предприятиям, которые занимаются этими вопросами. Связано это, прежде всего, с глобализацией мирового экономического пространства, что значительно увеличило транзитные пассажиропотоки через пограничные терминалы различных государств. Традиционные методы проверки участников пограничных транзакций уже не обеспечивают необходимой скорости обработки документальной информации идентифицирующего типа. Поэтому правительства ведущих мировых держав выделяют огромные финансовые средства на скорейшее внедрение прогрессивных методов, к которым относятся и биометрические технологии. Как известно, наличие бюджетных ресурсов на рынке товаров и услуг является наиболее привлекательным фактором развития тех сфер экономики, для которых эти ресурсы предназначены.

В ранний период развития применение биометрии носило скорее заместительный характер и применялось в основном в качестве альтернативы систем доступа по паролям. В настоящее время биометрические средства доступа трансформировались в самостоятельный компонент программно-технических средств защиты информации. В связи с этим при внедрении био-

метрических технологий сегодня необходимо принимать во внимание многие параметры и характеристики процессов автоматизированного распознавания, такие, например, как вероятность правильного решения, погрешность распознавания, стоимость обладания, скорость получения эталонных шаблонов и скорость обработки данных, уровни внутренней и системной безопасности, степень конфиденциальности информации, удобство интерфейса и одобрение пользователей.

Имеется большой интерес общества к данным технологиям. Слово «биометрия» часто встречается в новостных блоках различных средств массовой информации. К сожалению, использование этого понятия не всегда точно отображает суть термина. Необходимо разобраться в преувеличениях и мифах и в противовес им объективно описать возможности современных биометрических технологий. Биометрия является широкой областью исследований, включающей в себя многие аспекты, в том числе правовые и социальные проблемы, а также вопросы эргономики, безопасности, поддержания целостности данных и применения крупномасштабных систем (включая меры обеспечения отказоустойчивости и процедуры восстановления в случае сбоев) [2–7]. Биометрия тесно связана с теорией распознавания паттернов (образцов), в настоящее время она все более активно взаимодействует и с другими смежными дисциплинами. Обработка изображений, компьютерное зрение, обработка сигналов и распознавание речи, сверхширокомасштабная интеграция и машинное самообучение — все это имеет отношение к развитию биометрических технологий.

Сейчас очень важный период для биометрии. Сенсоры (датчики биометрических параметров) быстро дешевеют, компьютеры достигли высокого уровня производительности, а технологическая инфраструктура становится неотъемлемой частью нашей жизни.

Теперь только вопрос времени — сделать аутентификационные протоколы, контролируемые посредством биометрических идентификаторов, обычным, каждодневным явлением.

Классификационные схемы биометрических методов исследований

На текущий момент базовыми элементами защиты информации от несанкционированного доступа являются так называемые средства AAA (authentication, authorization, administration – аутентификация, авторизация, администрирование) [8]. При использовании последовательной цепочки этих элементов пользователь получает доступ к компьютерным ресурсам лишь после того, как успешно прошел процедуры идентификации и аутентификации.

Современные программно-технические средства идентификации и аутентификации по виду признаков, обеспечивающих распознавание, можно разделить на электронные, биометрические, комбинированные и разовые пароли (рис. 1).



Рис. 1. Классификационная схема процессов идентификации и аутентификации

При использовании электронных средств соответствующие признаки реализуются в виде кодов, хранящихся в запоминающем элементе физического носителя. К таким средствам относятся контактные и бесконтактные смарт-карты, USB-ключи (USB-token), контактная память (iButton).

Биометрические средства при осуществлении процедуры идентификации распознают личностные характеристики человека, называемые в данном случае биометрическими признаками или параметрами [9]. Применение этих средств подразумевает выделение таких характеристик и последующую процедуру их сравнения с хранящимися в базе эталонами. Следует разделять биометрические средства на статические и динамические в зависимости от того, что подлежит исследованиям: антропологические данные или поведенческие функции.

В комбинированных системах параллельно используются несколько признаков, что существенно увеличивает их количество и, тем самым, повышает вероятность правильной оценки. Причем, признаки могут принадлежать к системам одного или разных классов. Сейчас существуют комбинированные системы следующих типов: системы на базе бесконтактных смарт-карт и USB-ключей, системы на базе гибридных смарт-карт, биоэлектронные системы.

В настоящее время мировой рынок рассматриваемых средств представляет весьма широкий спектр различных систем контроля и управления доступом

к конфиденциальной информации [10]. На рынке подобные средства больше известны как биометрические средства защиты информации (БСЗИ).

БСЗИ классифицируются в зависимости от биометрических признаков, принципов функционирования и технологий изготовления (рис. 2).



Рис. 2. Классификационная схема БСЗИ

БСЗИ достаточно широко представлены в российском сегменте мирового рынка средств обеспечения информационной безопасности [11]. Среди различных типов этих средств в настоящее время наиболее эффективно используются биометрические устройства, работающие на базе систем технического зрения, основным элементом которых являются оптико-электронные датчики, регистрирующие биометрические параметры человека.

Заключение

Проведенный анализ способов биометрической идентификации и аутентификации личности позволил провести классификацию применяемых для этого подходов, что в свою очередь обеспечивает целенаправленную разработку методов и средств для их практической реализации. На основе этого анализа предполагается создание собственной методики расчета биометрических параметров субъектов с целью проведения процедур их распознавания.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Самсонова А.В. История биомеханики / А.В.Самсонова //Труды кафедры биомеханики, Междисциплинарный сборник статей / НГУ им. П.Ф. Лесгафта, СПб: ОЛИМП, 2013. – Вып. 2. – С. 4–15.
2. ГОСТ ISO/IEC 19794-1-2015 Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 1. Структура [Текст]: нац. стандарт РФ – Введ. 01.07.2016. – Стандартинформ, 2016. – 32 с.

3. ГОСТ Р ИСО/МЭК 19795-1-2007 Автоматическая идентификация. Идентификация биометрическая. Эксплуатационные испытания и протоколы испытаний в биометрии. Часть 1. Принципы и структура [Текст]: нац. стандарт РФ – Введ. 01.07.2009. – Стандартиформ, 2009. – 58 с.
4. ГОСТ ISO/IEC 24713-1-2013 Информационные технологии. Биометрические профили для взаимодействия и обмена данными. Часть 1. Общая архитектура биометрической системы и биометрические профили [Текст]: нац. стандарт РФ – Введ. 01.09.2014. – Стандартиформ, 2014. – 24 с.
5. ГОСТ Р 58273-2018 (ИСО/МЭК 29197:2015) Информационные технологии. Биометрия. Методология испытаний эксплуатационных характеристик биометрической системы на воздействие условий окружающей среды [Текст]: нац. стандарт РФ – Введ. 01.01.2019. – Стандартиформ, 2019. – 28 с.
6. ГОСТ Р 54412-2019 Информационные технологии. Биометрия. Общие положения и примеры применения [Текст]: нац. стандарт РФ – Введ. 01.06.2020. – Стандартиформ, 2020. – 44 с.
7. ГОСТ Р 58624.1-2019 Информационные технологии. Биометрия. Обнаружение атаки на биометрическое предъявление. Часть 1. Структура [Текст]: нац. стандарт РФ – Введ. 01.06.2020. – Стандартиформ, 2020. – 16 с.
8. Аверченков В.И. Аудит информационной безопасности, 3-е издание. 2016. – С.261 – 264. [Электронный ресурс] // Научная электронная библиотека «eLibrary». – Режим доступа: <https://www.elibrary.ru/item.asp?id=25083492>
9. Кухарев, Г. А. Биометрические системы: методы и средства идентификации личности человека [Текст] // СПб: Политехника, 2001. – 240 с.
10. Биометрические системы: актуальное состояние рынка в России и в мире [Электронный ресурс] / URL: http://www.allbiometrics.ru/wp-content/uploads/2017/05/2017_Nikolaev.pdf. (дата обращения: 22.03.2021).
11. Российская биометрия и цифровая экономика [Электронный ресурс] / URL: http://www.allbiometrics.ru/wp-content/uploads/2017/05/2017_Mamaev.pdf (дата обращения: 22.03.2021).

© С. В. Шуругин, А. У. Матвеев, Е. В. Грицкевич, 2021