УДК: 621.394.147 + 004.056.53

А. В. Еременко[1], канд. техн. наук, доцент кафедры "Инфокоммуникационные системы и информационная безопасность", e-mail: nexus-@mail.ru,
А. Е. Сулавко[2], канд. техн. наук, старший преподаватель кафедры "Комплексная защита информации", e-mail: sulavich@mail.ru,
Д. А. Волков[2], аспирант, e-mail: vlkv.d.a@gmail.com
[1] Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования "Омский государственный университет путей сообщения" (ОмГУПС (ОмИИТ), г. Омск
[2] Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования "Омский государственный технический университет" (ОмГТУ), г. Омск

Современное состояние и пути модернизации преобразователей биометрия—код*

Рассмотрена проблема защиты криптографических ключей в процессе их эксплуатации. Объектом исследования в работе выступают преобразователи биометрия—код. Приведен обзор методов, позволяющих использовать биометрические признаки человека в качестве исходного материала для получения криптографических ключей шифрования, а также для идентификации и аутентификации. Определены основные факторы, влияющие на надежность работы рассмотренных методов. Предложены возможные пути модернизации существующих методов генерации криптографических ключей на основе динамических биометрических признаков.

Ключевые слова: *биометрические технологии, защита персональных данных, помехоустойчивое кодирование, исправляющая способность, идентифицирующие признаки, нечеткие данные, ключевая последовательность*

Введение

Роль биометрических технологий в современном обществе стремительно возрастает. Все большее число получаемых потребителем услуг связано с предоставлением биометрических данных. Биометрические данные требуются при осуществлении государственного контроля — оформления биометрических паспортов с отпечатками пальцев, виз, прохождения миграционного контроля. Растет популярность биометрических технологий при реализации новых проектов в коммерческом секторе: банковском обслуживании, мобильных приложениях, платежных системах, защите информации, учете рабочего времени, контроле доступа и др. Прогнозируется, что к 2019 г. отечественный рынок биометрических технологий преодолеет рубеж 300 млн долл. [1].

При этом крайне актуальными становятся вопросы не только технического, но и правового характера, связанные с обеспечением защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну. Согласно Федеральному закону "О персональных данных" № 152-ФЗ, биометрические персональные данные — это "физиологические или биологические характеристики человека, в том числе изображение человека (фотография и видеозапись), которые позволяют установить его личность и используются оператором для установления личности субъекта". По предварительной оценке *Zecurion Analytics* (*Zecurion* — крупнейший разработчик DLP-систем для защиты от внутренних угроз и утечек информации), ущерб мировой экономике от утечек информации за 2013 и 2014 годы составил более 42 млрд долл. При этом доля инцидентов, связанных с утечкой персональных данных, составляет более 60 % [2].

Для того чтобы выполнить требования законодательства по защите биометрических персональных данных операторы применяют методы шифрования и разграничение прав доступа к файлам и базам

* Работа выполнена при финансовой поддержке РФФИ (грант № 15-07-09053).

данных с биометрическими признаками пользователей. Защищенность конфиденциальной информации в большой степени зависит от надежности пароля, выбранного для шифрования или аутентификации субъектов доступа, а также процедур его выработки, изменения и хранения. Использование биометрических данных позволяет решить проблему человеческого фактора при выборе и использовании пароля пользователями информационных сервисов [3].

В случае идентификации пользователей по биометрическим признакам актуальной становится другая проблема — защита биометрического эталона пользователя, хранящегося на удаленном сервере аутентификации, а также биометрических признаков при выполнении процедуры биометрического сканирования. Для аутентификации в разных информационных системах можно использовать отличающиеся пароли. В случае аутентификации, например, по отпечаткам пальцев, число вариантов для изменения скомпрометированного признака пользователя ограничено. Современный уровень технологий позволяет злоумышленникам создавать из отпечатка пальца муляж, который будет принят системой сканирования за "живой" образец. При использовании психофизиологических признаков задача фальсификации усложняется, однако располагая информацией из биометрического эталона, злоумышленник может восстановить сигналы, описывающие биометрический образ автора и использовать их для получения доступа к информационным сервисам или ресурсам.

Но каким образом можно защитить конфиденциальную информацию биометрическими методами и при этом обеспечить защищенность биометрических данных пользователя? Вариант решения обозначенной выше проблемы рассмотрен в работе [4]. Решение заключается в получении из биометрических данных пользователей криптографических ключей, что позволяет объединить преимущества от использования биометрических технологий и криптографических методов, а также защитить биометрические данные пользователей при выполнении сервисных процедур. Предложенный метод позволяет отказаться от хранения биометрических признаков в исходном виде и делает бессмысленной кражу персонального биометрического идентификатора человека, так как он может быть изменен в любой момент при необходимости.

Цель настоящей работы — рассмотреть текущее состояние исследований в области разработки и применения преобразований биометрия—код, определить пути модернизации метода, предложенного авторами ранее в работе [4] для повышения надежности его работы. Интегральную надежность систем генерации криптографических ключей по биометрическим признакам можно определить по оценке риска принятия решения R [5]:

$$R = c_0 \int\limits_{-\infty}^{x_0} \omega_2(x)dx + c_1 \int\limits_{x_0}^{\infty} \omega_1(x)dx,$$

где c_i — вес ошибки; ω_2 — значение ошибки 2-го рода (FAR — *False Accept Rate*); ω_1 — значение ошибки 1-го рода (FRR — *False Rejection Rate*). Равновероятное значение ошибки 1-го и 2-го рода обозначается EER (*Equal Error Rate*).

1. Обзор методов генерации криптографических ключей из биометрической информации пользователей

Идея связывания биометрических образов с криптографическими ключами шифрования возникла как производная от идеи, так называемой, аннулируемой биометрии [6]. Ее суть состоит в устранении существенного недостатка классической биометрии, связанного с невозможностью изменять физиологический биометрический признак в случае его компрометации.

Основной проблемой при генерации ключевых последовательностей по биометрическим данным является техническая невозможность получения одинаковых образов биометрических характеристик при их повторном вводе пользователем. Ситуационные изменения в психофизиологическом состоянии человека, изменение поведенческих характеристик в течение жизни, наложение шумов при получении биометрических образов приводят к проблеме несовпадения биометрических признаков одного и того же человека и генерация ключа при этом становится затруднительной. Для решения этой проблемы в мировой практике изначально сложились два подхода: нечеткое хранилище (*fuzzy vault*) [7] и нечеткий экстрактор (*fuzzy extractor*) [8] — теоретическая работа, ставшая фундаментальной основой для многочисленных современных исследований. Объединяет эти два подхода использование вспомогательной открытой информации, аналогичной той, что применяется при шифровании с открытым ключом. На основе пары открытая строка — предъявленный идентификатор при аутентификации происходит построение криптографического ключа. Различие между нечетким хранилищем и нечетким экстрактором состоит в том, что в первом случае открытая строка представляет собой множество произвольного вида, в то время как во втором случае — конечномерный вектор. Разработанные методы позволяют сгенерировать новый ключ пользователя на основе его биометрического признака. Таким образом, применение биометрии приближается по удобству использования к паролю и другим повторно выдаваемым идентификаторам.

Сравнение достигнутых результатов в области генерации криптографических ключей на основе биометрических признаков

Автор	Тип биометрического признака	FRR/FAR, %	Размер ключа, бит	Условия тестирования
Hao F. и др. [9] Bringer J. и др. [10] Rathgeb C. и Uhl A. [11]	Радужная оболочка глаза	0,47/0 5,62/0 4,64/0	140 42 128	70 испытуемых База данных (БД) ICE 2005 БД ICE 2005
Teoh A. и Kim J. [12] Nandakumar K. [13]	Отпечаток пальца	0,9/0 12,6/0	296 327	БД FVC 2002 БД FVC 2002
Ao A. и Li J. [14]	Изображение лица	7,99/0,11	>4000	294 испытуемых
Maiorana E. и Campisi P. [15]	Подпись	EER >9	>100	БД MCYT
Sutcu Y. и др. [16]	Изображение лица и отпечаток пальца	0,92/0,01	—	БД NIST DB 27 & Face 94
Nandakumar K. и Jain A. [17]	Отпечаток пальца и радужная оболочка глаза	1,8/0,01	224	БД MSU-DBI & CASIAv1
Kelkboom E. и др. [18]	3D-изображение лица	22/0,25	155	БД FRGC

О состоянии исследований в данной области можно судить по таблице, в которой собраны достижения зарубежных ученых по основным направлениям биометрических технологий.

В работе [19], поддержанной австрийским научным фондом (проект № L554-N15), авторы дали оценку робастности результатов, приведенных в таблице с учетом влияния шумовых воздействий на биометрические образы. Авторы пришли к выводу, что результаты, полученные с использованием разработанных методов, являются в определенной степени робастными и на практике должны показать сопоставимые с представленными в таблице оценками ошибки 1-го и 2-го рода.

Как видно из таблицы развитие биометрической криптографии двигается в направлении от использования единичных биометрических признаков к мультимодальным системам генерации криптографических ключей из биометрических признаков. Одна из ключевых проблем в данном подходе связана с формированием общего вектора описания биометрических характеристик с учетом вероятности их единичной ошибки. В работе [20] показана связь эффективности коррекции ошибок с методами группирования битов с разной вероятностью единичной ошибки. Несмотря на предпринятые в данном направлении усилия, единого подхода для решения этого вопроса до сих пор выработано не было.

Для психофизиологических характеристик достичь показателей систем, использующих для генерации ключей физиологические признаки, пока не удается. В работе [21] проведено самостоятельное исследование метода генерации ключей на подписях 126 испытуемых из базы данных рукописных паролей MCYTX. Работа поддержана испанским Министерством науки и технологий (MCYT TIC2003-08382-C05-01) и европейской комиссией по науке и технологиям (IST-2002-507634 Biosecure NoE projects). Результаты в работе получены следующие: ошибка 1-го рода (FRR) составила 57,30 % при ошибке 2-го рода (FAR) 1,18 % для профессиональных подделок и 0,32 % для подделок, выполненных без наблюдения аутентичной подписи и стиля ее написания. Снизить уровень ошибок 1-го рода автор предлагает за счет повторного ввода подписи.

Рассмотрим опыт предшественников. В работе [22] получена средняя ошибка 1-го рода (FRR) 7,05 % и ошибка 2-го рода (FAR) для профессиональных подделок 0 % для 11 испытуемых. Похожий результат был получен в работе [23] для метода замены скомпрометированных ключей с использованием биометрических хешей, получаемых из рукописного почерка. Значение равной ошибки (EER) для этого метода составило < 6,7 % для 40 испытуемых. В работе [24] разработан метод получения ключа из рукописного пароля с ошибкой 1-го рода 28 % при ошибке 2-го рода 1,2 %. Стоит отметить, что данный результат был получен без использования кодов, исправляющих ошибки.

Круг отечественных ученых, занимающихся вопросами совмещения биометрии и криптографии, не столь широк. В работе [25] рассматривается вопрос получения устойчивого криптографического ключа из биометрической характеристики изображения отпечатков пальцев. Предложенные автором методы позволяют строить вектор длиной 600...1728 битов, содержащий около 25 % ошибочных позиций. Для исправления ошибок используют коды Адамара, а также каскадное кодирование, включающее коды Боуза-Чоудхури—Хоквингхема (БЧХ) и репликацию. Такое кодирование обусловлено структурой ошибок: БЧХ-коды корректируют шумовые ошибки, в то время как репликация позволяет справляться с блочными ошибками (свя-

занными с "выпадением" минюций). Таким образом, с вероятностью около 90 % получим исходный ключ с энтропией в 20—36 бит (даже очень защищенные системы редко используют для формирования криптографических ключей материал свыше 200 бит). Для построения зашумленного биометрического вектора из изображения отпечатка пальца на сегодняшний день не существует общепринятого подхода, что связано с особенностями описания шаблона отпечатка пальца. В работе автор опробовал несколько методов для описания ключевых точек отпечатка пальца, лучший результат при энтропии ключа 30 бит для метода с введением внешнего порядка характеризуется уровнем ошибок FRR < 19 % при FAR < 0,01 %.

В работе Е. А. Харина под руководством канд. физ.-мат. наук С. М. Гончарова (см. также [26]) на тему "Генерация ключевых последовательностей на основе биометрических данных пользователей" рассматриваются вопросы генерации ключевых последовательностей на основе клавиатурного почерка и радужной оболочки глаза. Всего для экспериментальной проверки разработанных методов были собраны более 1400 образцов клавиатурного почерка от 26 пользователей, уровень владения клавиатурой которых оценивался как "хороший" или "отличный". В результате экспериментов была также получена зависимость значений ошибок 1-го и 2-го рода от чувствительности системы. Было обнаружено, что уровень ошибки 2-го рода может достигать 0 при вероятности ошибки 1-го рода 50 %. Коэффициент равновероятной ошибки составил более 12 %. Принципиальное отличие разработанной системы генерации ключевых последовательностей на основе радужной оболочки глаза от созданных ранее заключается в последовательном применении двух помехоустойчивых кодов, каждый из которых исправляет ошибки определенного типа. Применение такого подхода, а также маскирования позволило достигнуть уровней ошибок 1-го и 2-го рода 0,47 % и 0 % соответственно и получать ключи длиной 140 бит. Автор также делает вывод, что рисунок радужной оболочки глаза в настоящее время позволяет получать более длинные ключи, чем какая бы то ни было другая биометрическая характеристика, за исключением, быть может, кода ДНК.

Работа [27] посвящена разработке преобразователя биометрия—код доступа на основе электроэнцефалограммы (ЭЭГ) головного мозга человека. В качестве преобразователя используется двухслойная нейронная сеть сигмоидального типа. Нейросетевой преобразователь выдает на выходе 256-битовый ключ. В построенном преобразователе использовались 210 параметров. Прогноз вероятности ошибки 2-го рода составил $\leqslant 10^{-12}$. Участвовало 15 пользователей, проверено порядка 5000 ЭЭГ. В самом худшем случае расстояние Хэмминга до пароля при подделке составило 21 бит в 256-битном ключе. В целом данное направление выглядит перспективным, в качестве недостатка можно отметить необходимость использования специального оборудования и сложную на данный момент процедуру получения биометрического образа человека.

В описании к изобретению [28] указано, что поле кодовых комбинаций для рисунка отпечатка пальца составляет всего 1000 или 10 000 (страница 9 описания, строка 12). В случае доступа злоумышленника к кодам программы автоматически перебрать столь малое поле кодовых комбинаций крайне просто. Реализация атаки займет всего несколько секунд машинного времени, поэтому основным недостатком этого способа является его низкая стойкость к атакам подбора.

Известен способ идентификации человека по его биометрическому образу [29], основанный на использовании нейросетевого преобразователя биометрия—код с повышенной стойкостью к атакам подбора. В случае сохранения рукописного биометрического пароля из пяти букв в тайне данный способ позволяет получить стойкость на уровне порядка 10^{12} попыток атаки подбора (см. таблицу А2 приложения А стандарта [30]). Основным недостатком способа является его недостаточная стойкость к атакам подбора по современным требованиям. Увеличение длины ключа нецелесообразно, так как приведет к необходимости ввода гораздо более сложного рукописного пароля и значительно затруднит работу пользователя с системой. Так, если требуется безопасно обеспечивать доступ к криптографическому ключу длиной 256 бит (стойкость к атакам подбора 10^{77}), потребуется организовывать ввод рукописного пароля, состоящего примерно из шести слов по пять букв. Пользователь обязательно ошибется хотя бы в одном из шести слов и вынужден будет вновь писать шесть рукописных слов. Написать одно рукописное слово обычно удается с одной или двух попыток. Для безошибочного написания двух слов пароля требуется от одной до четырех попыток. Для написания трех слов необходимо уже около 12 попыток. При этом пользователь не знает, в каком слове он ошибся в связи с запретом стандарта (см. п. 7.6 ГОСТ Р52633—2006) снабжать однозначными индикаторами верного результата фрагменты составного биометрического пароля (ключа).

В соответствии с работой [31] код доступа перекодируют в код с обнаружением и исправлением ошибок (стр. 12 описания, п. 7 формулы изобретения, строка 34). Основным недостатком этого изобретения является его низкая способность исправлять нестабильные биометрические данные. Со-

временные коды способны обнаруживать до 80 % ошибок, но исправлять они могут не более 5 % ошибок. По этой причине при разработке нечетких экстракторов подобных тем, что предложены в данной работе, приходится использовать только малую часть наиболее стабильной биометрической информации. Биометрические данные со стабильностью менее 5 % приходится отбрасывать. Как следствие, нейросетевые преобразователи биометрия—код оказываются эффективнее нечетких экстрактов, так как они используют все данные и могут работать с произвольными кодами.

Вторым недостатком изобретения является то, что примеры биометрических образов, введенных с некоторыми ошибками, далее при аутентификации не используются. Это делает все описанные выше способы неэффективными при мультибиометрической аутентификации.

Третьим и главным недостатком является то, что его реализация для нескольких совместно используемых биометрических образов не дает экспоненциального выигрыша по стойкости биометрической защиты к атакам подбора, так как сложность восстановления каждой из частей ключа будет примерно одинаковой и каждую из частей составного ключа можно подбирать независимо.

Целью предлагаемого изобретения в работе [32] является повышение надежности биометрической аутентификации за счет использования нескольких биометрических образов при обеспечении приемлемого уровня дружественности системы, безопасно подсказывающей человеку при вводе какого именно образа он ошибся и тем самым сокращающей трудозатраты людей на высоконадежную мультибиометрическую аутентификацию. Для генерации аутентификатора используют совершенно разные биометрические образы (например, рукописный пароль, голосовой пароль, рисунок отпечатка пальца). При этом для каждого образа применяют свой преобразователь биометрия—код. Интересным решением является обучение нейросетевого преобразователя биометрия—код на самокорректирующийся выходной код, способный обнаруживать и исправлять ошибки. Все коды неудачной биометрической аутентификации в рамках одного сеанса запоминают и затем сравнивают между собой состояния их разрядов. Далее выявляют наиболее нестабильные разряды кодов и осуществляют их направленный перебор до момента появления кода биометрического образа без ошибки или с числом ошибок, поддающимся исправлению выбранным самокорректирующимся кодом.

Положительный технический эффект обусловлен использованием при восстановлении ключа всех введенных пользователем биометрических образов. Решение, предложенное авторами, позволяет сообщать пользователю, находящемуся в измененном состоянии (например, в стрессовой ситуации), о времени, которое потребуется на восстановление ключа. Таким образом, у пользователя есть выбор — продолжить ожидание восстановления (перебора) ключа, либо инициировать новый сеанс восстановления ключа.

Таким образом, в настоящее время ученые используют два подхода для преобразования биометрических характеристик в воспроизводимые битовые последовательности. Первый подход основан на нейронных сетях, второй носит название "нечеткий экстрактор" и работает с использованием помехоустойчивого кодирования. Классические самокорректирующиеся коды малоэффективны. Они требуют очень большой избыточности. Наблюдается экспоненциальный рост избыточности кода, способного править линейно растущий процент ошибок. В работе [33] приводится следующая точка зрения: классические коды на практике не могут исправить более 30 % ошибок, так как их информационная часть оказывается незначительной. Коды Безяева предназначены для биометрии и не поглощают биометрические данные своей избыточностью. Они безопасно хранят рядом синдромы ошибок в виде усеченных хэш-функций [34].

Нейросетевые преобразователи позволяют использовать полный объем выделяемых из биометрического образа человека характеристик, в то время как нечеткие экстракторы работают только со стабильной частью информации. Обучение каждого слоя нейронов сети выполняют своим автоматом, учитывающим особенности той или иной биометрической технологии для входных данных разного качества [35].

Основной проблемой, которую необходимо решить разработчику нейросетевых преобразователей биометрия—код, является оптимальный подбор коэффициентов обучения нейронной сети. Обучение нейросетевых преобразователей биометрия—код должно проводиться на примерах биометрических образов "Свой" и "Чужой" и от этой процедуры зависит защищенность ключа пользователя от попыток его восстановления злоумышленником. Качество защиты определяется законом распределения генерируемых значений биометрических характеристик, используемым в автомате для описания модели формирования признаков при фальсификации злоумышленником аутентичных образов. Несмотря на сложность данного подхода, методы нейросетевого преобразования биометрии в код показывают лучшие результаты.

Преимуществом преобразователей биометрия—код, основанных на помехоустойчивом кодировании, является возможность отказаться от хранения непосредственно самих биометрических данных,

так как вектор биометрических признаков "объединяется" с секретным ключом. Для того чтобы получить ключ, необходимо "знать" биометрические данные, "отсоединив" их от ключа, т. е. хранения самих биометрических данных не требуется. В качестве операций "объединения" и "разъединения" битовых последовательностей, как правило, используется побитовое сложение по модулю 2. При использовании нейросетевого подхода требуется где-то хранить эталон (веса нейронов), следовательно, нужно обеспечить защиту эталона.

Существует точка зрения, что в силу малоинформативности динамических процессов человека (рукописного и клавиатурного почерка, голоса и др.), получаемые при их преобразовании в возобновляемый код ошибки 1-го и 2-го рода будут на порядок больше, чем при преобразовании физиологических признаков (радужная оболочка глаза, отпечатки пальцев, изображение лица, геометрия ладони и др.). Известна причина нестабильности результатов для "психофизиологического" направления: ответ кроется в самой природе этих признаков — психофизиологии человека, которая изменчива.

2. Применение рассмотренных методов на практике

Рассмотренные методы могут быть использованы для повышения защищенности закрытых ключей шифрования конфиденциальной информации (хранение и обмен ключами не требуются, если секретный ключ "привязан" к личности), защиты авторских прав с помощью встраивания водяных знаков в электронные произведения авторов, в области биометрической идентификации пользователей компьютерных систем для повышения уровня защищенности от угрозы неавторизованного доступа.

Заключение

Изучение рассмотренных в статье научных работ, а также имеющийся у авторов задел, позволяют сделать заключение, что достичь прорыва в области генерации криптографических ключей по психофизиологическим признакам человека и снизить ошибки 1-го и 2-го рода до уровня систем, основанных на физиологии, возможно, если идти по следующим путям модернизации.

1. Выделить и определить потенциал признаков рукописного и клавиатурного почерка, голоса для генерации ключей шифрования.

2. Разработать алгоритм маркирования стабильных для каждого пользователя признаков.

3. Разработать алгоритм формирования битового вектора характеристик рукописного, клавиатурного почерка и голоса с учетом вероятности их единичной ошибки (см. работу [20], где была продемонстрирована связь эффективности коррекции ошибок с методами группирования битов с разной вероятностью единичной ошибки).

4. Разработать специальный программный модуль для воспроизведения вычислительного эксперимента по аналогии с тем, как это было реализовано в работе [36]. Предполагается предусмотреть возможности проведения экспериментов с использованием настоящих биометрических данных (реализаций подсознательных движений, введенных субъектами), а также с возможностью генерации реализаций биометрических параметров на основе эталонов (созданных из настоящих биометрических данных). Генерация значений признаков может быть осуществлена с помощью метода Монте-Карло по аналогии с тем, как это осуществлялось в работе [37].

5. Разработать комплексный преобразователь биометрия—код на основе кодов Безяева [34] и/или нейронной сети, настроенной на мультимодальную работу с несколькими типами биометрических признаков и обученной на самокорректирующийся выходной код, способный обнаруживать и исправлять ошибки.

6. Адаптировать генератор ключей к изменению психофизиологического состояния владельца биометрических данных.

Список литературы

1. **Биометрический** рынок России: прогноз на 2015 год и перспективу. М.: Биолинк Солюшенс, 2014. 17 с.

2. **Утечки** конфиденциальной информации. Предварительные итоги 2014 г. М.: Zecurion, 2015. 15 с.

3. **Сулавко А. Е., Еременко А. В., Левитская Е. А.** Разграничение доступа к информации на основе скрытого мониторинга действий пользователей в информационных системах: портрет нелояльного сотрудника // Известия Транссиба/ОмГУПС. 2015. № 1 (21). С. 80—89.

4. **Еременко А. В., Сулавко А. Е.** Исследование алгоритма генерации криптографических ключей из биометрической информации пользователей компьютерных систем // Информационные технологии. 2013. № 11. С. 47—51.

5. **Еременко А. В.** Повышение надежности идентификации пользователей компьютерных систем по динамике написания паролей: Автореф. дис. ... канд. техн. наук. Омск, 2011. 20 с.

6. **Ratha N. K., Connell J. H., Bolle R. M.** Enhancing security and privacy in biometrics—based authentication systems // IBM Systems Journal. 2001. N 40 (3). P. 614—634.

7. **Juels A., Sudan M.** A fuzzy vault scheme // Proc. IEEE Intil. Symp. Inf. Theory. 2002. 408 p.

8. **Dodis Y., Reyzin L., Smith A.** Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data // Proc. from Advances in Cryptology. EuroCrypt. 2004. P. 79—100.

9. **Hao F., Anderson R., Daugman J.** Combining Cryptography with Biometrics Effectively // IEEE Transactions on Computers. 2006. N 55 (9). P. 1081— 1088.

10. **Bringer J., Chabanne H., Cohen G., Kindarji B., Z'emor G.** Theoretical and practical boundaries of binary secure sketches // IEEE Transactions on Information Forensics and Security. 2008. N 3. P. 673—683.

11. **Rathgeb C., Uhl A.** Adaptive fuzzy commitment scheme based on iris-code error analysis // Proc. of the 2nd European Workshop on Visual Information Processing (EUVIP'10). 2010. P. 41—44.

12. **Teoh A., Kim J.** Secure biometric template protection in fuzzy commitment scheme // IEICE Electron. Express. 2007. N 4 (23). P. 724—730.

13. **Nandakumar K.** A fingerprint cryptosystem based on minutiae phase spectrum // Proc. of IEEE Workshop on Information Forensics and Security (WIFS). 2010. P. 1—6.

14. **Ao M., Li S. Z.** Near infrared face based biometric key binding // In Proc. of the 3rd International Conference on Biometrics 2009 (ICB'09) LNCS: 5558. 2009. P. 376—385.

15. **Maiorana E., Campisi P.** Fuzzy commitment for function based signature template protection // IEEE Signal Processing Letters. 2010. N 17. P. 249—252.

16. **Sutcu Y., Li Q., Memon N.** Secure biometric templates from fingerprint-face features // In IEEE Conference on Computer Vision and Pattern Recognition, CVPR'07. 2007. P. 1—6.

17. **Nandakumar K., Jain A. K.** Multibiometric template security using fuzzy vault // In IEEE 2nd International Conference on Biometrics: Theory, Applications, and Systems, BTAS '08. 2008. P. 1—6.

18. **Kelkboom E. J. C., Zhou X., Breebaart J., Veldhuis R. N. S., Busch C.** Multi-algorithm fusion with template protection // In Proc. of the 3rd IEEE Int. Conf. on Biometrics: Theory, applications and systems (BTAS'09). 2009. P. 1—7.

19. **Rathgeb C., Uhl A.** Iris-Biometric Fuzzy Commitment Schemes under Signal Degradation, ICISP'12 // In Proceedings of the 5th international conference on Image and Signal Processing. P. 217—225.

20. **Scotti F., Cimato S., Gamassi M., Piuri V., Sassi R.** Privacy-aware Biometrics: Design and Implementation of a Multimodal Verification System // 2008 Annual Computer Security Applications Conference, IEEE. 2008. P. 130—139.

21. **Santos M. F., Aguilar J. F., Garcia J. O.** Cryptographic key generation using handwritten signature // Proceedings of SPIE, Orlando, Fla, USA, Apr. 2006. 2006. Vol. 6202. P. 225—231.

22. **Vielhauer C., Steinmetz R., Mayerhöfer A.** Evaluating biometric encryption key generation // In Proc. ICPR. 2002. P. 123—126.

23. **Yip K. W., Goh A., Ling D. N. C., Jin A. T. B.** Generation of replaceable cryptographic keys from dynamic handwritten signatures // In Proc. ICB, Lecture Notes in Computer Science 3832, Springer. 2006. P. 509—515.

24. **Hao F., Chan C. W.** Private key generation from on-line handwritten signatures // Information Management & Computer Security, Is. 10. 2002. №. 2. P. 159—164.

25. **Ушмаев О. С., Кузнецов В. В.** Алгоритмы защищенной биометрической верификации на основе бинарного представления топологии отпечатков пальцев // Информатика и ее применения. 2012. Том 6, № 1. С. 132—140.

26. **Харин Е. А., Гончаров С. М., Корнюшин П. Н.** Построение систем биометрической аутентификации с использованием генератора ключевых последовательностей на основе нечетких данных // Матер. 50-й Всерос. межвуз. науч.-техн. конф. Владивосток: ТОВМИ, 2007. С. 112—115.

27. **Гончаров С. М., Боршевников А. Е.** Нейросетевой преобразователь "биометрия — код доступа" на основе мысленного pin-кода // Труды Научно-технической конференции кластера пензенских предприятий, обеспечивающих безопасность информационных технологий. Пенза, 2014. Том 9. С. 46—50.

28. **Медль А., Штефан Э., Мюллер Р.** Способ и система для генерирования набора ключа доступа, а также для аутентификации человека на основе его биометрического параметра. Патент России № 2267159. 2005. Бюл. № 36.

29. **Ефимов О. В., Иванов А. И., Фунтиков В. А.** Способ идентификации человека по его биометрическому образу. Патент России № 2005102541.02.02. 2005.

30. **ГОСТ Р 52633.0—2006.** Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации. М.: Изд-во стандартов, 2007.

31. **Чмора А. Л., Уривский А. В.** Биометрическая система аутентификации. Патент России № 2316120. 2008. Бюл. № 3.

32. **Иванов А. И.** Способ безопасной биометрической аутентификации // Патент России №2406143. 2010.

33. **Иванов А. И.** Нейросетевая защита конфиденциальных биометрических образов гражданина и его личных криптографических ключей. Пенза, 2014. 57 с.

34. **Безяев А. В., Иванов А. И., Фунтикова Ю. В.** Оптимизация структуры самокорректирующегося биокода, хранящего синдромы ошибок в виде фрагментов хеш-функций // Вестник Уральского федерального округа. Безопасность в информационной сфере. 2014. № 3 (13). С. 4—14.

35. **ГОСТ Р 52633.5—2011.** Защита информации. Техника защиты информации. Автоматическое обучение нейросетевых преобразователей биометрия — код доступа. Введен впервые; Введ. 01.12.2011. М.: Стандартинформ, 2012. 20 с.

36. **Сулавко А. Е.** Программный комплекс для быстрого прототипирования систем распознавания образов // Тезисы II Всероссийской конференции "Теория и практика Успеха": Омск 10—11 апреля 2014 г. С. 21—22.

37. **Епифанцев Б. Н., Ложников П. С., Сулавко А. Е.** Сравнение алгоритмов комплексирования признаков в задачах распознавания образов // Вопросы защиты информации. 2012. № 1. С. 60—66.

A. V. Eremenko, Ph. D., Associate Professor of the Department "Info-communication systems and information security", nexus-@mail.ru, Omsk State Transport University (OSTU),
A. E. Sulavko, Ph. D., Senior Lecturer of the Department "Comprehensive Information Protection", sulavich@mail.ru,
D. A. Volkov, Postgraduate Student, vlkv.d.a@gmail.ru,
Omsk State Technical University (OmSTU)

Current State and Ways to Modernize Converters Biometrics to Code

The article is devoted to the problem of the protection of cryptographic keys during their operation. The object of study in the article are the converters biometrics to code. An overview of the methods for use biometric characteristics of a human as a starting material for producing the cryptographic key encryption, as well as for identification and authentication is performed. The main factors affecting the reliability of the methods are considered. The conclusion about possible ways to modernize the existing methods to generate cryptographic keys based on dynamic biometric features is made.

Keywords: *biometric techniques, personal data protection, error-correcting codes, error correcting capability, biometric features, fuzzy data, key sequence*

References

1. **Biometricheskij** *rynok Rossii: prognoz na 2015 god i perspektivu* [Biometric market in Russia: Forecast for 2015 and for the feature]. Moscow: Biolink Soljushens, 2014, 17 p.

2. **Utechki** *konfidencial'noj informacii*. Predvaritel'nye itogi. Leakage of confidential information. Preliminary results of 2014, Moscow, Zecurion, 2015, 15 p.

3. **Sulavko A. E., Eremenko A. V., Levitskaja E. A.** Razgranichenie dostupa k informacii na osnove skrytogo monitoringa pol'zovatelej komp'juternyh sistem: portret neloial'nogo sotrudnika [Concurrent access to information based on hidden monitoring of computer systems users: Portrait of a disloyal employee]. *Izvestija Transsiba / OSTU*, Omsk, 2015, no. 1 (21), pp. 80—89.

4. **Eremenko A. V., Sulavko A. E.** Issledovanie algoritma generacii kriptograficheskih kljuchej iz biometricheskoj informacii pol'zovatelej komp'juternyh sistem [Investigation of algorithm for generating cryptographic keys from biometric information of users of computer systems]. *Informacionnye tehnologii*, 2013, no. 11, pp. 47—51.

5. **Eremenko A. V.** *Povyshenie nadezhnosti identifikacii pol'zovatelej komp'juternyh sistem po dinamike napisanija parolej* [Improving the reliability of computer systems to authenticate users on the dynamics of handwriting passwords], Abstract. dis. ... cand. tehn. sciences, Omsk, 2011. 20 p.

6. **Ratha N. K., Connell J. H., Bolle R. M.** Enhancing security and privacy in biometrics-based authentication systems, *IBM Systems Journal*, 2001, no. 40 (3), pp. 614—634.

7. **Juels A., Sudan M.** A fuzzy vault scheme, *Proc. IEEE Intil. Symp. Inf. Theory*. 2002. 408 p.

8. **Dodis Y., Reyzin L., Smith A.** Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data, *Proc. from Advances in Cryptology. EuroCrypt*, 2004, pp. 79—100.

9. **Hao F., Anderson R., Daugman J.** Combining Cryptography with Biometrics Effectively, *IEEE Transactions on Computers*, 2006, no. 55 (9), pp. 1081—1088.

10. **Bringer J., Chabanne H., Cohen G., Kindarji B., Z'emor G.** Theoretical and practical boundaries of binary secure sketches, *IEEE Transactions on Information Forensics and Security*, 2008, no. 3, pp. 673—683.

11. **Rathgeb C., Uhl A.** Adaptive fuzzy commitment scheme based on iris-code error analysis, *In Proc. of the 2nd European Workshop on Visual Information Processing (EUVIP'10)*, 2010, pp. 41—44.

12. **Teoh A., Kim J.** Secure biometric template protection in fuzzy commitment scheme, *IEICE Electron. Express*, 2007, no. 4 (23), pp. 724—730.

13. **Nandakumar K.** A fingerprint cryptosystem based on minutiae phase spectrum, *In Proc. of IEEE Workshop on Information Forensics and Security (WIFS)*, — 2010, pp. 1—6.

14. **Ao M., Li S. Z.** Near infrared face based biometric key binding, *In Proc. of the 3rd International Conference on Biometrics 2009 (ICB'09) LNCS: 5558*, 2009, pp. 376—385.

15. **Maiorana E., Campisi P.** Fuzzy commitment for function based signature template protection, *IEEE Signal Processing Letters*, 2010, no. 17, pp. 249—252.

16. **Sutcu Y., Li Q., Memon N.** Secure biometrie templates from fingerprint-face features, *In IEEE Conference on Computer Vision and Pattern Recognition, CVPR'07*, 2007, pp. 1—6.

17. **Nandakumar K., Jain A. K.** Multibiometric template security using fuzzy vault, *In IEEE 2nd International Conference on Biometrics: Theory, Applications, and Systems*, BTAS '08, 2008, pp. 1—6.

18. **Kelkboom E. J. C., Zhou X., Breebaart J., Veldhuis R. N. S., Busch C.** Multialgorithm fusion with template protection, *In Proc. of the 3rd IEEE Int. Conf. on Biometrics: Theory, applications and systems (BTAS'09)*, 2009, pp. 1—7.

19. **Rathgeb C., Uhl A.** Iris-Biometric Fuzzy Commitment Schemes under Signal Degradation, ICISP'12, *In Proceedings of the 5th international conference on Image and Signal Processing*, pp. 217—225.

20. **Scotti F., Cimato S., Gamassi M., Piuri V., Sassi R.** Privacy-aware Biometrics: Design and Implementation of a Multimodal Verification System, *2008 Annual Computer Security Applications Conference, IEEE*, 2008, pp. 130—139.

21. **Santos M. F., Aguilar J. F., Garcia J. O.** Cryptographic key generation using handwritten signature, *Proceedings of SPIE, Orlando, Fla, USA*, Apr. 2006, 2006, vol. 6202, pp. 225—231.

22. **Vielhauer C., Steinmetz R., Mayerhöfer A.** Evaluating biometric encryption key generation, *In Proc. ICPR*, 2002, pp. 123—126.

23. **Yip K. W., Goh A., Ling D. N. C., Jin A. T. B.** Generation of replaceable cryptographic keys from dynamic handwritten signatures, *In Proc. ICB, Lecture Notes in Computer Science 3832, Springer*, 2006, pp. 509—515.

24. **Hao F., Chan C. W.** Private key generation from on-line handwritten signatures, *Information Management & Computer Security*, 2002, Is. 10, no. 2, pp. 159—164.

25. **Ushmaev O. S., Kuznecov V. V.** Algoritmy zashhishhennoj biometricheskoj verifikacii na osnove binarnogo predstavlenija topologii otpechatkov pal'cev [Algorithms for secure biometric verification based on the binary representation of the topology of fingerprints]. *Informatika i ee primenenija*, 2012, vol. 6, no. 1, pp. 132—140.

26. **Harin E. A., Goncharov S. M., Kornjushin P. N.** Postroenie sistem biometricheskoj autentifikacii s ispol'zovaniem generatorafkljuchevyh posledovatel'nostej na osnove nechetkih dannyh [Design and construction of biometric authentication using the key sequence generator based on fuzzy data], *Mater. 50-th Vseros. mezhvuz. nauch.-tehn. konf., Vladivostok, TOVMI, 2007*, pp. 112—115.

27. **Goncharov S. M., Borshevnikov A. E.** Nejrosetevoj preobrazovatel' "biometrija — kod dostupa" na osnove myslennogo pin-koda [Neural network converter "biometrics — access code" on the basis of mental pin-code], *Trudy nauchno-tehnicheskoj konferencii klastera penzenskih predprijatij, obespechivajushhih bezopasnost' informacionnyh tehnologij*, Penza, 2014, vol. 9, pp. 46—50.

28. **Medl' A., Shtefan Je., Mjuller R.** *Sposob i sistema dlja generirovanija nabora kljucha dostupa, a takzhe dlja autentifikacii cheloveka na osnove ego biometricheskogo parametra* [A method and system for generating a set of access key, and for authenticating a person based on his biometric], Patent RU № 2267159. 2005. Bulletin № 36.

29. **Efimov O. V., Ivanov A. I., Funtikov V. A.** Sposob identifikacii cheloveka po ego biometricheskomu obrazu [A method of identifying a person by his biometric images], Patent Ru № 2292079, 2005.

30. **GOST P 52633.0—2006.** Zashhita informacii. Tehnika zashhity informacii. Trebovanija k sredstvam vysokonadezhnoj biometricheskoj autentifikacii. [Protection of information. Security technique. Requirements for means of highly reliable biometric authentication]. Moscow, 2007.

31. **Chmora A. L., Urivskij A. V.** Biometricheskaja sistema autentifikacii, [Biometric authentication], *Patent Ru № 2316120*, 2008, Bulletin N 3.

32. **Ivanov A. I.** *Sposob bezopasnoj biometricheskoj autentifikacii* [Way to secure biometric authentication], Patent Ru № 2406143, 2010.

33. **Ivanov A. I.** *Nejrosetevaja zashhita konfidencial'nyh biometricheskih obrazov grazhdanina i ego lichnyh kriptograficheskih kljuchej* [Neural protection of sensitive biometric image of the citizen and his personal cryptographic keys], Penza, 2014, 57 p.

34. **Bezjaev A. V., Ivanov A. I., Funtikova Ju. V.** Optimizacija struktury samokorrektirujushhegosja bio-koda, hranjashhego sindromy oshibok v vide fragmentov hesh-funkcij [Optimization of structure of bio self-correcting code stored syndromes errors in the form of fragments of hash functions], *The Bulletin of the Ural Federal District. Security in the field of information*, 2014, no. 3 (13), pp. 4—14.

35. **GOST P 52633.5—2011.** Protection of information. Security technique. Automatic learning of neural network converters biometrics — access code: 01.12.2011, Moscow, Standartinform, 2012, 20 p.

36. **Sulavko A. E.** Programmnyj kompleks dlja bystrogo prototipirovanija sistem raspoznavanija obrazov [Software package for rapid prototyping systems, pattern recognition] *Tezisy II Vserossijskoj konferencii "Teorija i praktika Uspeha",* Omsk, 10—11 April 2014, pp. 21—22.

37. **Epifancev B. N., Lozhnikov P. S., Sulavko A. E.** Sravnenie algoritmov kompleksirovanija priznakov v zadachah raspoznavanija obrazov [Comparison of algorithms for aggregation features in pattern recognition problems] *Voprosy zashhity informacii*, 2012, no. 1, pp. 60—66.