Protection of Biometric Information in the Framework of Aviation Security Procedures

D.I. Loboda

Azerbaijan National Aviation Academy (Mardakan ave. 30, Baku, AZ1045, Azerbaijan)

For correspondence:

Loboda Dmitriy / e-mail: dloboda@naa.edu.az

Abstract

One of the modern systems capable of countering the threat of terrorism in the air transport is a biometric identification system. An important issue in improving the aviation security system is also a protection of the biometric information and the biometric systems. The methodological basis of study, conducted in this article, is the analysis of mathematical models of the biometric identification systems. The application of software and hardware systems for the protection of biometric information is considered, and the main methods for identifying parameters and patterns of biometric identification are analyzed.

Keywords: *biometrics, identification, biometric feature, biometric template.*

DOI 10.52171/2076-0515_2022_14_04_21_28

Received *02.01.2022*
Revised *09.12.2022*
Accepted *12.12.2022*

For citation:
Loboda D.I.
[Protection of biometric information in the framework of aviation security procedures]
Herald of the Azerbaijan Engineering Academy, 2022, vol. 14, no. 4, pp. 21-28 *(in Russian)*

Aviasiya təhlükəsizliyi prosedurları çərçivəsində biometrik məlumatların mühafizəsi

D.İ. Loboda
Azərbaycan Milli Aviasiya Akademiyası (Mərdəkan pr. 30, Bakı, AZ1045, Azərbaycan)

Yazışma üçün:
Loboda Dmitriy / e-mail: dloboda@naa.edu.az

Xülasə

Hava nəqliyyatında terror təhlükəsinə qarşı durmağa qadir olan müasir sistemlərdən biri də biometrik identifikasiya sistemidir. Aviasiya təhlükəsizliyi sisteminin təkmilləşdirilməsində mühüm məsələ həm də biometrik məlumatların və biometrik sistemlərin mühafizəsidir. Bu məqalədə aparılan tədqiqatın metodoloji əsasını biometrik identifikasiya sistemlərinin riyazi modellərinin təhlili təşkil edir, biometrik məlumatların mühafizəsi üçün proqram və aparat sistemlərinin istifadəsi nəzərdən keçirilir və biometrik identifikasiyanın parametrlərinin və qanunauyğunluqlarının müəyyənləşdirilməsinin əsas üsulları təhlil edilmişdir.

Açar sözlər: *biometriya, identifikasiya, biometrik xüsusiyyət, biometrik şablon.*

DOI 10.52171/2076-0515_2022_14_04_21_28

УДК 629.7

Защита биометрической информации в рамках процедур авиационной безопасности

Д.И. Лобода
Азербайджанская Национальная академия авиации (Мардакянский пр. 30, Баку, AZ1045, Азербайджан)

Для переписки:
Лобода Дмитрий / e-mail: dloboda@naa.edu.az

Аннотация

Одной из современных систем, способных противостоять угрозе терроризма на воздушном транспорте, является биометрическая система идентификации. Немаловажным вопросом в совершенствовании системы авиационной безопасности является также защита биометрической информации и биометрических систем. Методологическую основу исследования, проведенного в данной статье, составляет анализ математических моделей систем биометрической идентификации. Рассматривается применение программно-аппаратных комплексов для защиты биометрической информации, а также анализируются основные методы выявления параметров и закономерностей биометрической идентификации.

Ключевые слова: *биометрия, идентификация, биометрический признак, биометрический шабло*.

Введение

Гражданская авиация на данный момент является транспортным сектором, наиболее подверженным чрезвычайным ситуациям - акты незаконного вмешательства отрицательно сказываются на работе данного сектора транспорта. Обеспечение авиационной безопасности стоит на первом месте среди основных задач гражданской авиации.

Безопасности уделяется особое внимание в связи с обострением политического и экономического шпионажа, международного терроризма, национализма, разжигания идеологических и религиозных распрей.

В рамках деятельности государства методы борьбы с терроризмом в правовом и организационном аспекте заключаются в предупреждении и пресечении террористических актов, осуществлении совместных мероприятий правоохранительных органов по выявлению террористических угроз и осуждению терроризма на мировом уровне. С 70-х годов прошлого века террористы совершали террористические акты, проходя пункты паспортного контроля в аэропортах и других стратегических объектах, используя поддельные паспорта и проездные документы.

Одной из современных систем, способных противостоять данным угрозам, является ***биометрическая система идентификации.*** В целях противостояния угрозам перспективным направлением совершенствования системы авиационной безопасности авиапредприятий является внедрение биометрических технологий.

Немаловажным вопросом в совершенствовании системы авиационной безопасности является также защита биометрической информации и биометрических систем. Полученная незаконным путем биометрическая информация или атаки злоумышленника на биометрическую систему может быть использована в осуществлении террористических актов на воздушном транспорте. Хронология террористических актов указывает на то, что для обеспечения безопасности гражданской авиации и предотвращения актов незаконного вмешательства в её деятельность должно быть акцентировано особое внимание при проведении паспортного контроля.

Одной из основных и современных технологий, обеспечивающих безопасность данного процесса на высоком уровне, является ***биометрическая технология.*** Биометрические технологии на данный момент используются в различных сферах деятельности и показывают свою надежность. Для обеспечения безопасности гражданской авиации важно изучение данной технологии и дальнейшее применение её в гражданской авиации.

Цель работы состоит в решении теоретических и прикладных вопросов использования биометрических систем идентификации для обеспечения авиационной безопасности.

Постановка задачи

Биометрические технологии являются ответной реакцией на удаление методов, традиционно использующихся для идентификации подозрительных лиц. С помощью такого вида идентификации можно отследить все перемещения индивида, которые он осуществлял.

Всеобщее внедрение биометрических технологий идентификации даст возмож-

ность противодействовать характерной черте терроризма – анонимности. “Идентифицировать” - означает сделать неизвестного человека известным, с помощью стабильных методов идентификации [1]. Но и в данном методе есть свои определённые недостатки и проблемы применения. Биометрические системы распознают людей на основе их физиологических особенностей (радужной оболочки, отпечатков пальцев, голоса, образа лица, рисунка линий ладони) или поведенческих черт (подписи, походки). В отличие от паролей, где нужно полное соответствие введенного вами пароля, биометрическая система идентификации основывается на степени схожести двух биометрических образцов.

Если посмотреть на наш современный образ жизни, биометрическими системами мы пользуемся постоянно. Мы разблокируем телефон с помощью отпечатка пальца, производим транзакции с банковской карты при помощи FaceID и многое другое. Но есть одна особенность, которая заставляет нас сосредоточить все ресурсы для обеспечения безопасности данной системы. Если пароль или же ID карту при краже мы можем заблокировать и поменять, то в случае биометрических систем такое невозможно. Биометрический признак даётся нам при рождении и является неизменным на протяжении всего жизненного цикла. И “сменить” его у нас не получится.

Биометрическая система также может быть скомпрометирована в результате атак, которые могут проводиться путем взлома системы биометрической идентификации через инсайдеров, управляющих данной системой. Злоумышленники также могут оказать воздействие на биометрическую систему посредством прямых атак на сканирующие датчики, модули экстракции черт или модули сопоставления. Также атаки могут быть направлены на повреждение либо перехват информации в соединительных узлах, либо в самой базе данных шаблонов.

Как же защитить такую глобальную систему от атак злоумышленников?

Решение задачи

Все атаки, производимые на различные модули биометрической системы, могут быть в равной степени использоваться для различных способов идентификации.

В процессе проведения биометрической идентификации система может быть подвержена атакам злоумышленников на разных этапах:

1) атака на устройство ввода;
2) атака на канал связи;
3) атака на параметризацию сигнала;
4) атака на канал передачи сигнала;
5) атака на элемент сравнения параметра и шаблона;
6) атака на элемент сравнения;
7) атака на канал связи с базой;
8) атака на элемент регистрации;
9) атака на канал между элементом регистрации и базой;
10) атака на элемент базы;
11) атака на приложение.

Все перечисленные выше атаки являются схожими для любой системы биометрической идентификации. Защита биометрической системы от подобных атак заключается в использовании временных меток, шифрования открытого канала передачи биометрических данных и цифрового кодирования [2]. На рис 1 продемонстрированы типичные атаки на биометрические системы.

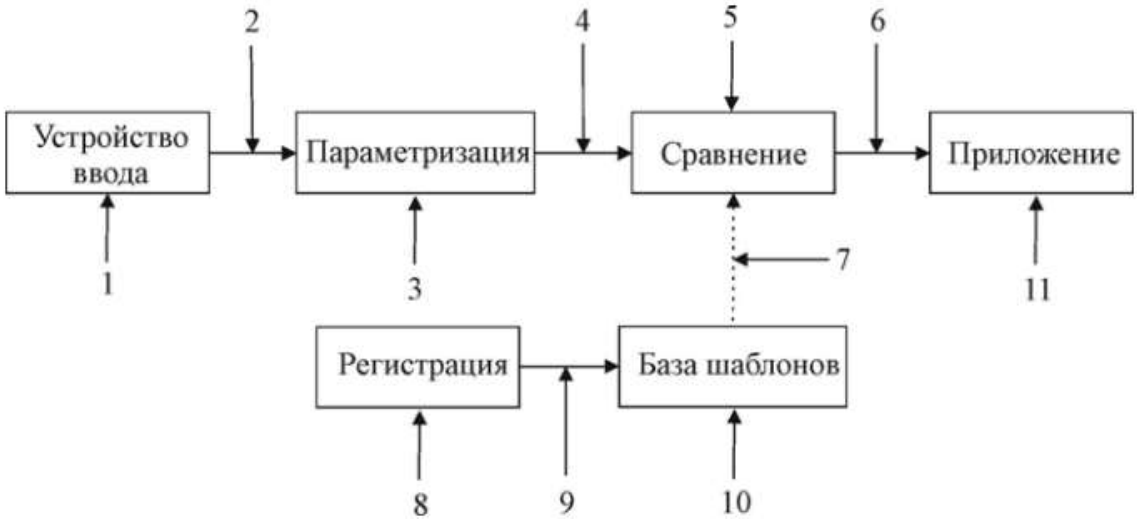

Рисунок 1 – Общая схема аутентификации с обозначенными атаками
Figure 1 – General authentication scheme with identity attacks

Имеется два общих принципа защиты биометрических шаблонов: биометрические криптосистемы и трансформация биометрических черт.

В случае ***трансформации биометрических черт*** (рис.2а) защищенный шаблон получен за счет применения необратимой функции трансформации к оригиналу шаблона. Такая трансформация обычно основана на индивидуальных характеристиках пользователя. В процессе аутентификации система применяет ту же функцию трансформации к запросу, и сопоставление происходит уже для трансформированного образца [3, 4].

Биометрические криптосистемы (рис. 2б) хранят только небольшой процент информации, полученной из биометрического шаблона, - эта часть называется ***защищенным эскизом (secure sketch).*** Хоть его самого недостаточно для восстановления оригинального шаблона, он все же содержит достаточное количество данных для восстановления шаблона при наличии другого биометрического образца, похожего на полученный при регистрации.

Защищенный эскиз обычно получают путем связывания биометрического шаблона с криптографическим ключом, однако защищенный эскиз - это не то же самое, что биометрический шаблон, зашифрованный с помощью стандартных методов. Когда системе предоставляют биометрический запрос, достаточно похожий на шаблон, она может восстановить и оригинальный шаблон, и криптоключ с помощью стандартных методов распознавания ошибок.

При обычной криптографии зашифрованный шаблон и ключ расшифровки - это два разных элемента, и шаблон защищен, только если защищен и ключ. В защищенном шаблоне же инкапсулируются одновременно и биометрический шаблон, и криптографический ключ. Ни ключ, ни шаблон нельзя восстановить, имея только защищенный эскиз.

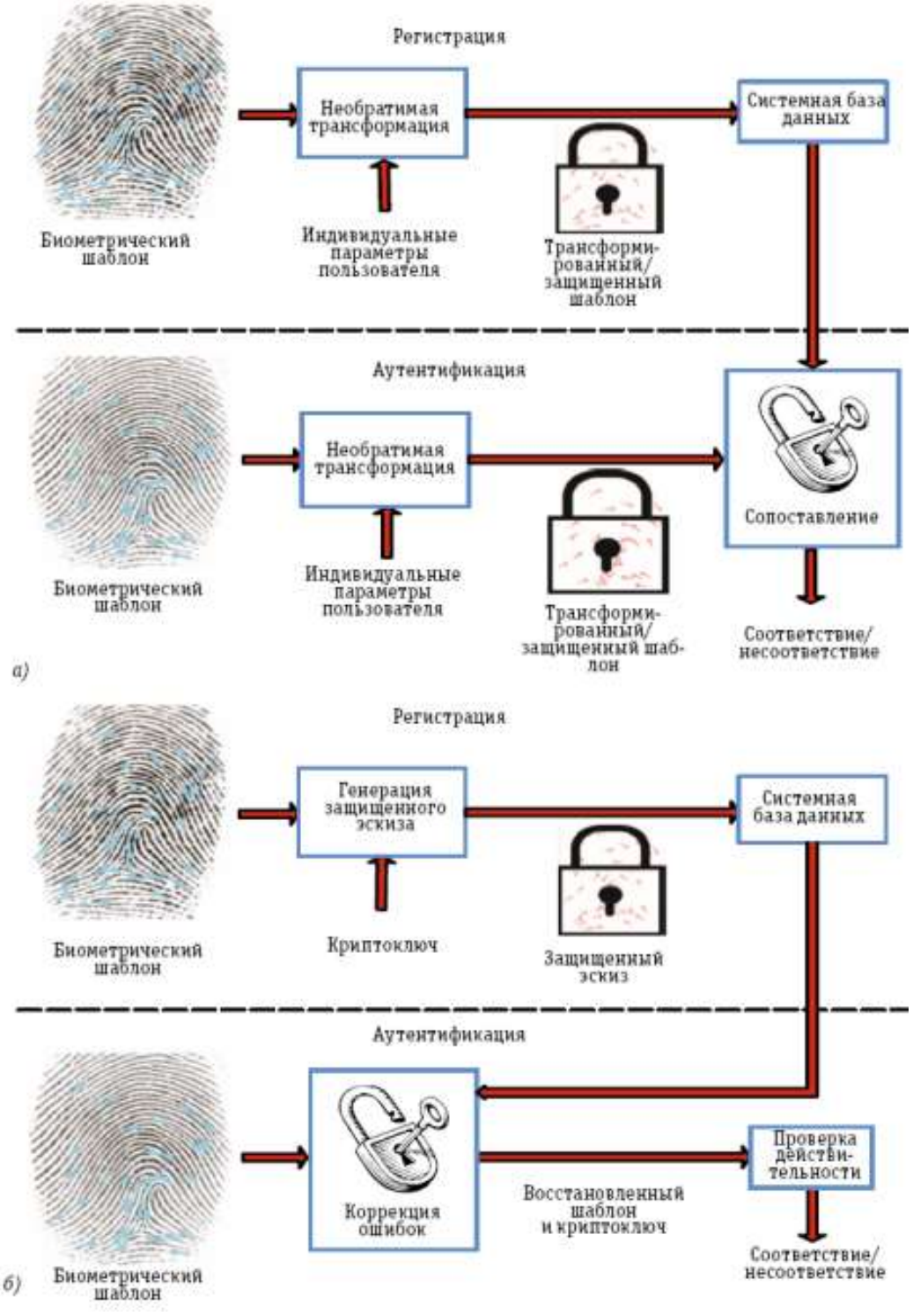

Рисунок 2 – Защита шаблонов с помощью:
а - трансформации биометрических черт; б - биометрических криптосистем
Figure 2 – Protection of templateswiththehelp of:
a - transformation of biometricfeatures; b – biometriccryptosystems

Помимо вышеперечисленных методов, к одним из наиболее прогрессивных методов защиты биометрической информации можно отнести ***гибридное шифрование*** – шифрование с открытым и симметричным ключом. Зашифрованная информация прерывается открытым ключом, а также обеспечивает симметричное шифрование. В этой схеме порт и сервер создают симметричный ключ и шифруют информацию через него. Затем они используют один из открытых ключей для шифрования симметричного.

Шифрование возможно только с помощью ключа, используемого в процедуре в то время (рис. 3).

При доступе к серверу личная информация сохраняется как пользовательское имя в имени персонального сервера, но биометрическая информация регистрируется на биометрическом сервере и хранится в зашифрованном состоянии [5].

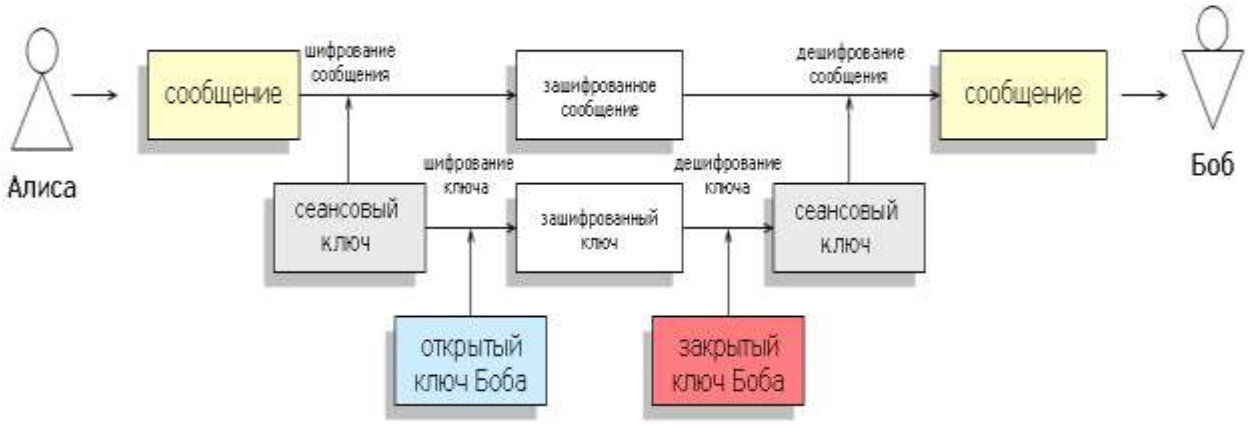

Рисунок 3 – Передачи данных с использованием гибридного шифрования
Figure 3 – Data transmission using hybrid encryption

Этап отправки:

- Алиса генерирует случайный сеансовый ключ;
- сообщение Алисы шифруется сеансовым ключом (с помощью симметричного алгоритма);
- сеансовый ключ шифруется открытым ключом Боба (асимметричным алгоритмом);
- Алиса посылает Бобу зашифрованное сообщение и зашифрованный сеансовый ключ.

Этап приёма:

- Боб получает зашифрованное сообщение Алисы и зашифрованный сеансовый ключ;
- Боб расшифровывает сеансовый ключ своим закрытым ключом;
- при помощи полученного таким образом сеансового ключа Боб расшифровывает зашифрованное сообщение Алисы.

Преимущества данной системы заключаются в разделение каждой записи в биометрической системе в два хранилища. Первое - для личной информации, второе - для биометрической информации.

Важно отметить, что каждое из этих хранилищ будет содержать *n* записей, но записи не будут связаны друг с другом [6].

Таким образом, если злоумышленник получает доступ к серверу, он не сможет распознать связь между личной и биометрической информацией.

Заключение

Проанализированы математические модели систем биометрической идентификации, рассмотрено применение программно-аппаратных комплексов для защиты биометрической информации, а также приведены основные методы выявления параметров и закономерностей биометрической идентификации.

Конфликт интересов

Автор заявляет об отсутствии конфликта интересов, связанных с публикацией данной статьи.

REFERENCES

1. **Sanjekar P.S., Patil J.B.** An overview of multimodal biometrics. *Signal & Image Processing: An International Journal (SIPIJ),* Vol.4, No.1, February 2013 *(in English)*
2. **Boll R.M., Konnel J.H.** Rukovodstvo po biometrii: Texnosfera, 2007. -368 s. *(in Russian)*
3. **Schuckers S.A.** Spoofing and Anti-Spoofing Measures. *Information Security Technical Report, Elsevier.* 2002. V. 7. No 4. Pp. 56-62. *(in English)*
4. **Pastushenko O.N., Nevlyudov I.S.** Analiz kacestvennix pokazateley biometriceskix system autentifikaci i polzivateley. *Xarkovskiy nacionalniy universitet radioelektroniki.* 2012. – 4 s. *(in Russian)*
5. http://ama.com.az/aze/arxiv/
6. **Modern I.J.** Development of Electronic Passport Scheme for Cryptographic Security and Face, Fingerprint Biometrics using ASP.*Net, Education and Computer Science,* 2012, p. 49 *(in English)*