3. *Малюгин В.Д.* Параллельные логические вычисления посредством арифметических полиномов. М.: ФИЗМАТЛИТ, 1997. – 192 с.
4. *Yanushkevich S., Shmerko V., Lyshevski S.* Logic design of nanoICs. CRC Press, 2005.
5. *Шалыто А.А.* Логическое управление. Методы аппаратной и программной реализации алгоритмов. – СПб.: Наука, 2000. – 780 с.
6. *Вишневский А.К., Финько О.А.* Реализация некоторых криптографических функций линейными числовыми полиномами // 4-я Международная научно-техническая конференция «Инфокоммуникационные технологии в науке, производстве и образовании». – Ставрополь, 2010. – С. 20-23.
7. *Белоусов А.И., Ткачев С.Б.* Дискретная математика: Учеб. для вузов / Под ред. В.С. Зарубина, А.П. Крищенко. – 3-е изд., стереотип. – М.: Изд-во МГТУ им. Н.Э. Баумана, 2004. – 744 с. (Сер. Математика в техническом университете. Вып. XIX).
8. *Шнайер Б.* Прикладная криптография. Протоколы, алгоритмы, исходные тексты на Си. – М.: ТРИУМФ, 2003. – 816 с.

Вишневский Артем Константинович
Краснодарское высшее военное училище (ВИ).
E-mail: vishn.artem@yandex.ru.
350035, г. Краснодар, ул. Красина, 4.
Тел.: +79094603415.

Шарай Вячеслав Александрович
Кубанский государственный технологический университет.
Институт информационных технологий и безопасности.
E-mail: ofinko@yandex.ru.
350072, г. Краснодар, ул. Московская, 2.
Тел.: +79615874848.

Vishnevsky Artem Konstantinovich
Krasnodar higher military school (MI).
E-mail: vishn.artem@yandex.ru.
4, Krasina, Krasnodar, 350035, Russia.
Phone: +79094603415.

Sharai Viacheslav Aleksandrovich
Kuban state technological university.
Institute of information technologies and safety.
E-mail: ofinko@yandex.ru.
2, Moscow, Krasnodar, 350072, Russia.
Phone: +79615874848.

УДК 004.056:378 (06)

С.Э. Бардаев

МНОГОФАКТОРНАЯ БИОМЕТРИЧЕСКАЯ ПОРОГОВАЯ КРИПТОСИСТЕМА

Предложена биометрическая криптосистема, полученная путем интеграции многофакторной биометрии, пороговой криптографии (схема Шамира) и методов преобразования нечетких биометрических параметров в ключевые последовательности, а также обсуждены преимущества такого решения.

Многофакторная биометрия; пороговые криптографические системы; преобразователь «биометрия – код»; биометрическая криптография; схема Шамира.

S.E. Bardaev, O.A. Finko

MULTIFACTOR BIOMETRIC THRESHOLD CRYPTOSYSTEM

The biometric cryptosystem received by integration of a multifactor biometry, threshold cryptography (Shamir's scheme) and methods of conversion of indistinct biometric parametres in key sequences, together with advantages of such association is considered.

Multifactor biometry; threshold cryptography; the converter «biometry – a code»; biometric cryptography; Shamir's scheme.

Интеграция биометрических и криптографических технологий открывает новые перспективы в сфере обеспечения информационной безопасности [1, 2]. В частности, объединение таких направлений, как *многофакторная биометрия*, *пороговая криптография с разделением секрета* и *методы преобразования нечетких биометрических параметров в ключевые последовательности*, образует новое направление в сфере защиты информации – *многофакторную биометрическую криптографию* (рис. 1) [3]. Данное направление позволяет создавать криптосистемы разделения секрета по биометрическим параметрам участников системы. Восстановить секрет такой многофакторной биометрической пороговой криптосистемы может участник, обладающий необходимым набором соответствующих биометрических параметров, или участники, в совокупности обладающие необходимым количеством параметров.

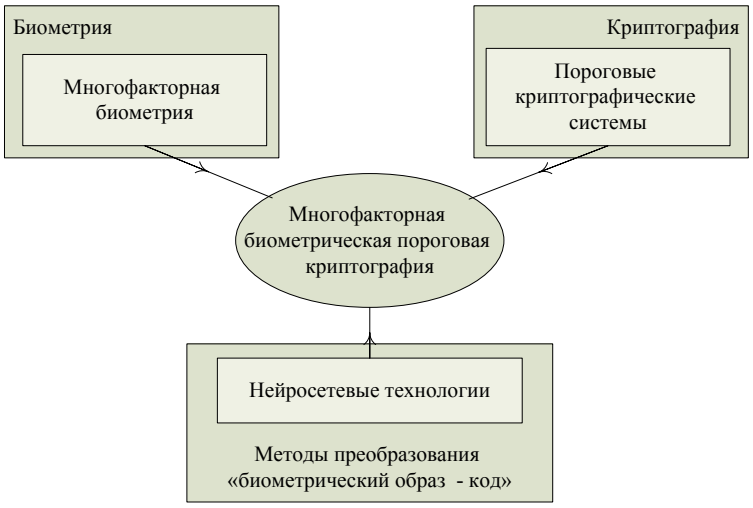

Рис. 1. Интеграция многофакторной биометрической криптографии из трех направлений

Многофакторная биометрия. В многофакторной биометрии для аутентификации используется совокупность нескольких биометрических технологий, например: отпечатки нескольких пальцев, лицо и сетчатка глаза, голос и почерк в различных комбинациях [4]. Качество биометрической аутентификации определяется вероятностями возникновения ошибок первого рода (FRR – англ. False Rejection Rate), когда система отказывает в доступе авторизованному пользователю, и ошибок второго рода (FAR – англ. False Acceptance Rate), когда доступ к системе ошибочно предоставляется неавторизованному пользователю. Необходимо учитывать взаимосвязь этих показателей: искусственном снижении уровня «требовательности» системы (FAR), как правило, уменьшается процент ошибок FRR, и наоборот.

Преимущество многофакторной биометрии выражено в том, что с увеличением количества проверяемых биометрических параметров существенно улучшается качество аутентификации.

Биометрическая криптография [5, 6]. В зависимости от цели применения биометрии в криптографии выделяются несколько видов биометрических криптографических систем: *системы с освобождением ключа* (англ. key release cryptosystems), *системы со связыванием ключа* (англ. key binding cryptosystems) и *системы с генерацией ключа* (англ. key generation cryptosystems) (рис. 2.).

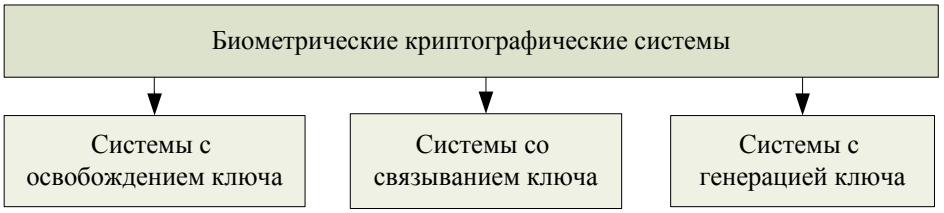

Рис. 2. Виды биометрических криптографических систем

1. *Биометрические криптографические системы с освобождением ключа.* В режиме освобождения ключа биометрическая аутентификация осуществляется независимо от механизма освобождения ключа, биометрический эталон и ключ хранятся отдельно друг от друга, сам ключ освобождается после успешной биометрической аутентификации. Данный вид биометрических криптосистем неприменим в большинстве случаев, поскольку существует возможность замены модуля сравнения при выполнении аутентификации.

2. *Биометрические криптографические системы со связыванием ключа.* В криптографических системах такого типа ключ и биометрический эталон криптографически связаны между собой. Ключ закрывается биометрическим эталоном пользователя и сохраняется в таком виде в базе данных, соответственно раскрыть ключ представляется возможным только обладателю биометрических параметров.

3. *Биометрические криптографические системы с генерацией ключа.* В такой биометрической криптосистеме ключ извлекается непосредственно из биометрических данных пользователя и не хранится в базе данных. Возможность не хранить ключ, полученный из биометрических данных, является неоспоримым преимуществом метода генерации криптографических ключей из биометрических данных пользователя по сравнению с другими существующими методами.

Таким образом, главным отличием двух последних видов биометрических криптосистем является то, что в одном из них криптографический ключ только закрывается при помощи биометрического эталона, а в другом ключ генерируется непосредственно из биометрических данных пользователя.

Методы преобразования «биометрический образ – код». Применение биометрического материала в качестве источника ключевой информации наталкивается на ряд сложностей: биометрические данные нечетко воспроизводимы и не имеют равномерного распределения, в то время как большинство криптографических преобразований требуют точного значения длины ключа. Кроме того, биометрические данные обладают рядом особенностей, которые создают сложности при использовании этих данных в качестве источника ключевого материала:

- биометрические данные могут изменяться со временем и в зависимости от физического и эмоционального состояния их владельца;
- проблема смены ключей – биометрические данные неотзываемы;

- невозможность держать биометрические данные в тайне, например, отпечатки пальцев могут быть оставлены на различных поверхностях, а изображение радужной оболочки глаза может быть зафиксировано камерой.

За последние несколько лет были предприняты многочисленные попытки создания методов генерации ключей из различных биометрических данных. Однако в большинстве работ длина ключей очень мала, а вероятность ошибки второго рода превышает 20 %, что неприемлемо для практического применения. На данный момент существуют два пути решения проблемы, наиболее удовлетворяющие требованиям: технология использования *нечетких экстракторов*, и использование больших *нейронных сетей*, заранее обученных преобразованию биометрического образа пользователя в его личный ключ (рис. 3).

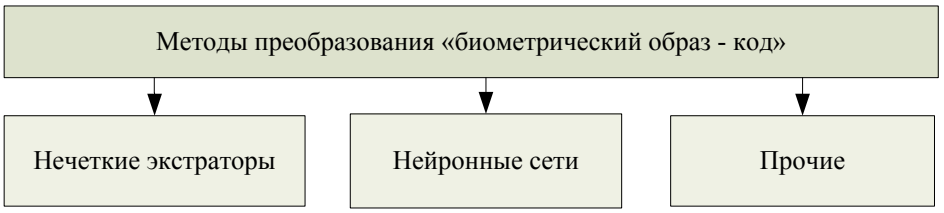

Рис. 3. Методы преобразования «биометрический образ – код»

1. *Нечеткие экстраторы* [7]. Данный способ позволяет однозначно восстанавливать секретный ключ из неточно воспроизводимых биометрических данных. Длина ключа задается в виде параметра, при этом для воспроизведения ключа требуются дополнительные открытые данные, соответствующие ключу, которые хранятся в памяти. Метод нечетких экстракторов извлекает случайную равномерно распределенную последовательность из первоначальных входных данных и далее правильно восстанавливает ее из любых данных, достаточно схожих с первоначальными. «Нечеткий экстрактор» позволяет получать только один ключ, качество выходной ключевой последовательности которого удовлетворяет всем критериям качества криптографических ключей.

2. *Нейронные сети*. Нейросетевой преобразователь «биометрия-код» – заранее обученная искусственная нейронная сеть с большим числом входов и выходов, преобразующая частично случайный вектор входных биометрических параметров «СВОЙ» в однозначный код криптографического ключа (длинного пароля) и преобразующая любой иной случайный вектор входных данных в случайный выходной код [8]. В отличие от парольной аутентификации, при биометрическо-нейросетевой аутентификации вместо хэша ключа хранится 256-битный код, полученный преобразованием тайного биометрического образа человека. Нейросетевой преобразователь «биометрия-код» способен после процедуры быстрого автоматического обучения преобразовывать нечеткие биометрические образы в однозначный код с криптографической стойкостью. Помимо многократного ускорения процедур обучения искусственных нейронных сетей и полной автоматизации процедур обучения, при использовании технологии высоконадежной биометрической аутентификации появляются гарантии безопасности, конфиденциальности, анонимности аутентификации, и доступности для использования рядовым гражданином [9].

Пороговые криптографические системы. Для реализации многофакторной биометрической криптографической системы возможно использование любой пороговой криптосхемы разделения секрета, например схемы Блэкли, схемы Шамира, схемы, основанной на Китайской теореме об остатках и других [11]. Криптографически связать получаемые доли секрета и биометрические параметры обла-

дателя соответствующей ключевой информации возможно, например, с помощью алгоритма шифрования ГОСТ 28147-89. В данном случае получится биометрическая криптографическая система со связыванием ключа. Для того чтобы избавиться от необходимости хранить криптографический ключ, необходимо построить биометрическую криптографическую систему с генерацией ключа. Однако это возможно при использовании *пороговых криптосхем* разделения секрета, обладающих некоторой избыточностью. Например, позволяющие определять доли секрета по определенному правилу в зависимости от последовательности, полученной с преобразователя «биометрия-код», или позволяющие использовать эту последовательность непосредственно в процессе вычисления долей секрета.

Пример реализации многофакторной биометрической пороговой криптографической системы разделения секрета с генерацией ключа, основанной на схеме Шамира. Многофакторная биометрическая пороговая схема разделения секрета $(k,\ n)$ определяется следующим образом (рис. 4):

- n источников биометрической ключевой информации b_i разделяют секрет s среди m участников, каждый из которых обладает w_j источниками биометрических параметров b_i , где $1 \le j \le m, 1 \le i \le n$, а $\sum_{j=1}^{m} w_j = n$;
- каждый участник – обладатель биометрических параметров владеет w_j количеством долей $\{b_i,\ I_i\}$ секрета s, стоит отметить, что w_j характеризует вес j-го участника в системе;
- секрет s может быть вычислен из любых k долей $\{b_i,\ I_i\}$ секрета;
- $k-1$ долей секрета $\{b_i,\ I_i\}$ не дают никакой информации о секрете s.

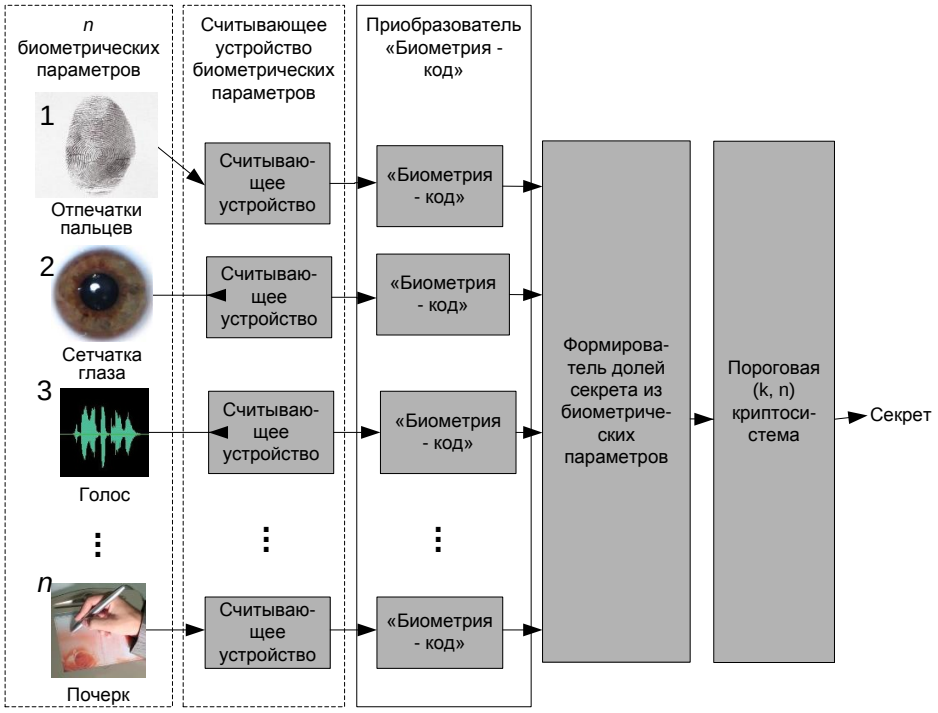

Рис. 4. Поясняющая блок-схема многофакторной биометрической пороговой криптосистемы

Основная идея схемы Шамира заключается в том, что для задания многочлена степени $k-1$ достаточно и необходимо k точек и базируется на полиномиальной интерполяции [11]. Отсюда, имея любые k пары $\{x_1, y_1\}, \dots, \{x_k, y_k\}$, где $x_i \neq x_j$ для любых $1 \leq i \leq j \leq k$, возможно существование одного единственного полинома $P(x)$ степени $k-1$, такого что $P(x_i) = y_i$ для всех $1 \leq i \leq k$:

- секрет s выбирается случайным образом, и используется в качестве свободного коэффициента полинома $P(x)$ степени $k-1$ из множества положительных целых чисел по модулю большого простого числа;
- доли секрета $\{b_i,\ I_i\}$ вычисляются $I_i = P(x_i)$ для всех $1 \leq i \leq n$, при значениях $x_i \neq b_i$, причем $b_i \neq b_j$, т.е. доли секрета $\{b_i,\ I_i\}$ являются координатами точек указанного многочлена, b_i – биометрическая составляющая доли секрета, а I_i – изменяемая составляющая, которая вычисляется и может храниться в защищенной базе данных или на отдельном носителе ключевой информации участника (смарт-карта, USB-токен и т.д.) [12, 13]. Отметим, что в качестве биометрической составляющей доли секрета возможно использование и классических способов аутентификации (пароль);
- наличие долей секрета $\{b_i,\ I_i \mid i \in A\}$ для некоторой группы A с $|A| = k$ позволяет вычислить полином $P(x)$, используя интерполяционную формулу Лагранжа:

$$P(x) = \sum_{j=0}^{n} I_j\, l_j(x), \tag{1}$$

где базисные полиномы определяются по формуле:

$$l_j(x) = \prod_{i=0, j\neq i}^{n} \frac{x - x_i}{x_j - x_i}. \tag{2}$$

И тем самым получить секрет $s = P(0)$.

Если представить полином $P(x)$ в виде многочлена степени $k-1$:

$$P(x) = a_0 + a_1 x^1 + \cdots a_{k-1} x^{k-1},$$

то секрет также может быть вычислен, решив систему уравнений:

$$\begin{cases} a_0 + a_1 x_{i_1}^1 + \cdots + a_{k-1} x_{i_1}^{k-1} = I_{i_1}, \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ a_0 + a_1 x_{k_1}^1 + \cdots + a_{k-1} x_{k_1}^{k-1} = I_{k_1}. \end{cases}$$

Вышеупомянутая система имеет k уравнений и k неизвестных $a_0, a_1, \dots, a_{k-1}$ и имеет единственное решение, потому что детерминант

$$\begin{vmatrix} x_{i_1}^{k-1} & \cdots & x_{i_1}^1 & 1 \\ x_{i_2}^{k-1} & \cdots & x_{i_2}^1 & 1 \\ \vdots & \ddots & \vdots & \vdots \\ x_{i_k}^{k-1} & \cdots & x_{i_k}^1 & 1 \end{vmatrix}$$

является ненулевым детерминантом Вандермонда.

Схема Шамира является совершенной. Действительно, только при наличии $k-1$ долей секрета система уравнений

$$\begin{cases} a_1 x_{i_1}^1 + \cdots + a_{k-1} x_{i_1}^{k-1} = I_{i_1} - a_0, \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ a_1 x_{k_1}^1 + \cdots + a_{k-1} x_{k_1}^{k-1} = I_{k_1} - a_0 \end{cases}$$

с $k-1$ уравнениями и $k-1$ неизвестными $a_1, \dots, a_{k-1}$ имеет единственное решение для любых a_0, т.е. все возможные значения секрета равновероятны.

Алгоритмы. Рассмотрим алгоритмы работы (k, n) многофакторной биометрической пороговой криптографической системы разделения секрета с генерацией ключа, основанной на схеме Шамира.

Алгоритм 1: Выработка ключевой информации.

Ввод: (k, n), b_i, где $1 \le i \le n$.

Вывод: I_i.

Шаг 1: Ввести биометрические параметры b_i.

Шаг 2: Преобразовать нечеткие биометрические параметры в ключевую последовательность h_i.

Шаг 3: Выбрать случайным образом $a_1, \dots, a_{k-1}$ и секрет $s = a_0$.

Шаг 4: Задать многочлен $P(x)$ степени $k-1$, зная коэффициенты $a_0, a_1, \dots, a_{k-1}$:

$$P(x) = a_0 + a_1 x^1 + \cdots a_{k-1} x^{k-1}.$$

Шаг 4: Вычислить значения $I_i = P(x_i)$ для всех $1 \le i \le n$, при значениях $x_i = h_i$, причем $h_i \ne h_j$.

Алгоритм 2: *Получение секрета.*

Ввод: $\{b_i, I_i\}$, где $1 \le i \le n$.

Вывод: s.

Шаг 1: Ввести биометрические параметры b_i.

Шаг 2: Преобразовать нечеткие биометрические параметры в ключевую последовательность h_i.

Шаг 3: Вычислить базисные полиномы для формулы Лагранжа (2), при $x_i = h_i$.

Шаг 4: Вычислить интерполяционный многочлен Лагранжа (1).

Шаг 5: Вычислить секрет $s = P(0)$.

Особенности системы:

- высокая криптостойкость (схема Шамира является совершенной);
- размер изменяемой составляющей I_i доли секрета не превышает размера самого секрета s;
- возможность задавать значимость каждого участника путем изменения веса w_j участника;
- при увеличении веса w_j j-го участника увеличивается качество биометрической аутентификации данного j-го участника (существенно уменьшаются вероятности ошибок 1-го и 2-го родов биометрической аутентификации);
- отсутствует необходимость хранения криптографического ключа (ключ вырабатывается непосредственно перед криптопреобразованием из биометрических параметров участников);
- возможность использования неквалифицированного персонала, так как отсутствует необходимость установления организационных мер защищенного использования, хранения и передачи ключевой информации;
- обладание в отдельности биометрическими составляющими b_i или изменяемыми составляющими I_i долей секрета s, а также $k-1$ парами $\{b_i, I_i\}$ не дает никакой информации о секрете s;
- проблема смены ключей решается сменой изменяемой составляющей I_i доли секрета, а также возможно решение путем чередования используемых биометрических технологий и применением изменяемых биометрических параметров;

- система является динамичной, т.е. не изменяя порог k, существует возможность добавить несколько долей секрета, не затрагивая другие доли, для добавления дополнительных долей секрета необходимо k участников;
- доли секрета возможно сменить, не изменяя сам секрет;
- возможность использовать взамен биометрической составляющей b_i классических способов аутентификации (пароль или ключ).

Таким образом, объединение многофакторной биометрии, методов построения пороговых криптосистем разделения секрета и методов преобразования нечетких биометрических параметров в ключевые последовательности, образует новое направление в сфере защиты информации – многофакторную биометрическую криптографию, позволяющую создавать пороговые криптосистемы разделения секрета по биометрическим параметрам участников системы.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Вилле Й.* Новые пути биометрии // Журнал сетевых решений LAN. – 2005. – № 10.
2. *Ефимов О.В. Иванов А.И.* Преимущества национального российского подхода к безопасному объединению механизмов биометрии и криптографии // Труды научно-технической конференции «Безопасность информационных технологий». – Пенза, 2005. – № 6. – С. 50-52.
3. *Бардаев С.Э. Финько О.А.* Многофакторная биометрическая криптография на основе пороговых систем // Материалы XI Международной научно-практической конференции «Информационная безопасность». Часть III. / Технологический институт ЮФУ. – Таганрог, 2010.
4. *Болл Р.М., Коннел Дж.Х., Панканти Ш., Ратха Н.К., Сеньор Э.У.* Руководство по биометрии. – М.: Техносфера, 2007. – 368 с.
5. *Uludag U., Pankanti S., Prabhakar S. and Jain A.K.* Biometric cryptosystems: issues and challenges. Proceedings of the IEEE, 2004. – Vol. 92, № 6. – P. 948–960,
6. *Бабенко Л.К., Макаревич О.Б., Тумоян Е.П.* Биометрические криптосистемы. Путь к защищенной биометрии // Вестник Южного научного центра РАН. – 2005. – Т. 1, № 3. – С. 95-99.
7. *Dodis Y., Reyzin L., Smith A.* Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data // April 13, 2004.
8. ГОСТ Р 52633-2006 «Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации».
9. *Брюхомицкий Ю.А., Доцук А.Н.* Нейросетевая модель генерации криптографического ключа по биометрическим данным пользователя // Информационное противодействие угрозам терроризма. – 2006. – № 8. – С. 200-215.
10. *Heiko H.* Secret Sharing. Cryptography Seminar, 2001.
11. *Shamir A.* How to share a secret. Communications of the ACM, 22 (11):612–613, 1979.
12. *Дшхунян В.Л., Шаньгин В.Ф.* Электронная идентификация. Бесконтактные электронные идентификаторы и смарт-карты. — М.: ООО «Изд-во АСТ»: НТ Пресс, 2004.
13. *Seto Y.* Development of personal authentication systems using fingerprint withsmart cards and digital signature technologies. The Seventh International Conferenceon Control, Automation, Robotics and Vision, Dec 2002.

Бардаев Сергей Эдуардович
Краснодарское высшее военное училище (ВИ).
E-mail: bsik@bk.ru.
350035, г. Краснодар, ул. Красина, 4.
Тел.: +79615992467.

Bardaev Sergey Eduardovich
Krasnodar higher military school (MI).
E-mail: bsik@bk.ru.
4, Krasina, Krasnodar, 350035, Russia.
Phone: +79615992467.