REPORTS OF THE NATIONAL ACADEMY OF SCIENCES OF THE REPUBLIC OF KAZAKHSTAN
ISSN 2224-5227
Volume 3, Number 301 (2015), 39 – 44

UDC 004

Research and development of the certifying centers of authentication of the personality with use of biometrics-neural network technologies

T.S. Kartbayev, G.S. Beketova, K. Mukapil
kaiyrkhan@mail.ru
Kazakh National Technical University named after K.I. Satpayev, Almaty, Republic of Kazakhstan

Key words: e-government, information security, identity authentication, biometrics-neural network technology, the development of certification authorities, electronic-digital signature.

Abstract. Research and development of certification authorities authenticate the identity of a system of e-government with the use of biometrics, neural network technology is promising for the development of information and telecommunication technologies in the Republic of Kazakhstan and around the world.

Existing certification centers provide services only to support public-key certificates citizens, but citizens do not want to officially register their public key to verify the legal value of electronic digital signature. The problem is that, in parallel with the registration of the public key citizen inevitably gets an extra risk of compromising his/her private key digital signature algorithm. The above problem is relevant and should be solved within the framework of the proposed project. Its solution is to create an identity centers which not only provide traditional services for certification of public key individuals and legal entities, but also perform completely different services on a local and remote biometric authentication personality.

Target consumers of the results are public and commercial organizations engaged in the processing of personal data within the electronic document without the threat of compromise of personal and biometric data of citizens.

ӘОЖ (УДК) 004

Биометриялы-нейрожелілік технологияларды қолдана отырып, тұлға аутентификациясының куәландыру орталығын зерттеу және өңдеу

Т.С. Қартбаев, Г.С. Бекетова, К. Мукапил
kaiyrkhan@mail.ru
Қ.И. Сәтбаев атындағы Қазақ Ұлттық техникалық университеті, Алматы, Қазақстан Республикасы

Тірек сөздер: электронды үкімет, ақпаратты қорғау, тұлға аутентификациясы, биометрико-нейрожелілік технологиялар, куәландыру орталықтарды өңдеу, электронды-сандық қолтаңба.

Аннотация. Электронды үкімет жүйесінде биометриялы-нейрожелілік технологияларды қолдана отырып, тұлға аутентификациясының куәландыру орталықтарын зерттеу мен өңдеу Қазақстан Республикасында да, сол сияқты барлық әлемде де ақпараттық-телекоммуникациялық технологиялардың дамуының перспективалық бағыты болып табылады.

Қазіргі кездегі бар куәландыру орталықтар азаматтардың ашық кілттері сертификаттарын қолдау бойынша ғана қызмет көрсетеді, дегенмен азаматтар электронды-сандық қолтаңбаның (ЭСҚ) заңды маңыздылығын тексеру үшін өзінің ашық кілттерін ресми түрде тіркегісі келмейді. Мәселе мынада: азамат өз ашық кілтін тіркеумен қатар ЭСҚ-сын құруда өз жеке кілтінің компрометациясына қосымша қауіпті сөзсіз қосып алады. Жоғарыда айтылған мәселе өзекті болып табылады және оның шешілуі жеке және заңды тұлғалардың ашық кілттерінің сертификатталуы бойынша дәстүрлі қызметтер көрсетіп қана қоймай, сонымен бірге, адам тұлғасының локальды және қашықтықтан биометриялық аутентификациясы бойынша мүлдем басқа қызметтерді де атқаратын жаңа буынның куәландыру орталығын құру болып отыр.

Алынған нәтижелердің мақсаттық тұтынушылары азаматтардың дербес және биометриялық

мәліметтерінің компрометациясының болу қауіпінсіз электронды құжат айналым аумағында дербес мәліметтерді өңдеуді жүзеге асыратын мемлекеттік және коммерциялық ұйымдар болып табылады.

Кіріспе. Қазіргі кезде интернет кеңістігі мен сандық мобильдік телефонияны жаппай қолдану процесі белсенді жүруде. Жуық арада сандық теледидарға көшу жүзеге асырылады, электронды үкімет және электронды кәсіпкерлік белсенді дамып жатыр. Барлық осы процестер биометрия мен криптография алдына бірқатар мәселелерді қояды. Биометриялық технологиялар саласында өткен ғасырда құрылғандары интернет кеңістігінде жүргізілмейді. Өкінішке орай, әлі де интернет жасырын, өзіне деген сенімділігі төмен иесіз орта болып келеді. Бұл бір жағынан түрлі алаяқтарға арналған орта болып табылады, ал басқа жағынан қарапайым азаматтардың жаңа ақпараттық технологияларға деген сенімін жояды.

Сондықтан, бір жағынан, интернет қызметтерін қолдануы кезінде азаматтардың анонимділігі мен тұлғасыздығын кепілді қамтамасыз ететін, ал басқа жағынан, азаматтардың тұлғасыздығы немесе анонимділігін, олардың қажеттілігі туындаған кезде, мақұлдамаушылық мүмкіндігі мен азаматтарды биометриялық тұлғасыз қуаттаудың арнайы механизмдері есебінен интернет ортасына деген сенімділікті жоғары деңгейде қамтамасыз ететін жаңа технологияларды құру қажет.

Ережеге сай, сандық технологияға көшу қолжетімді ақпарат көлемінің қарқынды өсуіне себепкер болады. Жағдайдың бұлай өзгеруі қарапайым азаматтарға хаос ретінде қабылданады. Бастапқы ақпараттық хаоспен күресу үшін сандық ақпараттың үлкен көлемінің есептілігі мен жіктелуінің арнайы механизмдерін құру қажет. Интернет кеңістігінде іздеу қызметтеріне мамандандырылған (интернетте ақпараттың үздіксіз жіктелуіне мамандандырылған) арнайы коммерциялық табысты компаниялар пайда болды. Мобильді телефондарда есеп механизмі рөлін ұялы телефондық байланыс операторының асимметриялық криптографиясы бар СИМ-карта атқарады. Қарапайым адамдар өздеріне маңызды сандық ақпараттарын қуаттау үшін электронды сандық қолтаңбаны қолдана алады.

Қазіргі заманғы криптография қазіргі таңда сандық ақпараттық қоғамның жаңа қажеттіліктеріне бейімделген арнайы механизмдер мен хаттамаларды белсенді түрде өңдейді. «Соқыр» электронды сандық қолтаңба, «әлсіз» сандық «мөлдір» белгілері де өңделді. Барлық бұл хаттамалар мен механизмдер өте тиімді, себебі жасырын өз криптографиялық кілттің иелігінен құрылған. Мінсіз жағдайларда, пайдаланушы шын мәнінде өз жеке кілтін жасырын сақтай алса, қорғаудың криптографиялық механизмдері расында күшті болады және тіпті хакерлер криптографиялық қорғауға шабуыл жасай алмайды. Яғни, сандық ақпараттық қоғам қауіпсіздігінің бүгінгі маңызды мәселесі ақпараттық қоғам азаматтарының жеке криптографиялық кілттерін жасырын сақтау мәселесі болып табылады.

Қазіргі таңда бұл мәселеге біздің еліміздегідей, шетелде де елеулі назар аударылып отыр. АҚШ пен Канада зерттеушілері автоматты аутентификацияның полицейлік жүйелерін қолданатын ашық биометриялық бейнелердің біршама әлсіз биометриясын құру және дамыту бойынша іс жүзінде әлемдік көшбасшылар болып табылады. Биометриялық аутентификация құралдары анық емес логиканы қолдану арқылы құрылады [1-9].

Ресей, Беларус және Қазақстан зерттеушілері биометрия-код нейрожелілік түрлендіргіштерін қолдануды ұсынады, бұған қоса биометриялық аутентификация құралдары үлкен өлшемдегі жасанды нейрондық желілерді қолдану арқылы құрылады [10-26].

Биометриялық технологиялардың екі тармағы да ақпараттық қоғамға қажет және бірін-бірі толықтырады.

Ертелі кеш бұл мәселе әлемдік қауымдастықта шешіледі және сол кезде нақты адамның биометриялық мәліметтерінің, олардың нейрожелілік немесе анық емес контейнерге орналасуынан кейін, қорғау беріктілігін бағалау мәселесі туындайды.

Ұсынылып отырған мақала, адам биометриялық мәліметтері мен оның жеке криптографиялық кілті бар нейрожелілік немесе анық емес контейнерлерді қорғау мәселелеріне арналған.

Мәселенің шешімі. Азаматтар үшін электронды үкіметпен құрылған электронды құжаттардың қуатталуы мен тұтастығы электронды үкіметтің құжаты арқылы электронды-сандық қолтаңбасын (ЭСҚ) қалыптастыру жолымен кепілденеді. Бұған қоса осы жерде азаматтың оған

жіберілген электронды құжат арқылы ЭСҚ-ны жеке тексеру мәселесі туындайды, қарапайым компьютерлерді қолданып қарапайым адам таба алмайтын бұрмалау шабуылдары мен ашық кілттерді әдейі ауыстыруға кепіл бола алмайды.

Қазіргі кездегі куәландыру орталықтары азаматтардың ашық кілттері сертификаттарын қолдау бойынша ғана қызмет көрсетеді, дегенмен азаматтар ЭСҚ-ның заңды маңыздылығын тексеру үшін өз ашық кілттерін ресми түрде тіркегісі келмейді. Мәселе мынада: азамат өз ашық кілтін тіркеумен қатар ЭСҚ-сын құруда өз жеке кілтінің компрометациясына қосымша қауіпті сөзсіз қосып алады. Адамның жеке кілтін ұрлаған кез келген біреу кез келген электронды құжат арқылы оның атынан ЭСҚ құруға қабілетті (сандық құлдыққа түсу қаупі). Қарапайым адамда өз жеке кілтін сенімді сақтау мүмкіндігі жоқ.

Жоғарыда айтылған мәселе өзекті болып табылады және оның шешілуі жеке және заңды тұлғалардың ашық кілттерінің сертификатталуы бойынша дәстүрлі қызметтер көрсетіп қана қоймай, сонымен бірге, адам тұлғасының локальды және қашықтықтан биометриялық аутентификациясы бойынша мүлдем басқа қызметтерді де атқаратын жаңа буынның куәландыру орталығын құру болып отыр. Адамның өзі биометриялық тіркелуден өту үшін, жеке өзі бір рет көрінуі жеткілікті, содан кейін адам өзінің биометриялық түпнұсқалылығын қауіпсіздік делдалы қызметін – жаңа буынның биометриялық куәландыру орталығын қолдана отырып, электронды үкіметке, электронды бизнеске, басқа азаматтарға дәлелдей алады.

Жаңа буынның биометриялық куәландыру орталықтары адамның биометриялық мәліметтері компрометациясы қауіптерін және оның жеке кілті компрометациясы қауіптерін алып тастайды. Адамның жеке биометриясы биометриялық куәландыру орталығында сенімді сақталады және адам өзінің биометриялық түпнұсқалылығын локальды (кепілдендірілетін орталықта жеке қатыса отырып) немесе қашықтықтан дәлелдей алады және куәландыру орталығынан, мысалы, оның электронды үкіметке жолдаған ЭСҚ растауды сұрай алады.

Электронды үкімет оған жүгінген әр азаматты биометриялық сәйкестендіру қажеттілігінен босайды. Ол азаматтың биометриялық аутентификациясының сенімділігіне қауіпсіз делдал – биометриялық куәландыру орталығы арқылы сенімді бола алады.

Зерттеу аумағындағы технологияның жетістігі қарапайым пайдаланушының криптография проблемаларымен соқтығыспайтындығында (өзінің жеке кілтін сақтау мәселелерімен және басқа заңды және жеке тұлғалардың ашық кілттері сертификаттарының әрекетін тексеру мәселелерімен соқтығыспайды). Бірінші бөлім проблемаларын жаңа буынның биометриялық куәландыру орталықтары шешеді. Жаңа буынның биометриялық куәландыру орталықтары беретін криптографиялық қызметтер тұтынушыдан жасырын формада беріледі, олардың дұрыстылығына куәландыру орталығы жауап береді. Пайдаланушы электронды үкіметке жүгіну кезінде немесе электронды үкіметтен оның жеке ақпараттарын алу кезінде қазіргі заманғы криптография сенімділігін алады. Адамның сандық құлдыққа түсу қаупі өзінің жеке кілтінің компрометациясы әсерінен жойылады. Өзінің биометриялық куәландыру орталығына локальды немесе қашықтықтан жүгіне отырып адам өз биометриясын өзінен басқа ешкім қолдана алмайтындығына сенімді бола алады.

Биометриялық куәландыру орталығында (БКО) барлық азаматтар қатаң есепке алынады (азаматтарға көрсетілетін БКО қызметтерінің тұрақты түрде төлемдері жүргізіледі және әр пайдаланушыға тұрақты түрде түбіртектер жіберіледі). БКО аймағында азаматтар биометриясы қорғалған нейрожелілік контейнерлерде сақталады. БКО қызметкерлерінің, өз клиенттерінің биометриясын қолдану мүмкіндігі жоқ, себебі оны қолдану кезіндегі шараға адамның өзі ғана қатыса алады (локальды немесе қашықтықтан).

Қорытынды. Қазіргі кезде, ашық ақпараттық кеңістікте азаматтардың бір-біріне жолданымында, азаматтардың электронды бизнеске немесе азаматтардың электронды үкіметке жүгінуінде қазіргі заманғы криптография көптеп қолданыла бастады. Бұған қоса пайдаланушы өз жеке кілтінің компрометациясына қауіптенбейді, олардың өз жеке кілті жоқ, олар өздері электронды үкіметке жүгінген кезде ЭСҚ қою кезінде биометриялық куәландыру орталығының жеке кілтін «жалға алады».

Жаңа буынның биометриялық куәландыру орталықтары беретін криптографиялық қызметтер тұтынушыдан жасырын формада беріледі, олардың дұрыстылығына куәландыру орталығы жауап

береді. Пайдаланушы электронды үкіметке жүгіну кезінде немесе электронды үкіметтен өзінің жеке ақпараттарын алу кезінде қазіргі заманғы криптография сенімділігін алады. Адамның сандық құлдыққа түсу қаупі өзінің жеке кілтінің компрометациясы әсерінен жойылады. Өзінің биометриялық куәландыру орталығына локальды немесе қашықтықтан жүгіне отырып адам өз биометриясын өзінен басқа ешкім қолдана алмайтындығына сенімді бола алады.

Биометриялық куәландыру орталығында (БКО) барлық азаматтар қатаң есепке алынады (азаматтарға көрсетілетін БКО қызметтерінің тұрақты түрде төлемдері жүргізіледі және әр пайдаланушыға тұрақты түрде түбіртектер жіберіледі).

ӘДЕБИЕТТЕР

[1] Dodis Y., Reyzin L., Smith A. Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy, April 13, 2004.

[2] Verbitskiy E., Tuyls P., Denteneer D., Linnartz J.-P. Reliable Biometric Authentication with Privacy Protection. In Proc. 24th Benelux Symposium on Information theory, 2003.

[3] Soutar C., Roberge D., Stoianov A., Golroy R. and Vijaya B. Kumar, "Biometric Encryption", ICSA Guide to Cryptography, McGraw-Hill, 1999, also available at http://www.bioscrypt.com/assets/Biometric Encryption.pdf

[4] Cavoukian A., Stoianov A. Biometric Encryption: A Positive-Sum Technology that Achieves Strong Authentication, Security AND Privacy, March 2007, http://www.ipc.on.ca

[5] John Daugman «Probing the Uniqueness and Randomness of Iris Codes: Results From 200 Billion Iris Pair Comparisons» Proceedings of the IEEE, Vol. 94, No. 11, November 2006, p.p. 1928-1935.

[6] Иванов А.И. Биометрическая идентификация личности по динамике подсознательных движений. – Пенза: Издательство Пензенского государственного университета, 2000. – 188 с.

[7] Иванов А.И. Нейросетевые алгоритмы биометрической идентификации личности // М.: Радиотехника. серии «Нейрокомпьютеры и их применение». 2004. Книга 15. – 144 с.

[8] Волчихин В.И., Иванов А.И., Фунтиков В.А. Быстрые алгоритмы обучения нейросетевых механизмов биометрико-криптографической защиты информации: Монография. – Пенза: Издательство ПГУ, 2005. – 273 с.

[9] Малыгин А.Ю., Волчихин В.И., Иванов А.И., Фунтиков В.А. Быстрые алгоритмы тестирования нейросетевых механизмов биометрико-криптографической защиты информации. – Пенза: Издательство ПГУ, 2006. – 161 с.

[10] Иванов А.И., Кисляев С.Е., Гелашвили П.А. Искусственные нейронные сети в биометрии, медицине, здравоохранении. – Самара: ООО «Офорт», 2004. – 236 с.

[11] Иванов А.И., Волчихин В.И. Информационный показатель КПД нейросетевых преобразователей биометрия-код // «Нейрокомпьютеры: разработка, применение», 2007. – № 12. – С. 18-19.

[12] Захаров О.С., Иванов А.И., Хозин Ю.В. Применение средств многомерной нейросетевой биометрии – путь к безопасному обмену в открытом информационном пространстве // «Нейрокомпьютеры: разработка, применение», 2007. – № 12. – С. 20-21.

[13] Иванов А.И. Оценка остаточных корреляционных связей при тестировании нейросетевых преобразователей биометрия-код // «Нейрокомпьютеры: разработка, применение», 2007. – № 12. – С. 25-26.

[14] Малыгин А.Ю., Волчихин В.И., Федулаев В.В., Безяев А.В. Оценка размеров технически реализуемых баз биометрических образов, необходимых для корректного тестирования высоконадежных нейросетевых преобразователей // «Нейрокомпьютеры: разработка, применение», 2007. – № 12. – С. 52-54.

[15] Малыгин А.Ю., Федулаев В.В., Надеев Д.Н. Требования к синтетическим базам биометрических образов и генераторам для их формирования // «Нейрокомпьютеры: разработка, применение», 2007. – № 12. – С. 60-64.

[16] Малыгин А.Ю. Системный подход к тестированию средств высоконадежной биометрии // Вестник Костромского государственного университета им. Н.А.Некрасова, 2007. – № 1. – С. 35-38.

[17] Малыгин А.Ю. Быстрые алгоритмы тестирования высоконадежной биометрической защиты // «Вопросы защиты информации», 2007. – № 4 (79) – С. 8-12.

[18] Захаров О.С., Иванов А.И. Учет корреляционных связей биометрических данных через дробный показатель степеней свободы закона распределения значений хи-квадрат // Инфокоммуникационные технологии, 2008. – № 1, – Т. 6. – С. 12-15.

[19] Ахметов Б.С., Иванов А.И., Картбаев Т.С., Малыгин А.Ю. Оценка вероятностей появления ошибок нейросетевых преобразователей биометрия-код на основе малых выборок // Труды II-Международной научной конференции «Высокие технологии-залог устойчивого развития». – Алматы: КазНТУ имени К.И.Сатпаева, 2013. Том I. – С. 234-237.

[20] Akhmetov B.S., Ivanov A.I., Kartbayev T.S., Malygin A.Yu., Mukapil K. Biometric Dynamic Personality Authentication in Open Information Space // International Journal of Computer Technology and Applications. India, 2013. – Vol.4., Issue 5. – P. 846-855. Available online at: http://ijcta.com/documents/volumes/vol4issue5/ijcta2013040520.pdf

[21] Ахметов Б.С., Волчихин В.И., Иванов А.С. Преимущества биометрико-нейросетевого хранения конфиденциальной информации мобильного пользователя // Вестник КазНТУ им. К.И.Сатпаева. – Алматы, 2011. – № 3 (85). – С. 173-178.

[22] Ахметов Б.С., Иванов А.С., Бияшев Р.Г. Предельно допустимые значения коррелированности разрядов биометрических кодов // Вестник КазНТУ им. К.И.Сатпаева. – Алматы, 2011. – № 4 (86). – С. 181-184.

[23] Ахметов Б.С., Иванов А.С., Трифонов С.Е. Биометрические удостоверяющие центры шаговой доступности // Новости науки Казахстана, 2011. – № 3-4. – С. 34-41.

[24] Ахметов Б.С., Иванов А.С., Фунтиков В.А. Статистическое описание выходных состояний нейросетевых преобразователей биометрия-код // Вестник КазНТУ им. К.И.Сатпаева. – Алматы, 2011. – № 6 (88). – С. 36-40.

[25] Ахметов Б.С., Волчихин В.И., Куликов В.С., Малыгина Е.А. Моделирование длинных биометрических кодов, воспроизводящих корреляционные связи выходных данных нейросетевого преобразователя // Журнал «Нейрокомпьютеры: разработка, применение». – Пенза, 2012. – № 3. – С. 40-43.

[26] Ахметов Б.С., Картбаев Т.С., Малыгин А.Ю., Захаров О.С., Иванов А.И., Огнев И.В. Метод оценки вероятностей появления ошибок нейросетевых преобразователей биометрия-код, использующий очень малые тестовые выборки // Вестник КазНТУ им. К.И.Сатпаева. – Алматы, 2013. – № 3 (97). – С. 279-283.

REFERENCES

[1] Dodis Y., Reyzin L., Smith A. Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy, April 13, 2004.

[2] Verbitskiy E., Tuyls P., Denteneer D., Linnartz J.-P. Reliable Biometric Authentication with Privacy Protection. In Proc. 24th Benelux Symposium on Information theory, 2003.

[3] Soutar C., Roberge D., Stoianov A., Golroy R. and Vijaya B. Kumar, "Biometric Encryption", ICSA Guide to Cryptography, McGraw-Hill, 1999, also available at http://www.bioscrypt.com/assets/Biometric Encryption.pdf

[4] Cavoukian A., Stoianov A. Biometric Encryption: A Positive-Sum Technology that Achieves Strong Authentication, Security AND Privacy, March 2007, http://www.ipc.on.ca

[5] John Daugman "ProbingtheUniquenessandRandomnessof Iris Codes: Results From 200 Billion Iris Pair Comparisons" Proceedings of the IEEE, Vol. 94, No. 11, November 2006, p.p. 1928-1935.

[6] Ivanov A.I. Biometricheskaya identification of the personality on dynamics of the subconscious movements. Penza: Publishing house of the Penza state university, 2000. 188 p.

[7] Ivanov A.I. Neural network algorithms of biometric identification of the personality, M.: Radio engineering. series "Neyrokompyyutera and their application". 2004. Book 15. 144 p.

[8] Volchikhin V.I., Ivanov A.I., Funtikov V.A. Fast algorithms of training of neural network mechanisms of biometriko-cryptographic information security: Monograph. Penza: PGU publishing house, 2005. 273 p.

[9] Malygin A.Yu., Volchikhin V.I., Ivanov A.I., Funtikov V.A. Fast algorithms of testing of neural network mechanisms of biometriko-cryptographic information security. Penza: PGU publishing house, 2006. 161 p.

[10] Ivanov A.I., Kislyaev S.E., Gelashvili P.A. Artificial neural networks in biometrics, medicine, health care. Samara: JSC Ofort, 2004. 236 p.

[11] Ivanov A.I., Volchikhin V.I. Information indicator of efficiency of neural network converters biometrics code. "Neyrokompyyutera: development, application", 2007. No. 12. P. 18-19.

[12] Zakharov O.S., Ivanov A.I., Hozin Yu.V. Application of means of multidimensional neural network biometrics – a way to a safe exchange in open information space. "Neyrokompyyutera: development, application", 2007. No. 12. P. 20-21.

[13] Ivanov A.I. Otsenk of residual correlation communications when testing neural network converters biometrics code. "Neyrokompyyutera: development, application", 2007. No. 12. P. 25-26.

[14] Malygin A.Yu., Volchikhin V.I., Fedulayev V.V., Bezyaev A.V. Otsenk of the extent of technically realized bases of the biometric images necessary for correct testing of highly reliable neural network converters. "Neyrokompyyutera: development, application", 2007. No. 12. P. 52-54.

[15] Malygin A.Yu., Fedulayev V.V., Nadeev D.N. Requirements to synthetic bases of biometric images and generators for their formation. "Neyrokompyyutera: development, application", 2007. No. 12. P. 60-64.

[16] Malygin A.Yu. System approach to testing of means of highly reliable biometrics. The Bulletin of the Kostroma state university of N.A.Nekrasov, 2007. No. 1. P. 35-38.

[17] Malygin A.Yu. Fast algorithms of testing of highly reliable biometric protection. "Questions of information security", 2007. No. 4(79). P. 8-12.

[18] Zakharov O.S., Ivanov A.I. The accounting of correlation communications of biometric data through a fractional exponent of degrees of freedom of the law of distribution of values a chi-square. Infocommunication technologies, 2008. No. 1, Vol. 6. P. 12-15.

[19] Akhmetov B.S., Ivanov A.I., Kartbayev T.S., Malygin A.Yu. Otsenka of probabilities of emergence of errors of neural network converters biometrics code on the basis of small selections. Works of the II International scientific conference "High Technologies Pledges of a Sustainable Development", Almaty, KazNTU named after K.I.Satpayev, 2013. Vol. 1. P. 234-237.

[20] Akhmetov B.S., Ivanov A.I., Kartbayev T.S., Malygin A.Yu., Mukapil K. Biometric Dynamic Personality Authentication in Open Information Space//International Journal of Computer Technology and Applications. India, 2013. Vol.4., Issue 5. P. 846-855. Available online at: http://ijcta.com/documents/volumes/vol4issue5/ijcta2013040520.pdf

[21] Akhmetov B.S., Volchikhin V.I., Ivanov A.S. Advantages of biometriko-neural network storage of confidential information of the mobile user. Herald of the KazNTU named after K.I.Satpayeva, Almaty, 2011. No. 3(85). P. 173-178.

[22] Akhmetov B.S., Ivanov A.S., Biyashev R.G. Maximum permissible values of correlation of categories of biometric codes. Herald of the KazNTU named after K.I.Satpayeva, Almaty, 2011. No. 4 (86). P. 181-184.

[23] Akhmetov B.S., Ivanov A.S., Trifonov S.E. The biometric certifying centers of step availability. News of science of Kazakhstan, 2011. No. 3-4. P. 34-41.

[24] Akhmetov B.S., Ivanov A.S., Funtikov V.A. The statistical description of output conditions of neural network converters biometrics code. Herald of the KazNTU named after K.I.Satpayeva, Almaty, 2011. No. 6(88). P. 36-40.

[25] Akhmetov B.S., Volchikhin V.I., Sandpipers V.S., Malygina E.A. Modeling of the long biometric codes reproducing correlation communications of the output data of the neural network converter. Journal "Neyrokompyyutera: development, application", Penza, 2012. No. 3. P 40-43.

[26] Akhmetov B.S., Kartbayev T.S., Malygin A.Yu., Zakharov O.S., Ivanov A.I., Ognev I.V. Metod of an assessment of probabilities of emergence of errors of neural network converters biometrics code using very small test selections. Herald of the KazNTU named after K.I.Satpayeva, Almaty, 2013. No. 3(97). P. 279-283.

Исследование и разработка удостоверяющих центров аутентификации личности с использованием биометрико-нейросетевых технологий

Картбаев Т.С., Бекетова Г.С., Мукапил К.
kaiyrkhan@mail.ru
Казахский национальный технический университет имени К.И. Сатпаева, Алматы, Республика Казахстан

Ключевые слова: электронное правительство, защита информации, аутентификация личности, биометрико-нейросетевая технология, разработка удостоверяющих центров, электронно-цифровая подпись.

Аннотация. Исследование и разработка удостоверяющих центров аутентификации личности в системе электронного правительства с использованием биометрико-нейросетевых технологий является перспективным направлением развития информационно-телекоммуникационных технологий как в Республике Казахстан, так и во всем мире.

Существующие удостоверяющие центры предоставляют услуги только по поддержке сертификатов открытых ключей граждан, однако граждане не хотят официально регистрировать свой открытый ключ для проверки юридически значимой ЭЦП. Проблема состоит в том, что параллельно с регистрацией своего открытого ключа гражданин неминуемо получает дополнительный риск компрометации своего личного ключа формирования ЭЦП. Вышеизложенная проблема является актуальной и должна быть решена в рамках предлагаемого проекта. Решение ее состоит в создании удостоверяющих центров, которые не только предоставляют традиционные услуги по сертификации открытых ключей физических и юридических лиц, но и выполняют совершенно иные услуги по локальной и дистанционной биометрической аутентификации личности человека.

Целевыми потребителями полученных результатов являются государственные и коммерческие организации, осуществляющие обработку персональных данных в рамках электронного документооборота без угрозы компрометации персональных и биометрических данных граждан.

Сведения об авторах

Картбаев Тимур Саатдинович, доктор PhD, и.о. доцент, Казахский национальный технический университет имени К.И. Сатпаева, Email: kartbaev_t@mail.ru

Бекетова Гульжанат, PhD докторант специальности 6D070400 – ВТиПО, Казахский национальный технический университет имени К.И. Сатпаева, Email: beketova_gs@mail.ru

Мукапил Кайырхан, PhD докторант специальности 6D070400 – ВТиПО, Казахский национальный технический университет имени К.И. Сатпаева, Email: kaiyrkhan@mail.ru, Моб. тел.: +7 778 499 93 00

Поступила 17.03.2015 г.