BULLETIN OF NATIONAL ACADEMY OF SCIENCES
OF THE REPUBLIC OF KAZAKHSTAN
ISSN 1991-3494
Volume 3, Number 355 (2015), 77 – 80

THREATS FOR SYSTEMS OF BIOMETRICS-NEURAL NETWORKS AUTHENTICATION

K. Mukapil, G. Beketova, N. Zhumangalieva, V. Tulemisova

Kazakh National Technical University named after K. I. Satpayev, Almaty, Kazakhstan.
E-mail: kaiyrkhan@mail.ru

Key words: biometrics-neural, network, authentication, threats, information security, artificial neural networks, multi-biometric systems.

Abstract. In this article a list of threats to the system, neural network biometrics authentication, as well as measures to reduce negative impacts are provided. Due to the fact that at the moment there are no the systems of biometric authentication which are completely meeting requirements of safety concept of multibiometric system, which combines different biometric systems, is considered.And also the main advantages of multibiometric system of authentication are considered.

ӘОЖ (УДК) 004

БИОМЕТРИЯЛЫ-НЕЙРОЖЕЛІЛІК АУТЕНТИФИКАЦИЯ ЖҮЙЕЛЕРІНЕ ТӨНЕТІН ҚАУІПТЕР

К. Мукапил, Г. Бекетова, Н. Жұманғалиева, В. Төлемісова

Қ. И. Сәтбаев атындағы Қазақ ұлттық техникалық университеті, Алматы, Қазақстан

Тірек сөздер: биометриялы-нейрожелілік аутентификация, қауіптер, ақпаратты қорғау, жасандынейрондық желі, мультибиометриялық жүйелер.

Аннотация. Мақалада биометрия-нейрожелілік аутентификация жүйелеріне төнетін қауіптер тізбесі және де кері әсерлерді төмендету шаралары көрсетілген. Қауіпсіздікті қамтамасыз етуді толығымен қанағаттандыратын биометриялық аутентификация жүйесінің болмауына байланысты түрлі биометриялық жүйелерді бірлестіретін мультибиометриялық жүйе ұғымы қарастырылған. Бірнеше биометриялық жүйелердің қосылуы кезінде олардың бірлесу механизмі жасалатындығы келтірілген. Сонымен бірге аутентификацияның мультибиометриялық жүйелерінің негізгі жетістіктері сөз етілді.

Биометриялы-нейрожелілік аутентификация жүйелеріне төнетін қауіптер қатары бар [1-3]. Оларға мыналар жатқызылады:

– *физикалық деңгейде адамның жасырын биометриялық бейнесінің компрометациясы.* Жасырын биометриялық бейне компрометациясының қаупі ең маңыздысы болып табылады. Биометриялық аутентификация жүргізу есебінен тек бақыланатын аймақта; қолтаңбалық құпия сөзді жаңғырту кезінде қалталы компьютер экранының өшуі есебінен; қарапайым құпия сөздерді ауыстыру ұқсастығы бойынша пайдаланушының жасырын биометриялық бейнесінің (биометриялық құпия сөздің) периодтық ауысуы есебінен төмендеуі мүмкін;

– *адамның биометриялық мәліметтері түрінде адамның жасырын электронды бейнесін ұстап қалу.* Биометриялық ақпаратты өңдеудің бағдарламалық қамсыздандыруын ауыстыру немесе түрлендіру адамның жасырын электронды биометриялық бейнесін алуға мүмкіндік береді. Егер бағдарламалық қамсыздандыру тұтастығын бақылау және биометриялық аутентификациясымен параллель жүретін есептеуіш процестер функцияларын бақылау жүйесімен қамтамасыз етілмесе адам ауыстыруды сезбейді. Бағдарламалық қамсыздандыруды ауыстырудың немесе оның түрлендіруінің сәйкес шабуылы арқылы бұл қауіптің берілуі – ең қарапайымдыларының, сонымен бірге тиімді жолдарының бірі. Бұл қауіп қолданатын бағдарламалық қамсыздандырудың тұтастығын бақылау және биометриялық-нейрожелілік аутентификация процедурасынан әрекетін бақылау жолымен төмендейді. Барлық амалдардың мамандандырылған есептеуіш ортада жеке немесе толық ауысуы мүмкін.

Егер биометриялық бағдарламалық қамсыздандыруда тұтастық чегі болса және іске қосу алдында оларға тексеру жүргізілсе, онда ауыстыру мүмкіндігі орындалмайды. Осыған қоса тұтастық чекін сенімді сақтауды қамтамасыз ету қажет, себебі оларды бағдарламалық қамсыздандыруымен бірге ауыстыруы мүмкін. Сондықтан тұтастық чегін бағдарламалық қамсыздандырудан бөлек сақтау қажет.

Ұстап қалу фактін табу кезінде немесе пайдаланушының электронды биометриялық бейнесін ұстап қалуға апаратын жоғары ықтималдықты шартты анықтау кезінде биометриялық бейнені өзгерту және кейін оны қарапайым құпия сөзді қолдану кезіндегідей қайта-қайта ауыстыру ұсынылады;

– *жасырын биометриялық бейнені физикалық деңгейде кездейсоқ іріктеу.* Бұл жаңа қауіп, және адамнан оның жазбалық қолтаңбасының үлгілерін ұрлау жолымен берілуі мүмкін. Әрине, бұл үшін биометриялық ақпараттардың (заңды пайдаланушымен кескіндік планшетте жаңғыртылған қолтаңбалық мәтіннің бірнеше парақтары) айтарлықтай көлемі жинақталуы қажет. Нақты адам имитаторын құру мүмкіндігі пайда болады, мысалы, олардың түрлі қиыстырылуындағы дәлме-дәл биометрия фрагменттерін қою. Биометриялық құпия сөзді тіпті білмей, бірақ бұл құпия сөз пайдаланушының тіліндегі қысқа сөз екендігін біле отырып, биометриялық құпия сөз нұсқаларын, олардың түрленуін есепке ала отырып, іріктеуге болады.

Қауіпті аутентификация әрекетін пайдаланушыға беретін санын шектеу есебінен және қолтаңбалық құпия сөз сапасын жоғарылату есебінен төмендетуге болады (қолжазбалық құпия сөздегі сөз санын және сөздегі әріптер санын жоғарылату, кері қолтаңбаны енгізу, қолжазбалық құпия сөзді тұрақты жазу бойынша дағдылану).

Жасырын биометриялық бейнені физикалық деңгейде кездейсоқ іріктеу ықтималдығын төмендету кепілі биометриялық құпия сөз сапасын бақылау жүйесін қорғаудың биометриялық өнімде берілуі болып табылады. Мұндай жүйе өте әлсіз құпия сөздерді қолдануды шығарып тастайды. Күшті биометриялық құпия сөздерді іріктеу пайдаланушының жазбалық қолтаңбасын енгізудегі биометриялық мәліметтерінің қосылуының автоматты түрде синтезделу қиындығы есебінен өте күрделі болады;

– *электронды жасырын биометриялық бейненің (бейненің биометриялық параметр векторы) кездейсоқ іріктелуі.* Кездейсоқ шығыс мәліметтерді синтездеу үшін олардың мүмкін динамикалық диапазондарын берсе және осы диапазонда кездейсоқ тәуелсіз мәліметтерді олардың жасанды нейрондық желілер шығысына берілуімен синтезделуі жеткілікті. Сондықтан жасанды нейрондық желілерді оқыту сапасының ішкі бақылауы биометриялы-нейрожелілік аутентификация жүйелерінде міндетті элемент болып табылады [3-5].

Тағы бір маңызды сәт биометриялық бейне құпиясының жеке-жеке бұзылуы болып табылады, мұнда биометриялық электронды бейненің қалған бөліктерін кездейсоқ іріктеуінің шабуылы тиімді болуы мүмкін.

Электронды жасырын биометриялық бейненің кездейсоқ іріктелуінің қауіпжасанды нейрондық желінің кірісі мен шығысы сандарын көбейту, нейрондар қабаты санын көбейту және әр нейрондағы байланыстар санын көбейту жолымен азаюы мүмкін.

Одан басқа, жасанды нейрондық желінің өзі қастық ойлаушыларға қолжетімсіз болуы мүмкін, мысалы, қорғалатын аймақтағы биометрикалық-нейрожелілік аутентификация жүйесін шығаруға тыйым салынуы мүмкін;

– *жасанды нейронды желі параметрлері мен құрылымынан құпия ақпаратты шығару.* Қазіргі уақытта әлі жасанды нейронды желі параметрлері мен құрылымынан құпия ақпаратты шығаратын және оған талдау жүргізетін жүйе құрылмады. Олар шығарылған кезде желі қабаттары санын, нейрондар кірістерінің санын көбейту есебінен кері түрлендіру күрделілігін көбейту қажет болады. Осы кезде нейрондар қабаттары саны да, кірістер саны да кері түрлендіру есептеуіш күрделілігінің өсуіне әсер етеді;

– *жасанды нейронды желіні оқыту кезінде пайдаланушылардың кері ниеттілігі мен іріткі салу қаупі.* Тәжірибе көрсеткендей, пайдаланушылар өздерінің әрекеттеріне жауапкершілікті күшейтуге теріс қарауы мүмкін. Пайдаланушы жүйені оқу кезінде әдейі тиянақсыз жазуға, ал содан кейін оған кіру кезінде қолжазбалық құпия сөзді бейберекет енгізуге тырысады. Бұл жаңа қатер. Егер жүйеге автоматтандырылған тестілеу және күтілетін сенімділікті болжау құралдары болса, бұл қатер нашарлайды;

– *келісім* – бұл дәстүрлі қауіп (жаман пиғылды пайдаланушы өз құпиясөзін әдейі басқа адамға беруі мүмкін). Бұл қатер биометрияны енгізуде бәсеңдейді. Басқа бір адамға заңды пайдаланушының қолтаңбасын тиімді енгізуді үйрету қиын. Қауіптің әр бөлігі, өз жасанды нейронды желісі мен өз пайдаланушысымен байланысқан ұзақ құрамдас кілт бойынша аутентификация кезінде төмендеуі мүмкін. Пайдаланушылар мен қауіпсіздік администраторы бір-бірін бақылай отырып, тек бірлескен күшпен жалпы кілт құра алады;

– *биометриялы-нейрожелілік аутентификация жүйесінің қауіпсіздік администраторының қате қылығы.* Биометриялық аутентификация жүйелерінде бұл қатер төмендейді, егер жүйе тек қана пайдаланушының биометриялық бейнелеріне бапталған болса. Онда администраторды биометриялық бейнелер мен ұзақ құпия сөзді құпияда ұстауға бағыттау қажеттілігі жоқ (пайдаланушының ұзақ құпия сөзін сақтау арнайы сейфте мөрленген конвертте жүзеге асырылады);

– *биометриялы-нейрожелілік аутентификацияның тұрақтылық деңгейін сәйкессіз бағалау.* Биометриялы-нейрожелілік аутентификациямен түрлендірілген пайдаланушының биометриялық бейнесі классикалық құпиясөздік қорғауынан тиімдірек болады, бірақ одан жағдайлардың сәтсіз тоғысуы кезінде әлсіздеу болады;

– *ауру, зақым, дәрілерді қабылдау, стресс, мастықтың әсерінен заңды пайдаланушының биометриялық бейнесінің жоғалуы және елеулі бұрмалануы.* Бұл адамның сресстік жағдай кезінде жазбалық қолтаңбасы параметрлерінің тез өзгеруіне байланысты жаңа қатер түрі. Бұған қоса, қолдың аурулары мен зақымдары да болады. Мастық, наркотикалық әсері бар кейбір дәрілерді қабылдау қорғаудың биометриялық технологиялары арқылы ақпаратқа ену мүмкіндігін жоғалтуға әкеп соқтырады.

Бұл қауіп кілттің немесе ұзақ құпия сөздің болуы арқылы аутентификацияның классикалық процедураларымен биометриялық аутентификацияны қайталау есебінен әлсіздеуі немесе төмендеуі мүмкін. Бұл кезде кілт немесе құпия сөз сейфте сақталады, ал ол арқылы ену штатсыз болады. Алынған кілт пен шынайы нақты кілттің сәйкестігін шығыстық тексеруде аутентификацияның штаттық жүйесін енгізу ұсынылады.

Қазіргі таңда қауіпсіздікті қамтамасыз етуді толығымен қанағаттандыратын биометриялық аутентификация жүйесінің болмауына байланысты өңдеушілер бір мультибиометриялық жүйеге түрлі биометриялық жүйелерді бірлестіруге тырысады [6]. Мысалға, жүйеге дауысты талдау мен пайдаланушының жазбалық қолтаңбасы бірігуі мүмкін. Әрине, бірнеше биометриялық жүйелердің қосылуы кезінде олардың бірлесу механизмі жасалуы керек.

Егер әртүрлі биометриялық жүйелердің бірлесу механизмін қолданатын болса, аутентификация жүйесін қорғаудың неғұрлым күшті нұсқасы алынады. Бұл үшін әр фрагменті өз биометриялық жүйесін қалыптастыратын құрамдас кілт қолданылады. Мұндай жағдайда енуге жалпы кілтті аутентификацияның барлық биометриялық жүйесін дәйекті ете отырып алады. Жалпы кілттің әр фрагментінің ұзындығы қалыптасатын оның жүйесінің пропорционалды беріктігі болуы қажет. Кездейсоқ іріктеу шабуылына тұрақтылығы төмен жүйелерінде жалпы кілттің қысқартылған фрагменті болады. Керісінше, неғұрлым берік жүйелерде соғұрлым ұзақ фрагменттері болуы қажет [4].

Аутентификацияның мультибиометриялық жүйелерінің негізгі жетістігі бір биометриялық жүйелердің кемшіліктерін басқаларының артықшылықтары есебінен компенсациялау мүмкіндіктерімен жасалады.

ӘДЕБИЕТ

[1] Иванов А.И. Биометрическая идентификация личности по динамике подсознательных движений. – Пенза: Изд-во ПГУ, 2000. – 156 с.

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

[3] ГОСТ Р 15.011-96. Система разработки и постановки продукции на производство. Патентные исследования. Содержание и порядок проведения.

[4] МалыгинА.Ю., ВолчихинВ.И., ИвановА.И., ФунтиковВ.А. Быстрые алгоритмы тестирования высоконадежных нейросетевых механизмов биометрической защиты информации. – Пенза: Изд-во ПГУ, 2006. – 161 с.

[5] ВолчихинВ.И., ИвановА.И., Безяев А.В. и др. Нейросетевые преобразователи биометрических образов человека в код его личного криптографического ключа / Под ред. А.Ю. Мальгина.Сер. «Нейрокомпьютеры и их применение».– М.: Радиотехника, 2008. – Книга 29. – 88 с.

[6] Руд Б. Руководство по биометрии. – М.: Техносфера, 2007. – 368 с.

REFERENCES

[1] Ivanov A.I. *Biometricheskaya identification of the personality on dynamics of subconscious movements.* Penza: Publishing house of PGU, 2000. 156 p.(in Russ.).

[2] Volchikhin V.I., Ivanov A.I., Funtikov V.A. *Fast algorithms of training of neural network mechanisms of biometriko-cryptography information security*. Penza: Publishing house of PGU, 2005. 273 p.(in Russ.).

[3] GOST P 15.011-96. *System of development and setting of production on production*. Patent researches. Contents and order of carrying out (in Russ.).

[4] Malygin A.Yu., Volchikhin V.I., Ivanov A.I., Funtikov V.A. *Fast algorithms of testing of high-reliable neural network mechanisms of biometric information security*. Penza: Publishing house of PGU, 2006. 161 p.(in Russ.).

[5] Volchikhin V.I., Ivanov A.I., Bezyaev A.V., etc. *Neural network transformers of biometric images of the person in a code of its personal cryptographic key.*Under the editorship of A.Yu. Malygin. It is gray. "Neurocomputers and their application". M.: Radio engineering, 2008. Book 29. 88 p.(in Russ.).

[6] Rud M. Ball. *A manual on biometry*. M.: Technosphere, 2007. 368 p.(in Russ.).

УГРОЗЫ ДЛЯ СИСТЕМ БИОМЕТРИКО-НЕЙРОСЕТЕВОЙ АУТЕНТИФИКАЦИИ

К. Мукапил, Г. Бекетова, Н. Жумангалиева, В. Тулемисова

Казахский национальный технический университет им. К. И. Сатпаева, Алматы, Казахстан

Ключевые слова: биометрико-нейросетевая аутентификация, угрозы, защита информации, искусственная нейронная сеть, мультибиометрические системы.

Аннотация. В статье приведен перечень угроз для систем биометрико-нейросетевой аутентификации, а также меры снижения отрицательного воздействия. В связи с тем, что на данный момент не существует систем биометрической аутентификации, полностью удовлетворяющих требованиям обеспечения безопасности, рассмотрено понятие мультибиометрической системы, который совмещает разные биометрические системы. А также рассмотрены основные достоинства мультибиометрической системы аутентификации.

Поступила 22.05.2015 г.