

make prognoses particular level of skills formation, and to take note in too individual tasks preparing and presentation process. Importance of this circumstance shows that, almost everybody respondents (officers of public police patrol service. in Kaunas MPK) used MAS on duty (98 %). In the questionnaire were mentioned the circumstances when were used on duty MAS, exp. The persons detention, which are suspected to commit a crime act, the persons detention, which doing active resistance to the officers vested requisition, detention the citizens which are aggressiveness and drunk or others aggressiveness the administrative law violators.

**BIOMETRINIŲ AUTENTIFIKAVIMO SISTEMŲ NAGRINĖJIMO
INFORMATIKOS STUDIJOSE ASPEKTAI**

Viktoras Stupak***Raimondas Vasiliauskas****

Mykolo Romerio universiteto Kauno policijos fakulteto Policijos veiklos katedra

V. Putvinskio g. 70, LT- 44211, Kaunas

Telefonas 8 (37) 30 36 45

Elektroninis paštas v.stupak@mruni.lt; r.vasiliauskas@mruni.lt

SANTRAUKA

Mykolo Romerio universitete Viešojo saugumo fakultete informatikos profilio dalykai dėstomi I, II ir III kursuose. Teisės ir valstybės sienos apsaugos bakalauro studijų programoje šie dalykai dėstomi I ir III kursuose, teisės ir policijos veiklos bakalauro studijų programoje – I kurse, policijos veiklos neuniversitetinių studijų programoje – I ir II kursuose. Dalykų programose, nagrinėjant priemones, užtikrinančias informacinių technologijų ir kitų objektų saugą, numatyti biometrinių autentifikavimo sistemų analizės klausimai.

Aptariami biometrinių autentifikavimo sistemų nagrinėjimo informatikos studijose ypatumai. Pateikiamas biometrinių sistemų klasifikavimas. Nagrinėjamos dvi grupės automatizuotų biometrinių sistemų. Pirmajai grupei priskiriamos sistemos, naudojančios unikalias fiziologines žmogaus kūno savybes, antrajai grupei – individualaus elgesio savybes ir charakteristikas. Analizuojama šių sistemų struktūra, sprendžiami uždaviniai ir panaudojimo sritis.

Pagrindinės sąvokos: atpažinimas, autentifikavimas, biometrinės sistemos, identifikavimas, verifikavimas.

IVADAS

Šiuolaikinė technika ir technologijos sparčiai keičia pasaulio žmonijos gyvenimą. XX a. 9 – jo dešimtmečio pradžioje, dėl sparčios informacinių technologijų plėtros, pasikeitė daugelio pasaulio šalių ekonomikos vystymosi charakteris. Inovaciniai procesai tampa pagrindiniu reprodukcijos faktoriumi, o taip pat sąlygoja imlių ištekliams pramonės kryptį pakeitimą kryptimis imliomis mokslui ir orientuotomis į naujausias informacines ir kitas technologijas, ryšio priemones ir t.t. Vis dažniau kompiuteris tampa įprastine darbo priemone įvairiose žmogaus veiklos srityse.

* Mykolo Romerio universiteto Kauno policijos fakulteto Policijos veiklos katedros docentas

** Mykolo Romerio universiteto Kauno policijos fakulteto Policijos veiklos katedros docentas

Tai lemia ne tik kardinalius technologinius pokyčius bet ir dideles socialines-ekonomines permainas, tame tarpe ir visuomenės saugumo. Visuomenės saugumui dideles grėsmes kelia tarptautinis nusikaltimų pobūdis. Tai vis labiau didėjantys nelegalios migracijos mastai, terorizmas, ir organizuotas nusikalstamumas, kurie dažnai yra susiję su naujausių informacinių technologijų panaudojimu, informacijos apdorojimo, apsaugos, perdavimo priemonėmis ir sistemomis.

Viena iš svarbių veiklos kryptių informacijos apsaugos ir nusikalstamos veikos tyrimo srityse yra technologijų ir sistemų, kurios atlieka automatizuotą asmens tapatybės nustatymą ir nusikaltėlių paiešką, sukūrimas.

Mykolo Romerio universiteto Viešojo saugumo fakultete rengiant būsimus policijos ir valstybės sienos apsaugos pareigūnus informatikos profilio disciplinos numatytos I, II ir III kursuose. Šių dalykų programose, nagrinėjant priemones, užtikrinančias informacinių technologijų ir kitų objektų saugą, numatyti biometrinių autentifikavimo sistemų analizės klausimai.

Straipsnyje aptariami biometrinių autentifikavimo sistemų nagrinėjimo informatikos studijose ypatumai. Pateikiamas biometrinių sistemų klasifikavimas. Nagrinėjamos dvi grupės automatizuotų biometrinių sistemų, analizuojamos šių sistemų struktūra, sprendžiami uždaviniai ir panaudojimo sritis.

1. BIOMETRINIŲ AUTENTIFIKAVIMO SISTEMŲ NAGRINĖJIMO INFORMATIKOS STUDIJOSE YPATUMAI

Informacinių technologijų, priemonių ir sistemų (toliau – sistemų) vystymasis kelia aukštus reikalavimus ir jų saugai. Tai svarbu kalbant apie informaciją, turinčią slaptumo laipsnį arba nuo kurios gali priklausyti žmonių gerovė ar netgi gyvybė.

Biometrinių autentifikavimo sistemų nagrinėjimą informatikos studijose studentai pradeda nuo susipažinimo su sistemų bei informacijos sauga ir autentifikavimo (identifikavimo) procedūromis, jie įgyja teorinių informacijos apsaugos žinių [1]. Toliau studentai įtvirtina apsaugos metodų taikymo kompiuterizuotose policijos ir valstybės sienos apsaugos tarnybos (VSAT) darbo vietose mokėjimus ir įgūdžius.

Užsiėmimuose pabrėžiama [1], kad sistemų saugumą, gali užtikrinti tik kompleksas technologinių ir administracinių priemonių [2, 3], akcentuojama kreipties valdymo metodo svarba. Nagrinėjamos ir paskirstytosios sistemos, kurių sudėtyje yra telekomunikaciniai ir kompiuterių tinklai. Analizuojant sistemos komponentų atpažinimo procedūras, pabrėžiama, kad jos atliekamos atsižvelgiant į nustatytus apribojimus (prieinamumo teisės, įgaliojimai), darbo reglamentą.

Toliau nagrinėjamas sistemos vartotojų, aptarnaujančio personalo ir aplamai asmenų atpažinimo (tapatybės nustatymo) klausimas. Akcentuojama, kad dabartiniu metu naudojami kaip įprasti, taip ir nauji metodai [1]. Atpažinimo (tapatybės nustatymo) metodai gali būti, atsižvelgiant į [4], sąlygiškai skirstomi į šias grupes:

- numatantys specialiųjų įrenginių ar daiktų panaudojimą (raktų, kortelių, paso ir kt.);
- panaudojantys specialias žinias (slaptažodis ar slaptažodžiai, kita konfidenciali informacija ir pan.);
- reikalaujantys biometrinių charakteristikų panaudojimo;
- metodai, kuriuose visa atpažinimo procedūra susideda iš kelių etapų (kelių metodų panaudojimo) – pvz. slaptažodžio surinkimas, specialios kortelės panaudojimas ir asmens biometrinių duomenų fiksavimas (gali būti pateiktas piršto atspaudas ar kt.).

Analizuojant šiuos metodus akcentuojama [1], kad dabartiniu metu plačiai naudojamos kortelės – plastikinės, magnetinės, optinės atminties kortelės, kortelės su mikroschemomis, kortelės su mikroprocesoriais, kortelės su dirbtinio intelekto galimybėmis. Pabrėžiama, kad kortelėse gali būti įrašoma įvairi skaitmeninė informacija, tame tarpe ir biometriniai asmens duomenys.

Toliau nagrinėjant biometrines autentifikavimo sistemas atliekamas šių sistemų klasifikavimas, analizuojama jų struktūra, panaudojimo sritys, sistemų techniniai ir kiti parametrai, sistemų naudojimo efektyvumas.

2. BIOMETRINIŲ AUTENTIFIKAVIMO SISTEMŲ KLASIFIKAVIMAS, SPRENDŽIAMŲ UŽDAVINIAI

Atsižvelgiant į reikalavimus, keliamus informacijos apsaugos sistemoms, nusikaltimų prevencijai ir išaiškinamumui, asmens tapatybės nustatymui dabartiniu metu plačiai naudojamos ir unikalios žmogaus savybės (biometriniai duomenys, pav. 1 [5,6]), kurias sąlyginai galima skirstyti į dvi grupes.

Pirmajai grupei dažniausiai priskiriamos šios unikalios fiziologinės žmogaus kūno savybės: rankos plaštakos geometrija; veninių kraujagyslių išsidėstymas išoriniame ir vidiniame plaštakos paviršiuje; pirštų ir delno papiliariniai raštai; vieninių kraujagyslių išsidėstymas delno paviršiuje; akies rainelės ir tinklainės piešinys; veido bruožai, ausies geometrija, genetinio kodo fragmentai ir veido termograma.

Antrajai grupei priskiriamos individualaus elgesio savybės ir charakteristikos:



Pav. 1. Unikalūs žmogaus fiziologiniai požymiai ir individualaus elgesio savybės rašto rašymo forma ir atlikimo būdas; darbo su klaviatūra charakteristika; balso parametrai, eisena.

Be šių paminėtų unikalių žmogaus kūno požymių ir elgesio savybių asmens tapatybės nustatymui rečiau yra naudojami: kūno kvapas; epiderminė odos struktūra po nagu; odos elementų cheminė struktūra.

Asmens automatizuoto tapatybės nustatymo sistemos, kurių darbas paremtas išvardytomis unikaliomis žmogaus kūno ir elgesio charakteristikomis, vadinamos biometrinėmis. Jų istorija visiškai neilga. Ir čia turėtų būti atkreipiamas dėmesys į tai [1], kad tapatybės nustatymo procedūros platesne prasme, naudojančios biometrinius duomenis (klasikinė daktiloskopija, habitoskopija, raštotyra), yra naudojamos gana seniai.

Biometrinių sistemų panaudojimas leidžia spręsti šiuos uždavinius [7– 9]:

- verifikavimo (*angl. verification*);
- identifikavimo (*angl. identification*);
- paieškos (stebėjimo) sąrašo analizės (*angl. watchlist arba dar kitaip – open – set identification*).

Verifikavimas – tai asmens tapatybės nustatymas, kai asmens pateikiamus biometrinius požymius (požymį) biometrinė sistema sulygina tik su vieno asmens biometriniais požymiais (požymiu), esančiais sistemos duomenų bazėse. Šiuo atveju visa atpažinimo procedūra susideda iš dviejų arba daugiau etapų – pvz. slaptažodžio surinkimas, specialios kortelės panaudojimas ir paskutiniame etape asmens biometrinių duomenų pateikimas. Sistema priima sprendimą ar tas asmuo, kuris pateikė biometrinius požymius ar požymį, yra tas pats, kuriuo jis bando prisistatyti ir kurio duomenys yra saugomi duomenų bazėse.

Sąvoka verifikavimas ar tiesiog verifikacija yra analogiška sąvokai autentifikacija [1]. Galima pažymėti, kad biometrijoje sąvoka autentifikacija vartojama dažniausiai tais atvejais, kada apilai kalbama apie asmens tapatybės nustatymą nekonkretizuojant šios procedūros detalių [7]. Su verifikacijos uždaviniu praktikoje galima susidurti pavyzdžiui įėjimo kontrolės į spec. patalpas ir teritorijas metu, atliekant finansines operacijas ir kt.

Identifikavimas – tai asmens, kurio duomenys saugomi biometrinės sistemos duomenų bazėje, tapatybės nustatymas. Šiuo atveju asmens biometrinius požymius (požymį) biometrinė sistema sulygina su daugelio kitų asmenų biometriniais požymiais (požymiu), esančiais sistemos duomenų bazėse. Sistema turi atsakyti į klausimą – kas yra nagrinėjamas asmuo? Priešingai negu verifikavimo uždavinio atveju, visa atpažinimo procedūra susideda iš vieno etapo, kuriame pateikiami tik asmens biometriniai duomenys.

Paieškos (stebėjimo) sąrašo analizės atveju sistemai pateikiamas asmens biometrinis požymis ar požymiai. Sistema turi atsakyti į klausimą: ar asmuo yra ieškomų ar sistemos stebimų asmenų sąrašė?

3. BIOMETRINIŲ AUTENTIFIKAVIMO SISTEMŲ STRUKTŪRA IR PANAUDOJIMO SRITIS

Pirmosios automatizuotos biometrinės sistemos buvo pradėtos naudoti dvidešimtojo amžiaus aštunto dešimtmečio viduryje sistemose [5], kontroliuojančiose ir valdančiose įėjimą į fizines zonas. Dėl šių sistemų aukštos kainos, jos buvo naudojamos dažniausiai valstybinėse organizacijose, užtikrinant ypatingai aukštą slaptumo lygį. Greitas biometrinių technologijų vystymasis sąlygojo šių sistemų kainų mažėjimą ir pritaikymo sričių plėtojimą.

Dabartiniu metu biometrinę sistemą sudaro šie pagrindiniai elementai [9]:

- biometrinių požymių nuskaitymo (skenavimo) ir šių duomenų pakeitimo į elektroninę formą (signalą), išskiriant charakteringus požymius, įrenginys;

- elektrinio signalo apdorojimo įrenginys. Čia atliekamas biometrinių duomenų kokybės įvertinimas ir biometrinio „šablono“ sudarymas. Šiuo metu egzistuojantys tarptautiniai standartai nustato apsisikeitimo biometriniais duomenimis formatus ir reikalavimus formatams duomenų įrašymui, saugojimui, registracijai ir informacijos perdavimui;
- biometrinių duomenų (šablonų) bankas, kuriame yra saugojami duomenys gaunami iš įvairių biometrinių duomenų registravimo įrenginių, nepriklausomai nuo jų geografinio išdėstymo;
- naujai sudarytų biometrinių šablonų sulyginimo su jau esančiais duomenų bazėje įrenginys;
- sistemos sprendimo, pagal biometrinių duomenų sulyginimo rezultatą, priėmimo ir vaizdavimo įrenginys.

Šiuolaikinės automatizuotos biometrinės sistemos yra naudojamos įvairiose srityse [5, 6] : užtikrinant informacijos apdorojimo sistemų apsaugą; policijos veikloje ir valstybės sienos apsaugoje (kriminalistikoje, pasienio kontrolės punktuose); skirstant įvairias socialines išmokas; atsiskaitant už prekes ar paslaugas prekybos įstaigose; naudojantis bankomatų ir prekybos automatų paslaugomis; kontroliuojant ir valdant įėjimą į valstybines organizacijas, patalpas ir uždaras teritorijas (oro uostai, jūrų uostai, karinės bazės, elektrinės, naftos perdirbimo įmonės, specialios paskirties įmonės) bei virtualias zonas (priėjimas prie tam tikrų elektroninių paslaugų).

Daugelyje šalių biometrinės sistemos plačiai naudojamos kontroliuojant įvažiuojančius į šalį asmenis (pvz. JAV, JAV ambasadose (tame tarpe ir Lietuvoje), Kanadoje, Australijoje, Saudo Arabijoje ir kt.). Jos įgalina identifikuoti asmenis, kurie yra įtraukti į „apribojimų sąrašus“. Šiuo tikslu artimiausiais metais biometrinės sistemos planuoja įdiegti ir visos Europos Sąjungos šalys. Šengeno sutartį pasirašiusios šalys susitarė pakeisti įvažiavimo vizų formatą, vizose bus fiksuojama asmens tapatybę patvirtinanti biometrinė informacija (veidas, piršto atspaudas, akies rainelė). ES mastu šia tema vyksta ir įvairios konferencijos.

Pažymima, kad šiuo metu didesnę dalį visų pasaulyje naudojamų automatizuotų biometrinių sistemų sudaro biometrinės daktiloskopinės identifikavimo sistemos. Pagrindinėmis nagrinėjamo tipo biometrinių sistemų kūrimo ir gamybos srityje galima laikyti šias JAV [10 – 14] ir Rusijos [15] firmas.

Nagrinėjant automatizuotas biometrinės autentifikavimo sistemas, aptariami jų privalumai ir trūkumai. Atkreipiamas studentų dėmesys į nagrinėjamų asmens tapatybės nustatymo metodų paklaidas, pirmo ir antro laipsnio klaidų tikimybes.

IŠVADOS

1. Dabartiniu metu vykdant informacinės visuomenės plėtros darbus ypatingą svarbą turi klausimai, susiję su informacinių technologijų ir kitų svarbios paskirties objektų sauga, asmenų tapatybės nustatymo procedūromis.
2. Biometrinių sistemų panaudojimas prieglobsčio suteikimo, nelegalios migracijos ir terorizmo prevencijos ir kontrolės procesuose, yra numatomas kaip vienas iš svarbių prioritetų Europos Sąjungoje.
3. Informatikos studijose studentai įgyja teorinių informacijos apsaugos žinių, toliau jie įtvirtina apsaugos metodų taikymo kompiuterizuotose policijos ir VSAT darbo vietose mokėjimus ir įgūdžius.
4. Analizuojant automatizuotas biometrines autentifikavimo sistemas, aptariamas jų struktūra, sistemos sprendžiami uždaviniai, pritaikymo sritys, privalumai ir trūkumai. Atkreipiamas dėmesys į nagrinėjamų biometrinių asmens tapatybės nustatymo metodų paklaidas.

LITERATŪRA

1. Stupak V., Vasiliauskas R. Autentifikavimo procedūrų nagrinėjimo informatikos ir informacinių technologijų studijose aspektai// Teoriniai ir praktiniai statutinių pareigūnų rengimo aspektai. Respublikinės mokslinės konferencijos straipsnių rinkinys. ISBN 9955–9777–0–1. –Kaunas: MRU KPF, 2005. – P. 101 – 110.
2. Jastramskas V. Informacijos apsaugos pagrindai. Kaunas: Technologija, 1999.
3. LST ISO 2382-8 : 1995. Informacijos apdorojimo sistemos. Terminai ir apibrėžimai. 8-oji dalis. Valdymas, vientisumas, saugumas. – Lietuvos standartizacijos departamentas.
4. Miller B. Vital signs of identity. IEEE Spektrum, 31(2). New York: IEEE, 1994. – P. 22–30.
5. The Biometric Consortium <<http://www.biometrics.org>>.
6. International Biometric Group <<http://www.biometricgroup.com>>.
7. Biometric Glossary <<http://www.biometrics.gov>>.
8. Blackburn D. Biometrics 101 <<http://www.biometriccatalog.org>>.
9. Bolle R., Connell J., Pankanti S., Ratha N., Senior A. Guide to Biometrics. New York: Springer – Verlag, 2004.
10. Cross Match Technologies, Inc. <<http://www.crossmatch.net/index2.html>>.
11. Identix, Inc. <<http://www.identix.com>>.
12. Iridian Technologies, Inc. <<http://www.iridiantech.com>>.
13. Lone Wolf Software, Inc. <<http://www.lonewolfsoftware.com>>.
14. Recognition System, Inc. <<http://www.recogsys.com>>.
15. Identification Technologies Company <http://www.itec.snz.ru/about_company.phtml>.

**THE ASPECTS OF ANALYSIS OF BIOMETRIC AUTHENTICATION
SYSTEMS OF THE TEACHING OF COMPUTER SCIENCE**

Viktoras Stupak*

Raimondas Vasiliauskas**

Mykolas Romeris University

S u m m a r y

At the faculty of Public Safety of Mykolas Romeris University, subjects of computer science are taught during the first, second and third year. For the program of preparation of bachelors for a specialty of the right and protection of frontier, these disciplines are taught during the first and third years. For the program of preparation of bachelors for a specialty of the right and activity of police – during the first year. For non– university training, under the program activity of police – during the first and second years. In programs of subjects during studying the means of safety for both information technologies, and other objects, the consideration of biometrics authentication systems is stipulated.

Features of consideration of biometrics authentication systems at studying computer science are analyzed. Classification of biometrics systems is provided. Two groups of the automated biometrics systems are analyzed. The systems using unique physiological features of human are included in the first group. The second group includes the systems using specific features of behavior. The structure of the systems, tasks they carry out and areas of their application are analyzed.

**BIOMETRINIŲ ATPAŽINIMO SISTEMŲ EFEKTYVUMO NAGRINĖJIMO
INFORMATIKOS STUDIJOSE ASPEKTAI**

Viktoras Stupak*

* Mykolas Romeris university Kaunas Faculty assoc. prof. dr. of Police Activity Department

** Mykolas Romeris university Kaunas Faculty assoc. prof. dr. of Police Activity Department