



REPUBLIKA SLOVENIJA

MINISTRSTVO ZA NOTRANJE ZADEVE  
POLICIJA

Roman Batis

OD MEHANOGRAFSKE

OBDELAVE PODATKOV

DO SCHENGNA

REPUBLIKA SLOVENIJA  
MINISTRSTVO ZA NOTRANJE ZADEVE  
**P O L I C I J A**

Roman Batis

**50 LET**  
**INFORMATIKE IN TELEKOMUNIKACIJ**  
**V SLOVENSKI POLICIJI**

**OD MEHANOGRAFSKE OBDELAVE PODATKOV**  
**DO SCHENGNA**

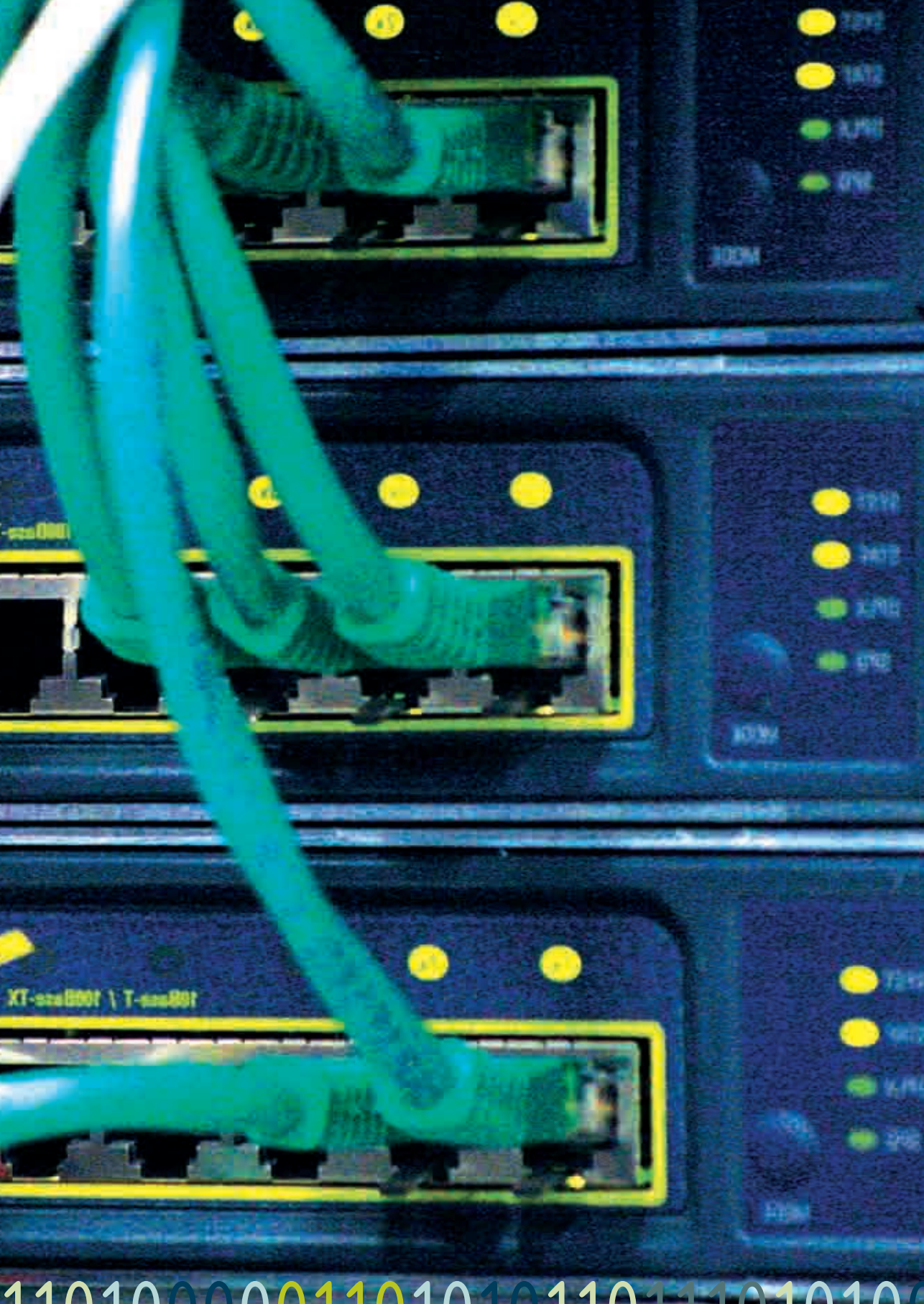






0101010111100010110110110101





1101000001101010110111010100

**Izdalo:** Ministrstvo za notranje zadeve Republike Slovenije, Policija

**Idejna zasnova in vsebina:** Roman Batis

**Tehnična obdelava:** Jelka Smrekar

**Lektoriranje:** Zdenka Zabukovec

**Oblikovanje:** Boris Teodorovič

**Tisk:** Tiskarna Pleško, d. o. o.

Ljubljana 2008



Nagovor ministra za notranje zadeve .....	7
Spremna beseda generalnega direktorja policije .....	9
Predgovor .....	11
I. Uvod .....	13
II. Pregled pomembnejših dogodkov, ki so zaznamovali razvoj informacijsko-telekomunikacijskega sistema Policije (ITSP) v petdesetih letih .....	14
III. Razvoj telekomunikacijskega sistema Policije .....	26
IV. Razvoj kriptozasčite .....	28
V. Razvoj varstva in zavarovanje (osebnih) podatkov .....	29
VI. Organiziranost Urada za informatiko in telekomunikacije (UIT) .....	32
- Pristojnosti in naloge .....	32
- Organiziranost .....	33
- Center za informatiko .....	33
- Center za zaščito podatkov .....	33
- Center za telekomunikacije .....	34
VII. Zaposleni v UIT .....	36
VIII. Usposabljanje in izpopolnjevanje v UIT .....	37
IX. Sodelovanje z domačimi in tujimi ustanovami .....	39
X. Publicistika .....	41
XI. Najpomembnejše informacijsko-telekomunikacijske rešitve .....	42
- Fonetičen indeks oseb (FIO) .....	42
- Elektronska pošta Policije (EPP) .....	42
- Internet .....	42
- Schengenski informacijski sistem (SIS) .....	43
- Nove funkcije SIS .....	47
- Sirene .....	48
- Prümska pogodba .....	49
- Novi informacijski sistem policijske postaje (ISPP) .....	51
- Intranet Policije .....	52
- Prenova fiksnega govornega omrežja Policije .....	53
- Klicni centri 113 .....	56
- Prenova informacijsko-telekomunikacijske infrastrukture .....	57
- Digitalni mobilni radijski sistem .....	57
XII. Investicije v informacijsko telekomunikacijska sredstva policije .....	60
XIII. UIT - skrbnik evidenc .....	61
XIV. Vizija .....	63
XV. Vodje informatike in telekomunikacij .....	64
Viri .....	65



0101010111100010110110110110101

# SCHENGENSKEMU INFORMACIJSKEMU SISTEMU NA POT -

## SPREMNA BESEDA MINISTRA ZA NOTRANJE ZADEVE OB 50-LETNICI INFORMACIJSKEGA IN TELEKOMUNIKACIJSKEGA SISTEMA SLOVENSKE POLICIJE

Spoštovani!

Lani smo se slovesno pridružili skupnemu schengenskemu prostoru. Po naključju se je tako pomemben dogodek, kot je vstop Slovenije v »schengen«, časovno ujel s praznovanjem 50-letnice informacijsko-telekomunikacijskega sistema slovenske policije. Prav informacijsko-telekomunikacijski sistem policije je bil osnova za uspešno integracijo v schengenski informacijski sistem (SIS) in je omogočil izpolnitev vseh informacijsko-tehnoloških zahtev schengenskega nadzora zunanjih meja. Naše priprave na vključitev v schengensko varnostno območje so obsegale številne kadrovske, organizacijske in druge ukrepe. Vendarle pa je implementacija ustreznih informacijskih rešitev v relativno kratkem času za uspešno integracijo nacionalnega s schengenskim informacijskim sistemom pomenila tisti še zadnji korak, brez katerega se o Sloveniji kot schengenski novinki ne bi mogli pogovarjati že konec lanskega leta.

Projekt schengenskega informacijskega sistema druge generacije, t. i. SIS II, je zamujal. Zato smo morali skupaj z drugimi državami članicami poiskati povsem konkretno rešitev, ki bi novim članicam omogočila čimprejšnji vstop v schengenski prostor, brez dodatnih zamud. Pri tem smo bili v Sloveniji še posebej aktivni, tako da nam tudi drugi priznavajo vodilno vlogo pri trdih pogajanjih za širitev schengenskega prostora. Na pobudo Portugalske in ob naši podpori je bila decembra 2006 sprejeta odločitev za prehodno rešitev, imenovano SISone4ALL. V vzpostavitev SIS smo nato vložili še veliko truda in sredstev, prestali pa smo tudi vsa predpisana ocenjevanja zunanjih strokovnjakov, t. i. schengensko evalvacijo. Ob tem smo uspeli vzpostaviti potrebno IT infrastrukturo in integracijo SIS z nacionalnim informacijskim sistemom ob upoštevanju vseh zahtev za varovanje osebnih podatkov v okviru tega sistema. Zagotovili smo informacijsko podporo za nacionalni urad Sirene, ki skrbi za mednarodno policijsko sodelovanje v schengenskih zadevah. Vse to je bil še zadnji pogoj za odločitev o dokončni odpravi kontrole na notranjih mejah v noči na 21. december 2007.

Veseli me, da so rezultati uvedbe nove informacijske podpore v boju proti ilegalnim migracijam in čezmejnemu kriminalu že vidni. V devetih mesecih uporabe te skupne elektronske baze podatkov je bilo v Sloveniji na zunanji meji opravljenih že za dobrih 14,6 milijona preverjanj oseb, listin in vozil in doseženih več kot pet tisoč zadetkov pri iskanih osebah ali predmetih! Tudi odzivni časi pri preverjanju so dobri, kar dokazuje, da slovenski policisti dobro poznajo uporabo tega sistema, ki je eden glavnih izravnalnih ukrepov za zagotavljanje ustreznih ravni varnosti v skupnem schengenskem prostoru po ukinitvi kontrole na notranjih mejah. Kvalitetna IT podpora, ki omogoča dostop do podatkov drugih držav o določenih posameznikih in predmetih, je predpogoj za uspešno izvajanje mejne kontrole na zunanjih mejah v imenu vseh članic.



S tem pa se je naša vloga v elitnem »klubu« schengenskih držav šele dobro začela. Ena prednostnih nalog med slovenskim predsedovanjem Svetu EU je bilo uvajanje SIS druge generacije, ki naj bi ga prevzeli predvidoma septembra naslednje leto. Poleg tega sodelujemo pri integraciji Švice v obstoječi SIS in pri tamkajšnji schengenski evalvaciji. Švica se je med slovenskim predsedovanjem že tehnično povezala v obstoječi SIS (s pomočjo portugalske prehodne rešitve SISone4ALL). Izvedli smo vsa potrebna testiranja, vključno s funkcionalnim testiranjem urada Sirene.

Zavedati se moramo, da odprte meje pomenijo novo poglavje v svobodi državljanov, a tudi večje varnostne izzive. Zadovoljen bom, če bo policijska informatika tudi v prihodnje, v naslednjih petdesetih letih svojega delovanja, tako uspešna in v takšno pomoč pri zagotavljanju varnosti slovenskih državljanov in državljanov EU, kot je bila doslej.



Dragutin Mate  
Minister za notranje zadeve





Spoštovani!

Dobro se še spomnim časov, ko so policisti depeše po cele popoldneve sprva pisali na roke, nato pa pretipkavali na pisalne stroje. Vse pomembne dokumente so prenašali v torbah in potrebnega je bilo kar precej časa in iznajdljivosti, da je informacija prišla od sporočevalca do prejemnika. Takrat si nismo mogli predstavljati, kako velike informacijske in tehnološke spremembe so pred slovensko policijo, tedanjo milico. V petdesetih letih smo od pisalnih in mehanografskih strojev ter ročnega vodenja seznamov po principu luknjanja kartic, ki je takrat pomenil vrhunec tehnološkega napredka, naredili skoraj neverjeten preskok v digitalno dobo.

Slovenska policija je bila med prvimi organizacijami v Sloveniji, ki so v svoje delovanje začele uspešno uvajati informacijsko-telekomunikacijsko podporo. Vzporedno z razvojem IT sistema in nalog se je spreminjala tudi organiziranost informatike in telekomunikacij, da bi lahko uporabniki kar najbolj učinkovito obvladovali moderne informacijsko-telekomunikacijske storitve. Tako delo v sodobni policiji brez najnovejših tehnoloških rešitev in razvejanega komunikacijskega omrežja praktično ni več mogoče. Policisti bi bili danes nemočni brez radijskih zvez in računalnikov ter spletne tehnologije, da ne govorimo o vseh drugih sistemih, opremi in napravah, ki omogočajo njihovo vsakodnevno opravljanje policijskih nalog. Kot pomembno orodje pri komuniciranju z javnostmi in izboljševanju javne podobe policije moram posebej izpostaviti tudi policijske spletne strani, preko katerih dodatno razvijamo partnerske odnose z državljani in institucijami ter tako prispevam k večji varnosti.

Pomembno vlogo je IT sistem odigral pri osamosvojitvi Slovenije. Policija je takrat potrebovala zanesljive komunikacijske poti, ki jim ne bi bilo možno prisluškovati. Takratna Uprava za informatiko je sprejela številne ukrepe, ki so omogočali varen prenos podatkov v vojnem času. Od tedaj se je policijska informatika skupaj s telekomunikacijami iz leta v leto le še posodabljala in nadgrajevala. Med najnovejšimi dosežki policijskega IT sistema pa je bila vsekakor vključitev v schengenski informacijski sistem, ki je s seboj prinesla nadgradnjo in nove rešitve ter prenovu IT infrastrukture. Tako lahko poskrbimo za še večjo zaščito podatkov, hitrejšo odzivnost policistov na terenu in še učinkovitejše operativno delo, kar nas umešča v sam vrh med evropskimi policijami.

Jože Romšek  
Generalni direktor policije



01010101111000101101101101101



Informacijsko – Telekomunikacijski Sistem Policije - **ITSPol** je lani slavil pomemben jubilej, 50 letnico razvoja. Pravzaprav gre za jubilej nekoč enovitega informacijsko – telekomunikacijskega sistema organov za notranje zadeve, ki ga je poleg ITSPol sestavljala tudi informacijski sistem upravnih notranjih zadev. Ker je bil to čas, ko so zelo intenzivno potekale naše priprave na polno integracijo v Schengenski informacijski sistem – SIS, nam je časa za slavlje zmanjkalo. Schengenska integracija je sedaj uspešno zaključena in prav je, da se spomnimo in slavnostno obeležimo oboje, tako pomemben jubilej – 50 letnico, kot tudi pomemben mejnik v razvoju ITSPol – integracijo s SIS. ITSPol je v okviru schengenske evalvacije prestal še en zahteven preizkus in dobil tudi potrditev ustreznosti s strani tujih ekspertov.

Pred vami je brošura, v kateri se boste lahko podrobneje seznanili z ITSPol in vlogo ter delovnim področjem ljudi, ki ga soustvarjajo. Za ITSPol skrbi skoraj 170 zaposlenih v Uradu za informatiko in telekomunikacije GPU MNZ, ki so organizirani v treh centrih: Centru za informatiko, Centru za telekomunikacije in Centru za zaščito podatkov. Sistemske in aplikativne ekipe Centra za informatiko skrbijo za zagotavljanje ustrezne informacijske podpore, v Centru za telekomunikacije so poleg tipičnih telekomunikacijskih vsebin (radijski sistemi, telefonija, prenosno omrežje), skoncentrirane še druge vsebine povezane s policijsko tehniko (video nadzor, tehnično varovanje, merilniki hitrosti in alkoholiziranosti), Center za zaščito podatkov pa skrbi za normativno ureditev in tehnične rešitve s področja varovanja osebnih in tajnih podatkov. Seveda ne smemo pozabiti na delavce Oddelkov za informatiko in telekomunikacije na policijskih upravah, ki skrbijo za prenos IT rešitev in neposredno podporo končnim uporabnikom.

Dovolite mi, da se v tem uvodnem nagovoru zahvalim vsem bivšim in zdajšnjim sodelavcem ter partnerjem, ki so soustvarjali ITSPol. Brez dvoma se lahko na dosežke v zadnjih 50 letih ozremo s ponosom. Zahvaljujem se tudi vodstvu Policije in Ministrstva za notranje zadeve za njihovo podporo pri razvoju ITSPol in razumevanje vloge in pomena ustrezne IT podpore. V današnjem, globalnem okolju so pred Policijo nedvomno veliki izzivi, k uspešnemu in učinkovitemu razreševanju problematike pa lahko veliko pripomore ustrezna informacijsko – telekomunikacijska podpora. Naj bodo torej doseženi rezultati vzpodbuda tudi za naprej!

Mag. Andrej Bračko

Direktor Urada za informatiko in telekomunikacije





0101010111100010110110110110101

# I. UVOD



Leta 2007 je Urad za informatiko in telekomunikacije GPU (UIT) praznoval petdeseto obletnico ustanovitve. Čeprav pet desetletij zgodovinsko ni posebej dolgo obdobje, pa je za informatiko ter telekomunikacije ravno pravnšnje, da je mogoče s primerne časovne razdalje razčleniti prehojeno pot in spoznati vse dosežke stroke. Z gotovostjo lahko trdimo, da se je ITSP od strojno-mehanografske do moderne računalniške obdelave podatkov razvijal zelo hitro in ambiciozno. Svoj vrh pa je dosegel z osamosvojitvijo Slovenije ter z vključitvijo v globalne informacijske sisteme.

SIS je bistveno vplival na razvoj slovenske policije in njeno vključevanje v evropske tokove, ITSP pa je primerljiv z informacijskimi sistemi v Evropi. Vključevanje v SIS je povezano s temeljito prenovo tega sistema in z uvajanjem številnih novih rešitev. Tako so za obdobje od leta 2000 značilni: intenzivna izgradnja lokalnih računalniških omrežij, kompletna prenova komunikacijskega omrežja in telefonije ter prehod z analognega na digitalni radijski sistem. V tem času je bil vzpostavljen tudi nov sodoben rezervni računalniški center, z možnostjo najboljšega dostopa do informacijsko-telekomunikacijskih storitev.

Na aplikativnem področju smo kompletno prenovili aplikaciji Informacijski sistem policijske postaje (ISPP) in Fonetični indeks oseb (FIO) – Mejna kontrola. Nacionalne informacijske rešitve pa smo povezali tudi s SIS. Upravna informatika se je ločila od policijske.

Tudi dostop policistov do podatkov upravnih notranjih zadev je v celoti prenovljen in temelji na sodobnih spletnih storitvah. Praznovanje se časovno ujema z vključitvijo Slovenije v schengensko območje, kjer poteka prost pretok ljudi, kapitala in storitev. Za Slovenijo je po osamosvojitvi, uvedbi evra in dokončni vključitvi v družino evropskih narodov to gotovo eden vrhuncev zgodovinskega razvoja.

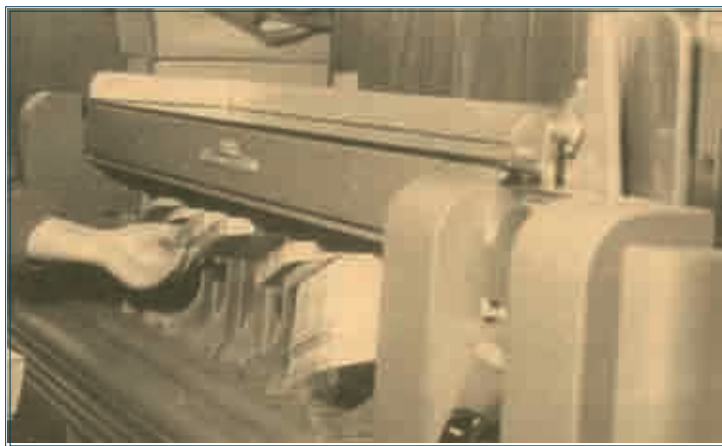
Uvajanje moderne policijske informatike je vsekakor prispevek vseh zaposlenih in tudi tistih, ki so UIT že zapustili in se upokojili. Vsem, ki so kakor koli pripomogli k ambicioznemu razvoju, ob jubileju iskreno čestitamo.



## II. PREGLED POMEMBNEJŠIH DOGODKOV, KI SO ZAZNAMovali RAZVOJ ITSP V PETDESETIH LETIH

### ZAČETKI MEHANOGRAFSKE OBDELAVE PODATKOV 1957–1967

Leta 1957 se je začela strojna oz. mehanografska obdelava podatkov, ki je postopoma zamenjala prejšnje ročno vodenje obsežnih kartotek<sup>1</sup> in seznamov. Ti stroji so bili zelo preprosti, niso bili še računalniki v današnjem pomenu besede, ampak mehanografski stroji, ki so zagotavljali osnovo za statistično raziskovanje in obdelavo podatkov. To je bil za tisti čas vsekakor velik napredek. Podatki so se vpisovali v 80-kolonske luknjane kartice, ki jih je bilo možno na sortirnih strojih sortirati po poljubnih pojmih, nato pa podatke na posebnem stroju izpisati v ustreznih tabelah. Poskusna obdelava podatkov o kaznivih dejanjih<sup>2</sup> je potekala na mehanografskih strojih Zavoda za statistiko in podjetja Organizator, kasneje pa je RSNZ stroje najel oziroma odkupil.



1 V takratnem Državnem sekretariatu za notranje zadeve so v petdesetih letih prejšnjega stoletja vodili več seznamov oziroma kartotek, med drugim centralno kartoteko, kartoteko pogrešanih oseb, najdenih neznanih trupel, ukradenih predmetov, poklicnih storilcev po MOS ipd. Za lažje iskanje in pregledovanje so bile kartoteke zložene v kartotečnih bobnih, še pred tem pa v predalnih omarah. Kartoteke so bile zložene po strogo abecednem vrstnem redu. Zbiranje in urejanje evidenc je bilo v prvem obdobju še neurejeno in je pogosto prihajalo do podvajanja podatkov. Po šestdesetem letu so v sekretariatu za notranje zadeve z navodilom centralizirali urejanje evidenc ter statistično poročanje. V ta namen so bile kasneje v posameznih obdobjih ustanovljene službe, ki so se ukvarjale z evidencami, statističnim poročanjem in administracijo. Preverjanje in poročanje posameznih policijskih enot se je izvajalo depešno preko teleprinterskega omrežja.

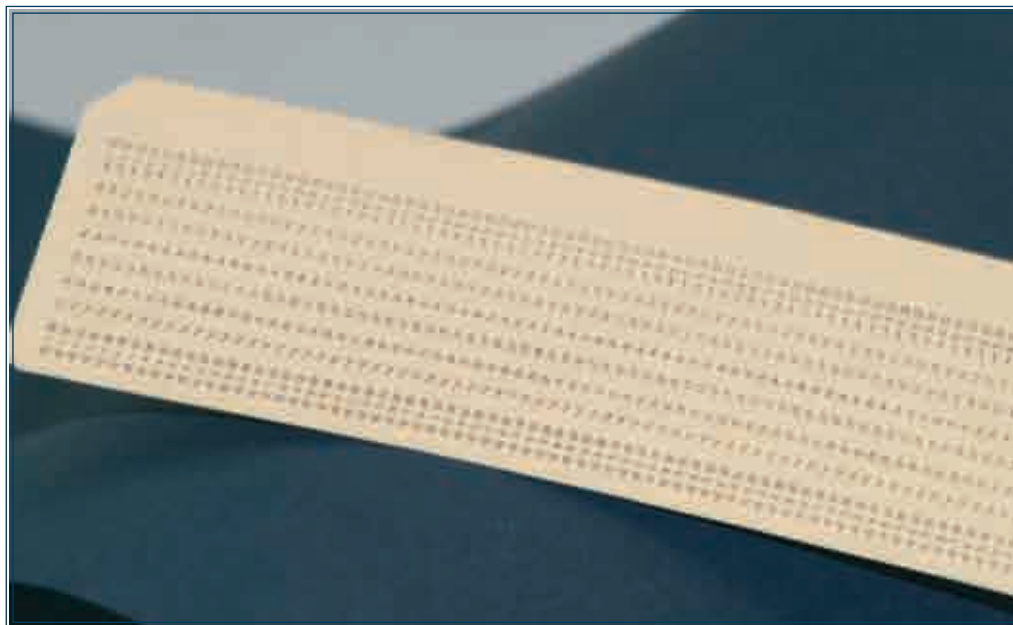
2 Najprej so bili na luknjane kartice preneseni podatki iz kartoteke kaznivih dejanj (1957), naslednje leto iz kartoteke prometnih nezgod, nato evidenca registriranih motornih vozil in lastnikov (1959), emigrantov in tujih diplomatov (1960), krvnih izvidov voznikov (1961) itn.

Ta način obdelave se je za takratne razmere pokazal kot zelo uspešen, zato smo leta 1961 kupili lasten komplet mehanografskih strojev. Zaradi hitrega razvoja avtomatizacije obdelave podatkov in naraščanja potreb organov za notranje zadeve po najrazličnejših obdelanih podatkih, je ta oprema v nekaj letih zastarela. Najprej smo na luknjane kartice prenesli kartoteke o kaznivih dejanjih, v naslednjih letih pa še kartoteke o prometnih nesrečah, o registriranih motornih vozilih in lastnikih, o emigrantih, o krvnih izvidih voznikov, ki jim je bila odvzeta kri, ipd. Depeše in različna obvestila so se v tem obdobju prenašala po teleprinterskem in telefonskem omrežju. Podatki so bili zavarovani s preprostimi tehničnimi in fizičnimi ukrepi, varen prenos pa je zagotavljala kriptozasčitna služba.

Leta 1967 je posebna komisija sprejela odločitev o prehodu na elektronsko obdelavo podatkov z ustrežno zmogljivim računalnikom. V ta namen so bile izvedene tudi ustrezne kadrovske in organizacijske priprave, naslednje leto pa so delavci organi za notranje zadeve že začeli delati na tujih računalnikih.

### Pomembnejši dogodki v tem obdobju:

- 1957:** - prva zbirka podatkov na luknjanih karticah – kazniva dejanja
- 1960:** - prva iskanja storilcev kaznivih dejanj po t. i. »modus operandi sistemu« (MOS) s pomočjo luknjanih kartic
- 1961:** - RSNZ najame nepopolno garnituro strojev luknjanih kartic
- 1963:** - RSNZ najete stroje odkupi
- 1967:** - imenovana je komisija za uvedbo elektronskega sistema za obdelavo podatkov v RSNZ





## PRVI KORAKI RAČUNALNIŠKEGA OBDELOVANJA PODATKOV V ORGANIH ZA NOTRANJE ZADEVE 1968–1977



V tem obdobju so bili postavljeni sistemski, organizacijski, kadrovski in tehnični temelji računalniško podprtega informacijskega sistema organov za notranje zadeve (ISONZ). Vse do leta 1972, ko je RSNZ dobil v najem prvi elektronski računalnik, so potekale pospešene priprave za prehod z mehanografske na avtomatsko<sup>3</sup> (elektronsko) obdelavo podatkov. Uradno odprtje lastnega elektronskega računskega centra, opremljenega z najetim računalnikom IBM 360/25, je bilo leta 1972. To leto je mejnik, ko se je začela prva avtomatizacija vodenja evidenc organov za notranje zadeve.

Delo na lastnem računalniku je omogočilo intenziven razvoj aplikacij in organizacijo podatkov iz obstoječih evidenc<sup>4</sup> na računalniških medijih (registracija vozil, statistika kriminalitete, MOS). Računalnik IBM 360/25 je bil že za takratne razmere sorazmerno malo zmogljiv. Zato je bila njegova izkoriščenost, kljub delu v več izmenah, presežena. Omejitve pa so se kazale tudi v zmogljivosti samih magnetnih diskov za vpis evidenc, do katerih je moral imeti računalnik stalen dostop. Na računalniku ni bilo možno organizirati obdelave množičnih evidenc, kot je bila npr. centralna abecedna evidenca. Zato se je že kmalu pokazala potreba po nabavi novejšega in zmogljivejšega računalnika.

V tem obdobju se je pokazalo kot neustrezno in prepočasno tudi samo sporočanje podatkov iz računalniškega centra policijskim enotam po vsej Sloveniji, ki je potekalo po telefonskih in telegrafskih zvezah ali interni pošti. Z novim računalnikom 4. generacije IBM 370/145 leta 1976 pa so bile dane tehnične možnosti za razvoj daljinske oz. lokalne terminalne mreže in obdelave podatkov. Pomemben razvoj je bil tudi na področju mikrofilske obdelave dokumentov, še posebej po nabavi sodobnega sistema MIRACODE, ki je omogočil hiter dostop do podatkov, posnetih na mikrofilmu. Vse pomembne podatke so v tem obdobju preslikali na

3 Brvar v svoji knjigi navaja, da se konec šestdesetih in v sedemdesetih letih najpogosteje uporablja kratica EOP – elektronska obdelava podatkov. Tako je bil tudi leta 1971 ustanovljen Sektor za elektronsko obdelavo podatkov pri RSNZ. Šele kasneje se začne uveljavljati izraz AOP – avtomatska obdelava podatkov, medtem ko se pojem informacijski sistem organov za notranje zadeve pojavi leto pred ustanovitvijo Komisije ISONZ – 1975.

4 Iz evidence na luknjanih karticah in kartotekah se je v računalniško evidenco najprej prenesel register motornih vozil (leta 1968), v naslednjih letih pa še ostale evidence, zadnja CEK leta 1977, ki se preimenuje v CAE. To je bila osnovna in najboljšežnejša baza podatkov policije in vsebuje podatke o osebah, ki so bili obravnavani v najrazličnejših postopkih ONZ (zaradi kaznivega dejanja, prekrška zoper javni red in mir, prometnega prekrška, zaradi razpisane tiralice ipd.).



mikrofilm, kopije pa je bilo ob izpadu računalnika možno uporabljati preko mikrofilmskih čitalnikov.

Mejnik v razvoju policijske informatike je bil prenos Centralne evidenčne kartoteke (CEK) v računalniško evidenco, ki je trajal več kot dve leti. Evidenca se je tudi preimenovala v Centralno abecedno evidenco (CAE). Pri zavarovanju podatkov so v ospredje prihajala vprašanja identifikacije in avtorizacije uporabnikov, avtomatskega evidentiranja vseh dostopov do podatkov, alarmiranja pri poskusih nepooblaščenega dela na terminalih ipd. Pomemben dogodek v razvoju ISONZ-a je bila ustanovitev Komisije za ISONZ (6. 3. 1975), ki je odločala o razvoju informacijskega sistema, o nabavi računalniške in mikrofilmske opreme, načinu opremljanja



takratnih uprav javne varnosti (UJV), postaj milice in služb v Republiškem sekretariatu na notranje zadeve (RSNZ), uvajanju novih pomembnih aplikacij, usklajevanju sodelovanja med Elektronskim računalniškim centrom (ERC) in operativnimi službami.

Imela je sedem podkomisij, in sicer za javno varnost; upravne notranje zadeve; varovanje ustavne ureditve; operativne evidence; kadrovske zadeve; materialno-finančne zadeve in za področje signala. Sestavljali so jo vodilni delavci RSNZ. Še v istem letu je skupščina SR Slovenije z odlokom opredelila finančna sredstva za nabavo računalniške in mikrofilmske opreme ONZ ter pooblastila RSNZ, da prevzame finančno-materialno odgovornost pri zbiranju sredstev za razvoj oziroma vzpostavitev informacijskega sistema za upravne notranje zadeve. Prvi dogovor je bil sklenjen s tedanjo Skupščino mesta Ljubljana.

Širjenje ISONZ v občinah in UJV pa je zahteval vzpostavitev in tudi sistemiziranje novih delovnih mest organizatorjev - programerjev na regijski ravni, ki so postali pomemben člen pri usmerjanju in razvoju ISONZ.

### Pomembnejši dogodki v tem obdobju:

- 1968:** - poskusne obdelave podatkov na elektronskem računalniku IBM v organizacijah (DES, Ljubljanska banka, Slovenija vino)
- prva evidenca na magnetnem disku - register motornih vozil

5 Uredba Zveznega izvršnega sveta je v letih 1972-1975 prepovedala nakup računalnikov, zato je RSNZ najemal računalnike pri slovenskih podjetjih (kot navaja tudi Brvar).

- 1971:** - ustanovitev sektorja za EOP v Službi za operativne evidence
- 1972:** - v RSNZ začne obratovati prvi najeti<sup>5</sup> računalnik IBM 360/25
- 1975:** - ustanovitev Komisije za ISONZ
- avtomatizacija poslovanja oddelkov za notranje zadeve v občinah
  - začetek prenosa centralne evidenčne kartoteke na računalnik
  - mikrofilmski servis dobi sistem MIRACODE
  - Odlok o financiranju opreme za ISONZ
  - Sektor za EOP preide v V. oddelek Službe državne varnosti (SDV)
  - ustanovitev lastne tehnične službe v ERC-u
  - začetek prenosa Centralne evidenčne kartoteke v računalniško evidenco
- 1976:** - RSNZ dobi nov računalnik 4. generacije IBM 370/145
- uporabljati se začne programski jezik PL/I in DOS/VS ter CICS
  - delovati začne prva lokalna terminalna mreža
  - prvi organizatorji-programerji na upravah za notranje zadeve (UNZ)

## DECENTRALIZACIJA INFORMACIJSKEGA SISTEMA ORGANOV ZA NOTRANJE ZADEVE IN VKLJUČEVANJE UPORABNIKOV PREKO TELEKS OMREŽJA

1978-1984

Za obdobje sta značilna decentralizacija ISONZ, ki se kaže v postopnem približevanju končnemu uporabniku, ter sklenitev Družbenega dogovora o enotnem informacijskem sistemu na področju notranjih zadev<sup>6</sup>. Prihaja do pospešene izgradnje daljinske terminalske mreže za področje upravnih notranjih zadev in za UJV, opustitev luknjanih kartic in prehod na off-line in on-line zajemanje podatkov ter posodobitev mikrofilmskega servisa s COM napravo. Ta je omogočila prenos podatkov iz magnetnega traku neposredno na mikrofilm. Informatiki so začeli izgradnjo banke podatkov ISONZ, v katero so združili oziroma povezali več datotek<sup>7</sup>. Leta 1979 se ERC združi z Upravo za analitiko in informatiko in v njeni sestavi deluje kot Center za avtomatsko obdelavo podatkov.

Že naslednje leto se informatika izloči iz Uprave za analitiko in se reorganizira, tokrat v povsem samostojno upravo v RSNZ – Upravo za informatiko. Ta postane prvič enakovredna drugim organizacijskim enotam v sekretariatu (Upravi milice, Upravi kriminalistične službe, Upravi službe državne varnosti ipd.). V tem obdobju je bila vzpostavljena tudi neposredna računalniška zveza med RSNZ Slovenije in Hrvaške ter zagotovljena pomoč pri organiziranju terminalske mreže med olimpijskimi igrami v Sarajevu. Za krajše izpise podatkov

6 Leta 1982 je bil izdan Zakon o družbenem sistemu informiranja, ki je uvedel skupne osnove (registrov, evidenc, klasifikacij) in povezovanje podatkov in je bil pomemben mejnik v razvoju registrske usmeritve Slovenije in ONZ. Vzpodbudil je nadaljnji razvoj registrsko usmerjene statistike ter izgradnje in standardizacije evidenc. Zanimivo je tudi, da je že Zakon o družbenem sistemu informiranja vseboval določbo, da so zaradi varstva osebne svobode in zaščite osebnosti ter z ustavo in zakonom zagotovljenih pravic posameznika osebni podatki predmet posebne zaščite, ki jo ureja zakon, in ta zakon je bil sprejet leta 1999 kot Zakon o varstvu osebnih podatkov (Ur. l. SRS, št. 8/1990).

7 Register motornih vozil, register legalnih imetnikov orožnih listov, register ovadenih oseb, MOS evidenca, register prebivalstva petih ljubljanskih občin in evidenca oseb na prestajanju zaporne kazni. Banko podatkov so leta 1981 razširili še na iskane osebe po glasniku, osebe v kazenski evidenci, voznike motornih vozil, osebe, evidentirane v posebnih operativnih akcijah, in osebe, zanimive za SDV.





so v tem obdobju delavci ERC-a razvili in razrešili problem vključitve teleks omrežja na računalnik, saj je bilo to omrežje prevladujoče in je segalo do vsake postaje milice.

Zaradi naraščajočih potreb po dodatnih računalniških zmogljivostih in za nadomeščanje glavnega računalnika ob izpadih ali okvarah je bil leta 1979 nabavljen dodatni računalnik IBM 3031.

Ta je bil štirikrat močnejši od IBM 370/145 in je vzdrževal terminalsko mrežo. Na obeh računalnikih so vpejlali tedaj najnovejše verzije sistemskih programov, ki so omogočali boljše izrabo računalniških zmogljivosti.

Na magnetnih diskih je bilo tedaj prostora za 3,7 milijarde znakov podatkov, ki so bili neprestano dosegljivi obema računalnikoma.

Celotna računalniška baza podatkov je bila dosegljiva preko devetdesetih terminalov, ki so bili v posameznih službah RSNZ, UNZ, Upravi za ljudsko obrambo, Skupščini mesta Ljubljana in stavbi Republiškega izvršnega sveta, krmiljenje in vzdrževanje terminalske mreže pa je potekalo preko računalnika IBM 3031, ki je bil leta 1984 zamenjan z novim računalnikom IBM 4381/M02. Zaradi distribuirane obdelave podatkov so bili nabavljeni še 4 mini računalniki IBM 8100, ki so bili inštalirani na UNZ Ljubljana, Koper, Maribor in Kranj. Posledica širjenja informacijskega sistema na regionalni ravni je bila tudi ustanovitev odsekov oziroma referatov za obdelavo in analitiko v UNZ.

Leta 1981 je bil sprejet tudi dogovor med RSNZ, Zavodom za statistiko in občinskimi upravnimi organi za notranje zadeve o izgradnji informacijskega sistema upravnih notranjih zadev. Nato so se začele priprave za prenos občinskih registrov prebivalstva v centralno vodeni register prebivalstva na računalnik ISONZ.

### **Pomembnejši dogodki v tem obdobju:**

- 1978:** - vzpostavljena prva banka podatkov, v kateri so bile povezane različne datoteke, kot so register motornih vozil, imetniki orožnih listov, MOS, register prebivalstva Ljubljane, evidenca oseb na prestajanju zaporne kazni ipd.
- dne 1. 1. 1978 začne računalnik ISONZ delovati neprekinjeno
- začetek uporabe programskega orodja SPM-II in CICS/VS ter STAIRS, ki omogoča iskanje podatkov v besedilih
- izdano Navodilo o zaščiti ISONZ





- 1979:** - ustanovljena Uprava za analitiko in informatiko
- 1979:** - RSNZ nabavi švicarske naprave za zaščito prenosa podatkov Gretacoder515
  - prenos osnovnih podatkov iz kazenske evidence na računalnik
  - nabava novega duplex računalnika IBM3031
- 1980:** - ustanovljena Uprava za informatiko
  - vzpostavljena neposredna računalniška povezava med RSNZ Slovenije in Hrvaške
- 1981:** - terminalsko mrežo vzdržujejo 4 (mini) računalniki IBM 8100
- 1982:** - začetek računalniškega preverjanja potnikov na letališču Brnik
  - zamenjan operacijski sistem DOS/VSE z zmogljivejšim MVS
  - RSNZ sprejme Pravilnik o določanju tajnih podatkov, o uporabi in čuvanju teh podatkov ter o načinu njihovega varovanja v ONZ
- 1983:** - Družbeni dogovor o enotnem informacijskem sistemu na področju notranjih zadev
- 1984:** - nabava novega računalnika IBM 4381/M02 z 8MB centralnega pomnilnika

## RAZVOJ MODERNE POLICIJSKE INFORMATIKE IN DELITEV NA UPRAVNI IN POLICIJSKI DEL UPORABNIKOV TER UVAJANJE OSEBNIH RAČUNALNIKOV

### 1985-1990

To obdobje opredeljujeta razvoj moderne policijske informatike ter uveljavljanje družbenega dogovora o enotnem informacijskem sistemu notranjih zadev. Informacijske storitve so bile zagotovljene tudi občinskim upravnim organom za notranje zadeve<sup>8</sup> ter organom pregona in sojenja.

Tako so upravni organi začeli neposredno vnašati podatke o osebnih izkaznicah, postopoma pa so se vključevale v informacijski sistem upravnih notranjih zadev tudi pooblaščen organizacije za opravljanje tehničnih pregledov in registracijo motornih vozil. Tako so bile lahko vzpostavljene številne evidence s področja upravnih notranjih zadev (evidenca osebnih izkaznic, potnih listin, orožja, državljanstva Republike Slovenije) ter možnosti za računalniške izpise dokumentov s področja prometa v občinskih upravnih organih<sup>9</sup>.

Vsebinsko se je informacijski sistem vse bolj delil na upravni in policijski del uporabnikov. Za to obdobje so značilni osebni računalniki<sup>10</sup>, ki so bili jedra mikroračunalniških delovnih postaj, delo na številnih projektih, kot so računalniška obdelava besedil, razvijanje postopkov za identifikacijo oseb, hranjenje in razpošiljanje originalnih dokumentov in slik, modernizacija pisarniškega poslovanja, razvoj relacijskih baz. ISONZ se vse bolj odpira in delovno povezuje tudi z zunanjimi institucijami ter z njihovo pomočjo razvija določene projekte. V tem obdobju je prišlo tudi do prvih resnejših nesoglasij med uporabniki ISONZ (zahteve po opremljanju z

8 Do konca leta 1990 je bilo v ISONZ vključenih že 43 občinskih upravnih organov za notranje zadeve.

9 To je omogočil programski paket FORM, ki je bil za upravne notranje zadeve nabavljen leta 1987.

10 Na osebnih računalnikih se je po letu 1987 začel uporabljati urejevalnik besedil Displaywrite 3, kasneje 4, na centralnem računalniku pa se je uporabljal program STAIRS.



osebni računalniki, njihova nepovezanost v ISONZ, ustvarjanje lastnih baz ipd.), posledica pa je bila preoblikovanje komisije ISONZ in podkomisij. Pri Upravi za informatiko se ustanovita tudi informacijski center in lastna tehnična služba, začne se tudi izgradnja lokalnih računalniških mrež. Uvedeni so številni dodatni ukrepi zaščite proti okužbi z računalniškim virusom.

### Pomembnejši dogodki v tem obdobju:

- 1985:** - uvedba programiranega identifikacijskega in avtorizacijskega mehanizma – SIGN
- začetek uporabe programa za statistične obdelave in analize podatkov – SAS
- uveljavljanje operacijskega sistema MVS in relacijske baze podatkov DB2
- 1986:** - obratovati začne testna neposredna povezava računalnikov RSNZ in Zavoda za statistiko (vzdrževanje registra stalnega prebivalstva ...)
- vzpostavljena prva lokalna baza na regionalnem računalniku
- vzpostavljena računalniška evidenca ukradenih in najdenih predmetov, evidenca samomorov, evidenca kaznivih dejanj ...
- terminalsko omrežje vzdržuje nov računalnik IBM 3275, centralni računalnik IBM 3130 pa zamenja nov računalnik IBM 4381/Q14
- 1987:** - vključevanje pooblaščenih organizacij za tehnične preglede v ISONZ
- začetek uporabe urejevalnika besedil DW4
- vzpostavljena evidenca nevarnih snovi
- 1988:** - občine neposredno vnašajo podatke o osebnih izkaznicah v centralni register izkaznic ter potnih listinah
- izdano navodilo o ščitenju in varovanju podatkov na MRDP
- 1989:** - pojav virusa na osebni računalnik v ISONZ
- vzpostavljena evidenca ukrepov prepoved vožnje z motornim vozilom in odvzem vozniškega dovoljenja
- 1990:** - prvič uporabljena elektronska pošta z integrirano kriptografsko zaščito med RSNZ in UNZ
- vzpostavljena evidenca o orožju
- vzpostavljen računalniško voden opomnik za delo stalnega dežurnega

## SAMOSTOJNA SLOVENIJA

### VKLJUČEVANJE MODERNE POLICIJSKE INFORMATIKE V SVETOVNI INFORMACIJSKI SISTEM

#### 1991-1997

Za prvi del obdobja je značilno uveljavljanje samostojne slovenske države in vojaški spopad z JLA. Temu je Uprava za informatiko sledila z ustreznim varstvom in zavarovanjem podatkov, z lastno avtonomno kriptografsko zaščito pri prenosu podatkov, s sistemom elektronske pošte in s pripravo ustreznih predpisov o varovanju podatkov. Vsi ukrepi so bili ustrezna podlaga za popolnoma varen prenos podatkov v vojnem času, ki so onemogočali vdor v ISONZ. Ustanovljen je bil tudi Center za varovanje podatkov. Drugi del obdobja pa sta zaznamovala izgradnja moderne policijske informatike in vključevanje informacijskega sistema MNZ v nadnacionalne informacijske sisteme. Nacionalni biro Interpola Slovenije se je z elektronsko pošto povezal z Generalnim sekretariatom Interpola v Lyonu. Potekala je izgradnja omrežnega računalništva, interneta in

intraneta, sistema za podporo odločanju, za izmenjavo podatkov in dokumentov neposredno v elektronski obliki. Končnemu uporabniku se je policijska informatika približevala tako z elektronsko pošto kot z uporabniškimi rešitvami.

Integriran policijski informacijski sistem, ki temelji na transakcijah s centralnimi bazami podatkov, ima jedro v fonetičnem indeksu oseb – FIO (nadomestil je stari aplikaciji CEK in CAE), katerega razvoj se je začel leta 1992 in obsega »servis osebe« ter vseh z njo povezanih predmetov in pojmov.

Njegov razvoj je temeljil na lastnem znanju in uporabi sodobne informacijsko-telekomunikacijske opreme<sup>11</sup>. Izgrajujejo se tudi geografski informacijski sistem (GIS) ter sistemi za podporo odločanja, ki se v svojih rešitvah vse bolj približujejo končnemu uporabniku. Najpomembnejši med njimi je vsekakor informacijski sistem policijske postaje - ISPP, ki se razširi tudi na področje prometa, javnega reda in miru ter mejnih zadev in omogoča ustrezno operativno spremljanje varnostne problematike ter izdelavo ustreznih analiz.

Na področju upravnih zadev so bile dopolnjene evidence o državljanstvu, potnih listinah, društvih, registraciji motornih vozil, izdaji lastniških certifikatov ipd. Vse bolj postajajo pomembna lokalna računalniška ter internetna oziroma kasneje intranetna omrežja, ki temeljijo na odnosu strežnik – spletni odjemalec. V tem obdobju se reorganizira Uprava za informatiko in preimenuje v Upravo za informatiko in telekomunikacije, informacijski sistem se s telekomunikacijskim sistemom združi v enotni ITSONZ. Temu ustrezno se oblikuje tudi nova komisija za ITSONZ, ki so jo sestavljale tri podkomisije (za javno varnost, upravne notranje zadeve in sistem državne uprave ter podkomisija za logistični sistem MNZ). V Upravi za upravno-pravne zadeve MNZ pa se ustanovi Oddelek za upravno informatiko in analitiko, ki postopoma prevzema razvijanje in upravljanje informacijskega sistema upravnih notranjih zadev.

V MNZ je bil leta 1997 nabavljen nov računalnik IBM 9672-RB s CMOS tehnologijo, ki je bil kar 2,6-krat zmogljivejši od predhodnika z oznako 9121-511, ki je bil zasnovan še na ECL tranzistorski tehnologiji. Z njim je bilo razrešeno nevzdržno stanje, ki je vladalo v tem obdobju. Računalnik je bil med delovnim časom zaseden že več kot 90 % samo z on-line transakcijami, tako da so se morala razvojna dela in druge naloge opravljati zvečer in ponoči. Najbolj pa so posledice take obremenitve občutili uporabniki, saj v delovnem času ni bilo možno izvajati skoraj nobenih paketnih obdelav. Novi model 9672-RB5 pete generacije tehnologije CMOS (edini te vrste v Sloveniji) je imel dve procesni enoti in zmogljivosti 85 milijonov inštrukcij na sekundo, več novih kanalov (ESCON) za priključevanje zunanjih enot (komunikacijskih, tračnih, diskovnih enot, tiskalnikov ...). Na novi računalnik je bilo priključenih preko 3.500 terminalov. Zamenjan je bil tudi operacijski sistem MVS/ESA z OS/390, ki je omogočil nadaljnji razvoj informacijskega sistema (strežniške funkcije – za Lotus Domino; podpora omrežnega računalništva – aplikacije preko intraneta in interneta, tehnologija JAVA; odprt sistem, ki je omogočal delovanje aplikacij, napisanih za UNIX okolje ter Windows/NT; rešitev problema dvomestnih letnic s prehodom v novo tisočletje ipd.).

---

11 FIO je bil izdelan po načelu kooperativnega procesiranja, ki je kombiniral prednosti centralnega zbiranja podatkov s fleksibilnostjo obdelav v lokalnem okolju. Slednje so bile zagotovljene z rešitvijo, imenovano ISPP. S FIO sta bila uvedena relacijska baza podatkov DB2 in programsko okolje (Cross System Product) CSP (enako Bračko, 2002).



## Pomembnejši dogodki v tem obdobju:

- 1991:**
- med osamosvojitveno vojno je potekal prenos podatkov z lastno kriptografsko zaščito
  - projekt »ODMEV« je razširil krog uporabnikov elektronske pošte
  - nabava novega centralnega računalnika IBM 9112/320
  - širjenje kroga uporabnikov elektronske pošte
  - vzpostavitev fonetičnega indeksa oseb (FIO)
  - razvoj geografskega informacijskega sistema (GIS)
  - terminal MOBIDATA, ki preko radijske mreže omogoča neposreden dostop do podatkov v centralnih bazah
  - uporaba CASE orodja ADW za razvoj aplikacij
  - ustanovitev Uprave za informatiko in telekomunikacije ter preimenovanje ISONZ v ITSONZ
- 1992:**
- narejen katalog zbirk osebnih podatkov
  - računalniški izpis slovenskega potnega lista
  - izpis potrdil o državljanstvu
  - računalniški izpis slovenskega potnega lista
  - projekt nova kazenska ovadba
  - zasnova projekta ISPP
- 1993:**
- vzpostavljena elektronska pošta z Interpolom
  - upravljanje z operacijskim sistemom MVS/ESA ter uvedba orodij NETVIEW in CICS/ESA
  - uveljavitev Pravilnika o določanju zaupnih podatkov in varovanju zaupnih in osebnih podatkov
  - centralni računalnik IBM ES 9000 upravlja operacijski sistem MVS/ESA
  - projekt izdaje in uporabe lastniških certifikatov
- 1994:**
- vzpostavljeni lokalni register stalnega prebivalstva
  - priprava nove osebne izkaznice
- 1995:**
- zaključen projekt ISPP-PROM ter ISPP-JRM
  - vključitev v internet
  - nova digitalna telefonska centrala
  - izide prva številka internega glasila Pregledi
  - izide prvi Statistični letopis ONZ
  - vzpostavljena evidenca o društvih
- 1996:**
- prehod na kodo Latin 2
- 1997:**
- nov centralni računalnik CMOS tehnologije – IBM 9672-RB5
  - zaključen projekt ISPP - MEJA
  - zaključek informatizacije matičnih knjig
  - program FORM se razširi na izpis dokumentov prijavnno-odjavne službe, osebnih stanj, potnih listin in vizumov, prometa ipd.

## ČAS SPREMEMB IN VIZIJA MODERNE INFORMATIKE LOČITEV INFORMACIJSKO TELEKOMUNIKACIJSKIH SISTEMOV POLICIJE OD MNZ IN VKLJUČEVANJE V SCHENGENSKI INFORMACIJSKI SISTEM 1998-2007

Po uveljavitvi novega Zakona o policiji obdobje zaznamuje dokončna ločitev ITSP od MNZ.

Informacijski sistem policije se povezuje z drugimi informacijskimi sistemi, kar omogoča hitrejši pretok in izmenjavo podatkov: elektronska prijava - Gestor, izmenjava zapisov o prometnih nesrečah s Slovenskim zavarovalnim združenjem, izterjava denarnih kazni z DURS itd.. Z elektronsko prijavo kaznivega dejanja je bila vzpostavljena tudi prva spletna storitev za državljane.

Nadaljujejo se: izgradnja modernega policijskega informacijsko-telekomunikacijskega sistema in njegova dokončna prilagoditev in vključitev v SIS, avtomatizacija izmenjave podatkov z Europolovim informacijskim sistemom, povezava s sistemom Eurodac, vključitev v omrežje za elektronsko izmenjavo podatkov o pravih in ponarejenih identifikacijskih dokumentih (FADO), informatizacija podatkov v okviru Prümske pogodbe ter zagotavljanje kakovostne informacijsko-telekomunikacijske podpore policijskemu delu na vseh ravneh delovanja.



Za operativne in analitične službe so vzpostavljene številne vnaprej pripravljene paketne aplikacije, ki omogočajo statistične obdelave in poročila in podatke za podporo odločanja. Vzpostavljen je bil tudi rezervni računalniški sistem ter novi ISPP. Nova elektronska pošta pa je nadomestila za starelo EPONZ.

Tehnološki razvoj informacijsko-telekomunikacijske opreme je zahteval dograditev oz. posodobitev digitalnega prenosnega omrežja do vseh policijskih postaj, postopno uvajanje video-

konferenčnih prenosov, digitalizacijo radijskega omrežja ter uvajanje GPS AVL sistema. Nova telefonska centrala omogoča t. i. »internet protokol« (IP) telefonijo in razvoj novih integriranih informacijsko-telekomunikacijskih storitev. Zagotovljena je bila tudi ustrezna raven tehničnega varovanja objektov (popolna digitalizacija videonadzornih sistemov), zaščite podatkov ter informacijske in telekomunikacijske infrastrukture Policije. Obdobje zaznamuje tudi predstavitev Policije preko spletnih strani ter intraneta in zagotovitev dostopa do informacij javnega značaja.



Potrebno je izpostaviti tudi obdobje pred letom 2000, ko so se v UIT ukvarjali s problematiko letnice 2000 in prilagoditvijo informacijsko-telekomunikacijskega sistema ministrstva po tem obdobju. V ta namen je bila 1. 2. 1999 ustanovljena tudi delovna skupina<sup>12</sup>, ki je nalogo uspešno končala že 30. 11. 1999. Samo delovanje informacijskega sistema upravnih notranjih zadev so delavci UIT uspešno preizkusili že 18. 9. 1999, policijski informacijski sistem pa je bil za delovanje po letu 2000 prilagojen z začetkom produkcijske uporabe KRIM II dne 13. 11. 1999, medtem ko je bila nadgradnja omrežnega operacijskega sistema končana sredi decembra 1999.

### Pomembnejši dogodki v tem obdobju:

**1999:** - prehod na operacijski sistem OS/390

**2000:** - nadgradnja računalnika na IBM System 390 model R26  
- ločitev informacijsko-telekomunikacijskih sistemov policije od MNZ

**2003:** - nakup računalnika IBM eServer zSeries 900 model 102 (bakrena vezje)  
- nakup diskovnega sistema IBM Enterprise Storage System 105-800  
- prehod na operacijski sistem z/OS

**2004:** - nadgradnja avtomatske tračne knjižnice Magstar 3494 na model 3592

**2005:** - začetek uporabe programskega jezika Java in aplikacijskega vmesnika WebSphere

**2006:** - nakup računalnika IBM System z9 Business Class model R04 z dodatnim zAAP procesorjem

**2007:** - vzpostavitev rezervne lokacije z računalnikom IBM eServer zSeries 890 model 220 z možnostjo začasne uporabe dodatnega procesorja (CBU)  
- diskovni sistem IBM Enterprise Storage System 105-800  
- avtomatska tračna knjižnica Magstar 3494, model 3592  
- GDPS/XRC povezava med računalniškima sistemoma  
- zamenjava aplikacije ISPP z novo, centralizirano aplikacijo  
- integracija informacijskega sistema slovenske Policije s SIS I. generacije (SISone4ALL)

**2002-2007:** - zamenjava elektronske pošte DISOSS z elektronsko pošto Lotus Notes

**2006-2007:** - vzpostavitev podatkovnega skladišča

---

<sup>12</sup> V akciji Milenium so, kot piše Bračko, sodelovali posamezni ključni delavci UIT, ki so nekatere vitalne informacijsko-telekomunikacijske sisteme dodatno preizkusili še 1. in 2. januarja 2000. Določeno število zaposlenih pa je bilo z odločbami pripravljenih na domu od 31. 12. 1999 do 7. 1. 2000 oziroma razporejenih na delo v štabu akcije Milenium. Informacijsko-telekomunikacijski sistem ministrstva je na prehodu v leto 2000 normalno deloval, s tem je bila delovna naloga delovne skupine tudi uspešno končana. V tem obdobju je bil testiran tudi datum 29. 2. 2000, ker je bilo leto 2000 prestopno.





### III. RAZVOJ TELEKOMUNIKACIJSKEGA SISTEMA

Prvi zametki žičnih in radijskih zvez takratnih organov za notranje zadeve (ONZ) segajo v prva leta po drugi svetovni vojni. Njihova dejavnost je bila zagotavljanje zvez za potrebe varnostnih organov in je slonela na zastareli tehniki nemškega izvora. Uporabljale so se ročne telegrafske centrale s teleprinterji. Za to obdobje je bilo značilno, da so se sporočila oziroma depeše prenašale po teleprinterju ali telefonu, zelo zaupne depeše pa s kurirsko pošto.

Pred dograditvijo teleprinterkega omrežja sredi 60-ih let so ONZ komunicirali z odprtimi in šifriranimi depešami preko kratkovalovnih sprejemnikov v policijskih enotah. Ta radijski sistem se je kasneje v 70-ih letih moderniziral in je postal predvsem rezervni sistem za zagotavljanje zvez ob prekinitvah žičnih povezav oziroma ob izrednih in drugih razmerah. Ob osamosvojitvi je bil kratkovalovni sistem opuščen. Poleg lastnega telekomunikacijskega omrežja so ONZ uporabljali še javne PTT komunikacijske sisteme, telegrafsko in telefonsko omrežje.

Mobilne brezžične zveze so sprva imele samo prometne patrolje, kasneje pa tudi druge enote. Temu razvoju je sledila tudi izgradnja repetitorjev, ki so pokrili večino ozemlja Slovenije.

Za upravljanje radijske mreže smo do nedavnega uporabljali sistem COMPAD, ki je z novim načinom komuniciranja postal vse manj uporaben. Zato je bil zasnovan nadzorni sistem, imenovan RAKOS (Radijski komunikacijski sistem), s katerim operater OKC komuniciranje nadzoruje z enega mesta.

Tudi žične zveze (telefoni, teleprinterji, telefaksi, sistem za komutacije in povezave, oprema za tehnično varovanje) so zaradi tehnološkega razvoja doživele korenite spremembe. Sedanja dejavnost sledi razvoju digitalizacije. V zadnjem desetletju je bil poudarek na uvajanju sodobnih digitalnih radijskih sistemov (TETRA) in povečevanju zmogljivosti integriranega omrežja ITSP za vključitev v SIS. Izvedeni sta bili prenova in konsolidacija hrbtničnega omrežja ITSP, adaptirani ali postavljeni so bili antenski stolpi na gorskih objektih, postavljeni novi stacionarni in pomorski radarski sistemi, stacionarni sprejemniki, sistemi za prenos in sprejem helikopterske slike ter posodobljeni sistemi za snemanje govornih komunikacij.



Postopno je govorne storitve fiksne telefonije nadomestila tehnologija internetnega protokola (IP), izvedena je bila nadgradnja lokalnih omrežij in navideznih zasebnih omrežij (VPN), ki omogočajo uvedbo novih informacijskih aplikacij in storitev. Na mejnih prehodih sta bili implementirani telekomunikacijska in tehnična oprema, v lokalno govorno telekomunikacijsko omrežje Policije se je vključevala digitalna oprema. Posodobljen je bil sistem klicev na številko 113 v OKC in modernizirani so bili videonadzorni sistemi na športnih prireditvah in v policijskih akcijah, policijski objekti pa so bili postopno opremljeni s sistemi tehničnega varovanja.



## IV. RAZVOJ KRIPTOZAŠČITE



Organizacija in razvoj kriptozasčite v organih za notranje zadeve sicer sega v obdobje druge svetovne vojne, toda pravi razvoj sodobne kriptozasčite se začne v 70. letih. Tedaj se področje kriptozasčite organizira v Oddelku za zveze in kriptozasčito pri Upravi skupnih služb, sestavljali pa so ga: šifroteleprinterski center v RSNZ, šifrerski podcentri v UNZ in šifrerske postaje na tedanjih postajah milice. Z reorganizacijo RSNZ (1991) je kriptozasčita postala naloga Centra za zaščito podatkov v Upravi za informatiko in telekomunikacije.

Pred osamosvojitvijo sta bila kriptozasčita in protielektronsko zavarovanje podatkov pravno urejena s tedanjo jugoslovansko zakonodajo, zato je bila ena izmed prvih nalog Centra za zaščito podatkov (ustanovljen 1991) pripraviti nove predpise o izvajanju omenjenih postopkov v organih za notranje zadeve. Poleg tega je Center za zaščito podatkov pripravil alternativne in avtonomne sisteme za varno komuniciranje z zaupnimi podatki z uporabo domačega algoritma ter ustrezno zamenjal šifrirne ključe. Rezultat teh prizadevanj je bila vzpostavitev varne komunikacije, t. i. elektronska pošta »SEJA«, ki je med vojno za Slovenijo omogočila varen prenos podatkov. Po osamosvojitvi je Center za zaščito podatkov nadaljeval z razvojem kriptozasčite ter pripravil celostno rešitev za varne dostope do podatkov v okviru ITSP.



## V. RAZVOJ VARSTVA IN ZAVAROVANJE (osebnih) PODATKOV

V obdobju mehanografske oziroma strojne obdelave podatkov se je zavarovanje podatkov in opreme osredotočilo v glavnem na tehnično in fizično varovanje prostorov. Namen teh ukrepov je bilo preprečevanje nepooblaščenim osebam dostop do strojne opreme ter podatkov, shranjenih v kartotekah in na drugih nosilcih podatkov (luknjanih karticah). Zaščita je bila usmerjena predvsem v preprečevanje morebitnega nepooblaščenega odtujevanja, kraje, ponarejanja ali poškodovanja podatkov. Sistemsko zavarovanje podatkov se je začelo v sedemdesetih letih, ko je bil v RSNZ pripravljen interni pravilnik o zaščiti podatkov v ERC (leta 1977), naslednje leto pa je v SDV nastalo prvo navodilo o zaščiti ISONZ. Za tehnično zaščito prenosa podatkov pa so se tedaj uporabljale švicarske naprave Gretacoder 515.

Z razvojem terminalske obdelave podatkov so se v tedanji informatiki že zavedali nujnosti celovitega zavarovanja podatkov (identifikacija ter avtorizacija uporabnikov, evidentiranje dostopa do podatkov, zaznave nepooblaščenega vstopa v računalniški sistem ipd.). Leta 1985 je UI pripravila sistemsko programsko zaščito, nekoliko kasneje pa še Navodilo o ščitenju in varovanju podatkov na mikroračunalniških delovnih postajah ISONZ. V tem obdobju se je z zaščito podatkov ukvarjala tudi Komisija ISONZ, ki je svoje strokovnjake pošiljala na različna izpopolnjevanja ter tematske posvete. Tedaj se pojavijo tudi prvi informacijski varnostni »škandali«, povezani z novo nastajajočim računalniškim kriminalom; ti dogodki pospešijo razmišljanja informatikov o varovanju informacijsko-telekomunikacijskih sistemov.

O zaščiti podatkov so tedaj obstajali le redki predpisi, ki so v manjšem obsegu urejali tedanjo avtomatsko (elektronsko) obdelavo podatkov (Zakon o ljudski obrambi, Uredba o merilih, po katerih se določa za LO pomembni podatki, Zakon o temeljnih sistema zvez), pa še ti so se nanašali zgolj na varovanje in ščitenje podatkov, ki so bili označeni s stopnjo tajnosti. Leta 1982 RSNZ izda Pravilnik o določanju tajnih podatkov, o uporabi in čuvanju teh podatkov ter o načinu njihovega varovanja, 1989 pa je bil v ISONZ evidentiran prvi pojav računalniškega virusa. Komisija ISONZ je temu problemu posvetila posebno pozornost ter sprejela vrsto ukrepov za preprečevanje vnosov in razširjanje računalniških virusov.

Devetdeseta leta so bila namenjena predvsem zaščiti »informacijske zasebnosti posameznika« v skladu z 38. členom Ustave RS<sup>13</sup> in na njegovi podlagi sprejetega Zakona o varstvu osebnih podatkov<sup>14</sup>.

Neposredno pred osamosvojitvijo so delavci UIT sodelovali pri pripravi Zakona o varstvu osebnih podatkov, leta 1992 pa je UIT pripravila in izdala prvi Katalog zbirk osebnih podatkov ministrstva za notranje zadeve. Center za zaščito podatkov je pripravil vrsto pravnih aktov, med njimi tudi: Pravilnik o določanju zaupnih

13 Določbe navedenega člena Ustave RS zagotavljajo varstvo osebnih podatkov, prepovedujejo uporabo osebnih podatkov v nasprotju z namenom njihovega zbiranja ter vsakomur zagotavljajo pravico do seznanitve z zbranimi podatki, ki se nanašajo nanj, in pravico do sodnega varstva ob njihovi zlorabi.

14 Zakon o varstvu osebnih podatkov, Ur. list RS, št. 8/90



podatkov in o varovanju zaupnih in osebnih podatkov, Pravilnik o merilih in postopkih za določanje zaupnih podatkov Policije, Pravilnik o varovanju podatkov Policije (spremenjen 2008), Pravilnik o hrabi komunikacijskih podatkov Policije in o dostopu do policijskih baz podatkov, Pravilnik o načinu vodenja policijskih evidenc ter Strokovno navodilo o uporabi videonadzornih sistemov pri varovanju policijskih objektov. S povezovanjem Slovenje z EU je varstvo osebnih podatkov postalo še bolj pomembno. Schengenska konvencija tako poleg določenih zbirk osebnih podatkov med drugim ureja tudi varstvo zasebnosti in zavarovanje osebnih podatkov<sup>15</sup>. Ne glede na navedene slovenske pravne akte in tudi pravne akte Sveta Evrope in EU o varstvu osebnih podatkov pa ne smemo pozabiti še določb Zakona o policiji. Ta v IV. poglavju ureja »Zbiranje, varstvo in zavarovanje podatkov«, s tem pa postavlja temeljne pogoje za ureditev zbirk osebnih podatkov Policije in obdelovanje osebnih podatkov v Policiji ter nadaljuje pravno ureditev zbirk (evidenc) osebnih podatkov, ki jih je začrtal že Zakon o evidencah javne varnosti.

Med pripravami na vstop Slovenije v NATO in EU se izpostavijo zahteve po ureditvi tega področja oziroma vzpostavitvi enotnega sistema obravnavanja in varovanja tajnih podatkov. Tako na osnovi zahtev omenjenih »integracij« in tudi na osnovi prizadevanj Centra za zaščito podatkov nastane prvi slovenski Zakon o tajnih podatkih<sup>16</sup>, ki je temelj tedaj še bodoče celovite pravne ureditve obravnavanja in varovanja tajnih podatkov. Na osnovi tega zakona je nato sprejeta vrsta podzakonskih predpisov, uredb in pravilnikov, katerih sprejem se zaokroži s sprejemom Uredbe o varovanju tajnih podatkov v komunikacijsko- informacijskih sistemih (2007).

Na podlagi Zakona o tajnih podatkih je Center za zaščito podatkov izvedel vrsto aktivnosti, med drugim: pripravo predpisov (pravilnik, navodila), vzpostavitev sistema varnostnega preverjanja posameznikov in izdaje dovoljenj organizacijam za obravnavo tajnih podatkov; vzpostavitev različnih informacijskih, logično-tehničnih in organizacijskih rešitev za varno obravnavanje in varovanje tajnih podatkov. Poleg tega je bil vzpostavljen sistem usposabljanja za področje tajnih podatkov, vzpostavljena so bila upravna in varnostna območja ...

15 Schengenska konvencija države pogodbenice zavezuje, da v zvezi s svojim nacionalnim delom SIS sprejmejo potrebne ukrepe:

**kontrola dostopa do opreme** - za preprečitev dostopa nepooblaščenim osebam do opreme, ki se uporablja za obdelavo osebnih podatkov;

**nadzor nosilcev podatkov** - preprečitev nepooblaščenega branja, prepisovanja, spreminjanja ali odnašanja nosilcev podatkov;

**nadzor shranjevanja** - preprečitev nepooblaščenega vnašanja podatkov v podatkovne zbirke in nepooblaščenega pregledovanja, spreminjanja ali brisanja shranjenih osebnih podatkov;

**nadzor uporabe** - preprečitev, da bi nepooblaščene osebe prek opreme za prenos podatkov uporabljale sisteme za avtomatsko obdelavo podatkov;

**nadzor dostopa** - zagotovitev, da imajo osebe, pooblaščene za uporabo sistema za avtomatsko obdelavo podatkov, dostop samo do podatkov, ki jih zajema njihovo pooblastilo za dostop;

**nadzor prenosa** - zagotovitev, da se lahko preveri in ugotovi, katerim organom se lahko prek opreme za prenos podatkov pošiljajo osebni podatki;

**nadzor vnosa** - zagotovitev, da se lahko naknadno preveri in ugotovi, kateri osebni podatki so bili vneseni v sisteme za avtomatsko obdelavo podatkov ter kdaj in kdo jih je vnesel;

**nadzor pošiljanja** - preprečitev nepooblaščenega branja, prepisovanja, spreminjanja ali brisanja osebnih podatkov med prenosom osebnih podatkov ali med pošiljanjem nosilcev podatkov, sprejeti morajo biti posebni ukrepi, da se zagotovi varnost podatkov med pošiljanjem službam zunaj ozemlja pogodbenic (Vir: S. konvencija, isto Arko, 2008).

Intenzivni razvoj »policijske« informatike je neločljivo povezan z razvojem t. i. policijskega informacijskega prava. Njegov razvoj na kratko pojasnjujejo že navedeni pravni akti.

Vendar moramo posebej opozoriti tudi na to, da se prav ob jubileju zaščita ITSP še naprej nadgrajuje s tehnološkega in pravnega vidika.

Tako se v sodelovanju z IBM Slovenija in S&T vzpostavlja nov sistem enotne prijave v ITSP (na podlagi »več-funkcijske« pametne kartice, ki omogoča vpeljavo elektronskega certifikata in/ali biometričnih podatkov). V preteklem letu je bil posodobljen sistem za avtorizacijo uporabnikov zbirk osebnih podatkov, v letošnjem letu pa bo nadgrajen sistem spremljanja dela uporabnikov ITSP (»enotni« dnevnik dela). S tem bomo v celoti posodobili celoten sistem AAA.

Dogradili smo tudi sistem varnostne pregrade, ki ITSP povezuje z drugimi informacijskimi sistemi ter vzpostavili dodatni sistem za odkrivanje vdorov v sistem preko interneta. Urejen je bil varen dostop preko prenosnega mobilnega računalniškega terminala, ki komunicira preko javnega mobilnega telefonskega omrežja. Uvedena sta bila avtomatizacija obdelave statističnih podatkov preko internetne varnostne pregrade in filtriranje (preprečevanje) določenega poštnega prometa na priključni točki ITSP na internet. Uvedeno je kriptoščiteno nove elektronske pošte ter internet protokola prenosa podatkov. Za varovanje dostopa do podatkov SISone4ALL je bila nabavljena potrebna oprema, ki omogoča, da sinhronizacija podatkov med C.SIS in N.SIS poteka po posebno kriptoščitnem komunikacijskem omrežju. Zagotovljena je bila tudi ustrezna zaščita rezervnega centralnega računalnika, digitalnega radijskega omrežja TETRA ...

Naj opis aktivnosti za zaščito ITSP končamo z napovedjo skorajšnje vzpostavitve novega „paralelnega“ informacijsko-komunikacijskega sistema, namenjenega obravnavi oz. prenosu nacionalnih tajnih podatkov.



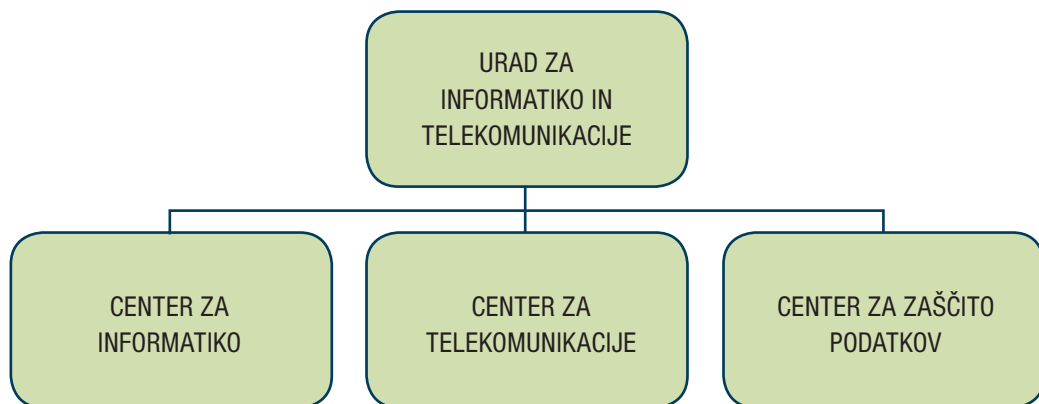




## VI. ORGANIZIRANOST UIT

### Pristojnosti in naloge

Urad za informatiko in telekomunikacije upravlja ITSP, načrtuje informacijsko-telekomunikacijske rešitve in storitve, nabavlja programsko, strojno opremo ter elektronsko opremo in sisteme tehničnega varovanja. Pripravlja strategijo razvoja ITSP, izdeluje in nadzira izvajanje srednjeročnih in letnih načrtov razvoja in sodeluje z MNZ ter drugimi državnimi organi pri povezovanju v informacijske in telekomunikacijske sisteme državne uprave Republike Slovenije in EU. Sprejema tudi standarde, na katerih temelji ITSP, nadzira sodelovanje z zunanjimi strokovnimi in znanstvenimi ustanovami, organizacijami in združenji v zvezi z razvojem ITSP.



## Organiziranost

Organiziranost informatike in telekomunikacij se je z leti izpopolnjevala in spreminjala vzporedno z razvojem informacijsko - telekomunikacijskega sistema in nalog, obenem pa se je spreminjalo tudi ime enote. Sedanja organiziranost omogoča uporabnikom višjo obliko sodelovanja in obvladovanja najsodobnejših informacijsko-telekomunikacijskih storitev. UIT sestavljajo trije centri:

### Center za informatiko

Center za informatiko upravlja, razvija in vzdržuje informacijski sistem Policije. Sestavlja ga šest oddelkov, ki so organizirani za sistemsko in aplikativno podporo ter za informacijsko strojno opremo. Osrednji del informacijskega sistema je centralni strežnik, do katerega ima dostop preko 7.000 uporabnikov. Za dostop uporabljajo osebne računalnike, ki so povezani v lokalna računalniška omrežja, omogočen pa je tudi mobilni dostop. Na centralnem strežniku so policijske podatkovne baze.

Center za informatiko je informatiziral postopke poslovanja tudi z drugimi organizacijami in organi, tudi zunaj državne uprave. Državljanom je omogočil elektronsko poslovanje preko interneta, z vključitvijo v Evropsko unijo pa center razvija mednarodno elektronsko poslovanje in sodelovanje v skupnih informacijskih projektih.

Center za informatiko organizira tečaje za uporabo lastnih aplikacijskih rešitev ter nekaterih standardnih programskih orodij.

### Center za zaščito podatkov

Center pripravlja predloge, predpise, ki se nanašajo na varovanje določenih delovnih mest in tajnih podatkov Policije in organizira, nadzira in izvaja postopke ter ukrepe za varstvo osebnih podatkov, katerih upravljavec je Policija. Pri tem vodi in vzdržuje tudi katalog zbirk podatkov Policije. Pri svojem delu načrtuje, projektira ter izvaja postopke za protiobveščevalno, fizično in kriptološko varovanje ITSP in izvaja protiprislušovalne preglede prostorov oziroma izvaja ukrepe za protiprislušovalno zaščito.



## Center za telekomunikacije

Center za telekomunikacije izvaja smiselno zaokrožene delovne procese na področju telekomunikacij. Poleg osnovnih dejavnosti vzdržuje elektronsko opremo ter opremo za tehnično varovanje in videonadzor. Ukvarja se s projektiranjem, z načrtovanjem, gradnjo in nadziranjem ter vzdrževanjem policijskih analognih in digitalnih radijskih omrežij, linijskih prenosnih sistemov, komutacijskih sistemov, sistemov za medomrežne povezave in drugih. Sodeluje pri standardizaciji, tipizaciji in sistemizaciji telekomunikacijske, elektronske in druge opreme ter jo preizkuša.



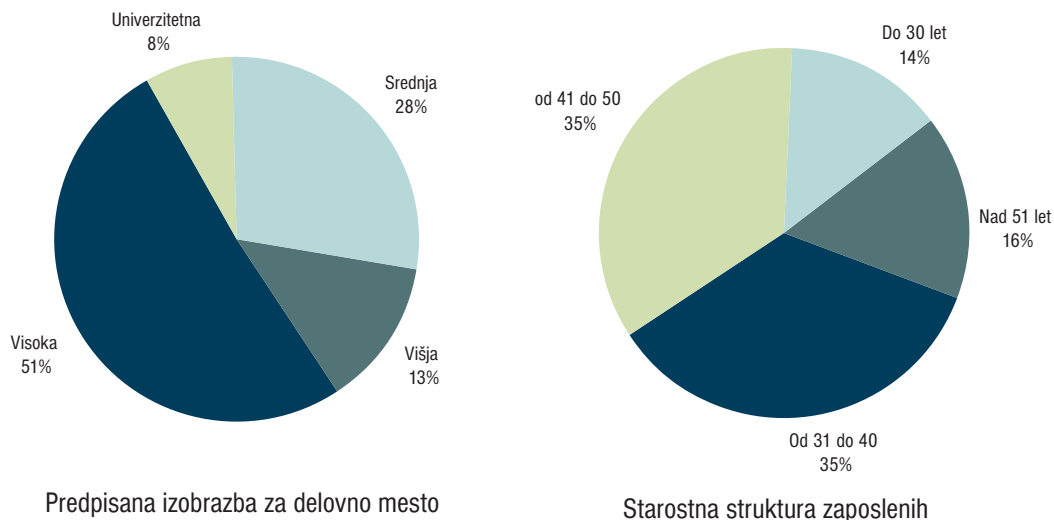


110100001101010110111010100

## VII. ZAPOSLENI V UIT

Ob zaključku leta 2007 je bilo v UIT 159 zaposlenih. Zahtevnejša tehnologija dela vpliva na zaposlovanje ustrezno izobraženega strokovnega kadra v informatiki in telekomunikacijah. Zato se nadaljuje težnja povečevanja deleža zaposlenih z univerzitetno strokovno izobrazbo. Svoje znanje dopolnjujejo v izobraževalnih centrih v Sloveniji in tujini, tako da so seznanjeni z najnovejšimi tehnologijami in sodobnimi metodami dela. V vseh obdobjih razvoja ITSP so zaposleni zagotavljali nemoteno delovanje računalniških in telekomunikacijskih sistemov in stalno spremljali razvoj nove informacijske tehnologije in jo preizkušali doma in v tujini.

Dosedanja politika zaposlovanja, usposabljanja in izobraževanja je delavce UIT vodila k doseganju zelo kakovostnih informacijsko-telekomunikacijskih storitev ter razvojnih usmeritev Policije. Znanje in izkušnje zagotavljajo uspešno delovanje in razvoj urada. Zaposluje pomemben delež kadra z višjo in visoko strokovno izobrazbo, razvija in vzpostavlja vrednote in organizacijsko kulturo, ki krepijo motivacijo, kreativnost in pripadnost službi. Visoka izobrazbena struktura zagotavlja, da urad uspešno deluje na področju informacijske, telekomunikacijske opreme in opreme s področja varstva podatkov, pri usposabljanju in izpopolnjevanju delavcev Policije in prenosu znanja in tehnologije drugim službam v Policiji.



Najpomembnejše IT storitve UIT razvija z lastnimi kadri, kar omogoča maksimalno prilagajanje potrebam Policije ter možnost stalnega prilagajanja, nadgrajevanja in dopolnjevanja rešitev skladno s temi potrebami. Starostna struktura v UIT kaže dokaj uravnoteženo zaposlitev vseh generacij. Tako tistih, ki so informacijski sistem desetletja gradili in izpopolnjevali, kot mlajših, ki šele prihajajo iz fakultet, polni znanja in željni dokazovanja. Nove zaposlitve sicer vplivajo na pomladitev kolektiva, a zahtevajo tudi veliko vlaganja v izobraževanje novih kadrov.

## VIII. USPOSABLJANJE IN IZPOPOLNJEVANJE V UIT

V Uradu za informatiko in telekomunikacije se že vrsto let izvajajo usposabljanja za delavce Policije, ki potekajo po načrtu usposabljanja (katalogu) ter potrebah uporabnikov. Vsako leto se različnih usposabljanj udeleži 2000–3000 zaposlenih. Posebno pozornost vodstvo UIT namenja tudi usposabljanju novih sodelavcev, da se z načrtnim mentorstvom lahko hitreje vključijo v delo. Za navedeno dejavnost oziroma za razvoj zaposlenih je bilo leta 2006 namenjenih preko 12,5 milijona tolarjev ali 78 tisoč tolarjev na zaposlenega. Največ pozornosti je bilo usmerjene v interne tečaje, ki jih izvajajo usposobljeni delavci informatike in telekomunikacij. Večina internih usposabljanj je bila organizirana za uporabo fonetičnega indeksa oseb - FIO, programskih paketov Word, Excel in Power Point, operacijskega sistema Windows 2000, osnov Lotus Notesa, SPIS in nove elektronske pošte, v zadnjem obdobju pa je bilo največ usposabljanj o obravnavi tajnih podatkov in za delo z novim ISPP.

Zaradi uvajanja novih, sodobnejših sistemov in opreme, se je velika pozornost namenjala tudi ustreznemu usposabljanju in izpopolnjevanju tehničnega kadra v UIT in informatikov v oddelkih za informatiko in telekomunikacije na policijskih upravah. Posamezni delavci v UIT namreč potrebujejo visoko raven znanja, ki so ga v preteklosti uspešno predstavljali tudi na različnih seminarjih in konferencah. Vlaganje v usposabljanje zaposlenih v UIT in v seznanjanje in nabavo nove tehnologije (instrumente in merilno opremo) so nujni pogoji za uspešno delo informatikov v vseh obdobjih.

Pregled števila udeležencev v posameznih letih

Vrsta	2001	2002	2003	2004	2005	2006	2007
	Štev. udeležencev	Štev. udeležencev	Štev. udeležencev	Štev. udeležencev	Štev. Udeležencev	Štev. udeležencev	Štev. udeležencev
Interni tečaji	752	1844	1137	2888	3007	1680	3873
Zunanje ustanove	101	81	63	74	105	89	95
Tujina	15	15	20	15	13	12	19
<b>SKUPAJ</b>	<b>868</b>	<b>1940</b>	<b>1220</b>	<b>2977</b>	<b>3125</b>	<b>1781</b>	<b>3987</b>

Velika fluktuacija kadrov, prihod novih delavcev, ki šele osvajajo specifična znanja, mlademu vodstvu povzroča velike težave. Usposabljanju zaposlenih doma in v tujini kljub omejenim finančnim sredstvom namenjajo veliko pozornost. Zaposleni morajo namreč nenehno slediti najnovejšemu razvoju informatike in telekomunikacij v svetu in dognanja ustrezno implementirati v IT okolje Policije. Redni letni razgovori, ki jih izvaja vodstvo z vsemi zaposlenimi, pa so osnova za spodbujanje delovne uspešnosti in načrtovanje osebnega razvoja.



Stroški usposabljanja v posameznih letih (v SIT)

Leto	Stroški usposabljanj pri zunanjih institucijah in v tujini		Stroški internih tečajev	
	SIT	EUR	SIT	EUR
2001	14.127.231,76	58.951,89	2.035.000,00	8.491,90
2002	9.200.000,00	38.390,92	4.600.000,00	19.195,46
2003	9.577.986,00	39.968,23	3.675.000,00	15.335,50
2004	11.543.226,00	48.169,03	1.529.200,00	6.381,24
2005	10.260.401,00	42.815,89	1.436.411,00	5.994,04
2006	10.055.355,00	41.960,25	1.348.970,67	5.629,15
2007	10.531.219,52	43.946,00	2.026.512,07	8.456,48



# IX. SODELOVANJE Z DOMAČIMI IN TUJIMI USTANOVAMI

Sodelovanje z domačimi in s tujimi ustanovami je za slovensko policijsko informatiko ter telekomunikacije nedvomno ena od prioritet. Že od začetka poteka sodelovanje s številnimi slovenskimi podjetji, ki so imela takrat visoke računalniške zmogljivosti, medtem ko ministrstvo zaradi prepovedi uvoza računalniške tehnologije v prvem obdobju ni imelo lastnih računalnikov. Maloštevilni informatiki so opravljali računalniške storitve na sposojenih oziroma najetih računalnikih ter si izmenjevali izkušnje z drugimi informatiki.

Delavci Urada za informatiko in telekomunikacije danes sodelujejo s številnimi organizacijami in organi ter ministrstvi v Sloveniji in Evropski skupnosti oziroma NATU pri načrtovanju, razvijanju in opravljanju skupnih nalogah s področja računalniške in telekomunikacijske tehnologije ter normative dejavnosti. V zadnjem obdobju se je to sodelovanje še posebej razširilo pri razvoju nove generacije SIS. Povezovanje Policije z drugimi organizacijami v zadnjem obdobju obsega:

- **Slovensko zavarovalno združenje:** dnevno pošiljanje zapisnikov o prometnih nesrečah;
- **Zavod za zdravstveno zavarovanje Slovenije:** izmenjava zapisov o prometnih nesrečah;
- **Statistični urad RS:** pošiljanje statističnih podatkov;
- **Davčni urad RS:** izterjave mandatnih kazni;
- **Ministrstvo za pravosodje:** izdelava identifikacijskih izkaznic ter koriščenje radijskih sistemov ONZ;
- **Ministrstvo za zunanje zadeve in CURS:** dostop do schengenskih podatkov;
- **Ministrstvo za znanost in tehnologijo (Urad za standardizacijo in meroslovje):** sprejemanje različnih standardov s področja telekomunikacij in umerjanja elektronske opreme, aktivnosti v zvezi z ustanovitvijo lastnega laboratorija za overjanje merilnikov v Policiji;
- **Ministrstvo za obrambo in SOVA:** načrtovanje koriščenja radijskih frekvenc in skupnih gorskih objektov za potrebe telekomunikacij;
- **RTV (Oddajniki in zveze), Elektro Ljubljana, Telekom Slovenije, Mobitel:** koriščenje gorskih objektov in antenskih sistemov;
- **Agencija za pošto in elektronske komunikacije:** normativno urejanje telekomunikacij in usklajevanje radijskih frekvenc;
- **Ministrstvo za promet in zveze:** medresorska skupina za pripravo Strategije razvoja digitalnih radijskih sistemov državnih organov;

## MEDNARODNO SODELOVANJE

- Europol:
  - EIS projektni odbor in programski odbor za informacijsko-telekomunikacijsko področje (ICT programski odbor), Haag, Nizozemska
  - uporabniško testiranje EIS, Haag, Nizozemska
  - Security Committee, Haag, Nizozemska
- Interpol



- Schengenski informacijski sistem:
  - SISTech-a, Bruselj, Belgija
  - odbori SIS II, Bruselj, Belgija
- FADO:
  - delovne podskupine, Bruselj, Belgija
- EURODAC:
  - EURODAC/DubliNET, Bruselj, Belgija
- PRÜM:
  - Prümska delovna skupina, Bruselj, Belgija
- Trilateralni avstrijsko-italijansko-slovenski center za policijsko sodelovanje:
  - inštalacija programske in telekomunikacijske opreme, mejni prehod Vrata - Megvarje



## X. PUBLICISTIKA

V začetnem obdobju je informatika posamezne službe v ministrstvu oskrbovala s potrebnimi podatki, ki so bili večinoma zaupni, šele kasneje se je začelo občasno objavljanje posameznih statističnih edicij. Publikacije so bile prilagojene takratnim potrebam in so se nanašale predvsem na prikaz kazenskih evidenc ter statističnih serij o kaznivih dejanjih, kršitvah javnega reda in miru ter cestnoprometnih prekrških in nesrečah. Kasneje pa so strokovno usposobljeni delavci urada začeli pripravljati in oblikovati stalne letne statistične biltene, letopise, ter z njimi obveščati tudi zunanjo javnost.



K statističnim podatkom so prilagali tudi obvezne strokovne komentarje ter s tem izboljševali tudi kakovost biltenov in opomnikov.

Urad opravlja tudi osnovne statistične raziskave in oblikuje statistične preglede za letna poročila, ki jih ponuja v uporabo drugim službam v GPU. Publicistična dejavnost vedno sledi razvoju statistične dejavnosti in tudi strokovnim izsledkom na področju

obveščanja in usposabljanja. Svoje delavce in druge službe v Policiji in ministrstvu oskrbuje tudi s številnimi priročniki za uporabo posameznih računalniških programov, strokovnimi navodili za uporabo različnih transakcij, normativnimi akti ter raznimi zbirankami ipd.

Pred leti so v UIT izdajali tudi revijo Pregledi, v kateri so objavljali novosti na področju informatike in telekomunikacij, ter Statistični letopis MNZ in Policije, ki je bil zelo obsežen in je na enem mestu zajemal pregled najpomembnejših statističnih podatkov Policije.

Urad je sodeloval tudi na sejamskih prireditvah INFOS v Cankarjevem domu, kjer se je, poleg propagandnega materiala, predstavljal tudi s tematskimi predavanji. Posamezni strokovnjaki urada so sodelovali na različnih mednarodnih in domačih strokovnih seminarjih in simpozijih, kjer so javnosti predstavljali dosežke na področju informatike in telekomunikacij slovenske policije.

Uporaba spletne tehnologije je zahtevala nov način objavljanja statističnih podatkov. Leta 2000 so delavci UIT prenovili spletne strani Policije in tako omogočili uporabnikom pregleden in hiter dostop do različnih statističnih informacij in podatkov ([www.policija.si](http://www.policija.si)).

# XI. NAJPOMEMBNEJŠE INFORMACIJSKO- TELEKOMUNIKACIJSKE REŠITVE

## Fonetični indeks oseb (FIO)

Fonetični indeks oseb je osrednji in izredno obsežen del ITSP. Predstavlja skupek vseh policijskih, zakonsko predpisanih evidenc, ki se vodijo o vsaki obravnavani osebi (indeks »enotne policijske osebe«). Do podatkov o osebi lahko pridemo tudi s fonetičnim iskanjem (iskanje po podobnostih). Z njim smo nadomestili stari aplikaciji CEK (Centralna kartoteka) in CAE (Centralna abecedna evidenca), ki sta se uporabljali za operativno preverjanje. Vsebinska in tehnološka posodobitev pa je omogočila tudi vključitev FIO v spletno okolje, tako da so se odprle možnosti za vključevanje digitalnih podob (prstni odtisi, fotografije, dokumenti). Hkrati pa je sistem postal osnova za povezovanje znotraj državne uprave in zunaj nje oziroma za tesno integracijo s SIS (SISone4ALL).

## Elektronska pošta Policije (EPP)

Nova Elektronska pošta Policije temelji na posebej prilagojeni aplikaciji sporočilnega sistema Lotus Notes in je zamenjala staro Elektronsko pošto organov za notranje zadeve (EPONZ). Namenjena je izmenjavi uradnih dokumentov med policijskimi enotami. V pošto je implementiran tudi elektronski podpis, ki predstavlja sodobno alternativo klasičnemu podpisu. Elektronski podpis zagotavlja:

- identiteto imetnika digitalnega potrdila,
- originalnost digitalno podpisanega dokumenta (podpisnik ne more zanikati podpisanega sporočila),
- celovitost sporočila (podatkov ni mogoče spremeniti ali popraviti brez vednosti podpisnika).

Elektronska pošta je zasnovana tako, da različnim vrstam uporabnikov omogoča pregledno spremljanje, shranjevanje in prilagajanje ter ustreza novim pravilom poslovanja z dokumentarnim gradivom. To je omrežna aplikacija, ki omogoča delo več uporabnikom v istem predalu na različnih računalnikih. Urad za informatiko in telekomunikacije je pripravil tudi podrobna navodila o digitalnih potrdilih in usposabljanje uporabnikov.

## Internet

Svoje prve spletne strani je MNZ (oziroma Policija) predstavilo že leta 1995 na strežniku Centra vlade za informatiko, ko so bila prikazana številna gradiva ministrstva in delovanje Policije. Že naslednje leto so v UIT oblikovali strani na lastnem strežniku in tako je postalo ministrstvo eden od vodilnih oglaševalcev in ponudnikov informacij med ministrstvi v Sloveniji. Z vzpostavitvijo Policije kot organa v sestavi ministrstva so bile leta 2000 njene spletne strani na novo oblikovane in vzpostavljene. Sedaj so med uporabniki interneta že dobro uveljavljene in prepoznavne, saj jih vsak mesec obiše več tisoč uporabnikov.





Preko novih spletnih strani Policije je javnosti omogočen dostop do vseh podatkov in informacij, pomembnih za čim uspešnejše delo Policije, za izboljšanje njene javne podobe in za razvijanje partnerskih odnosov z vsemi družbenimi subjekti, ki lahko prispevajo k izboljšanju varnostnih razmer. Policijski strežnik je v slovenskem in angleškem jeziku in se obnavlja dnevno ter obsega že več kot 12.000 dokumentov. Predstavlja vstop v virtualni svet Policije. Dnevno je med 2500 do 3000 zadetkov oziroma vstopov. Vsebinsko so spletne strani razdeljene na več delov (Predstavitev, Aktualno, Novo na straneh, Za državljane, Kronika, Prometni zastoji, Sporočila za javnost itd.). Informacije ureja uredniški odbor, ki ga imenuje generalni direktor Policije

## Schengenski informacijski sistem (SIS)

SIS<sup>17</sup> je skupna baza podatkov, ki policistom pri mejni kontroli in postopkih s tujci, delavcem carine in upravnih enot v postopkih z državljani in tujci ter pristojnim pravosodnim organom držav članic in konzularnim predstavništvom ob izdaji vizuma omogoča dostop in pravico do neposredne uporabe podatkov o posameznikih in predmetih. Seznam organov, ki so pooblaščen za dostopi do podatkov, vsebovanih v SIS, določa Schengenska konvencija.

---

17 Območje »schengna« pomeni območje brez mejne kontrole na notranjih mejah. Schengen je izraz za dva mednarodna sporazuma, ki sta bila v kraju Schengen v Luksemburgu podpisana s ciljem, da bi bila med državami podpisnicami odpravljena mejna kontrola na notranjih mejah in s tem zagotovljeno prosto gibanje ljudi. Gre za Sporazum o postopni odpravi kontrol na skupnih mejah, podpisan leta 1985, in za Konvencijo o izvajanju schengenskega sporazuma (imenujemo jo tudi Schengenska konvencija), ki pomeni nadgradnjo in konkretizacijo prvega sporazuma. Oba sporazuma sta bila s posebnim protokolom k Amsterdamski pogodbi, ki je začela veljati 1. maja 1999, vključena v pravni red EU. Da pa odprava notranjih meja ne bi povzročila večje nevarnosti za varnost in javni red v državah članicah, obstaja še vrsta t. i. izravnalnih ukrepov, katerih cilj je boj proti nezakonitemu priseljevanju in trgovini z ljudmi, preprečevanje groženj notranji varnosti, javnemu redu in zdravju ter mednarodnim odnosom držav članic. Ti ukrepi se izvajajo predvsem na zunanjih mejah, pa tudi v notranjosti, s čezmejnimi policijskim sodelovanjem, preko SIS in s harmonizacijo zakonodaje držav članic.

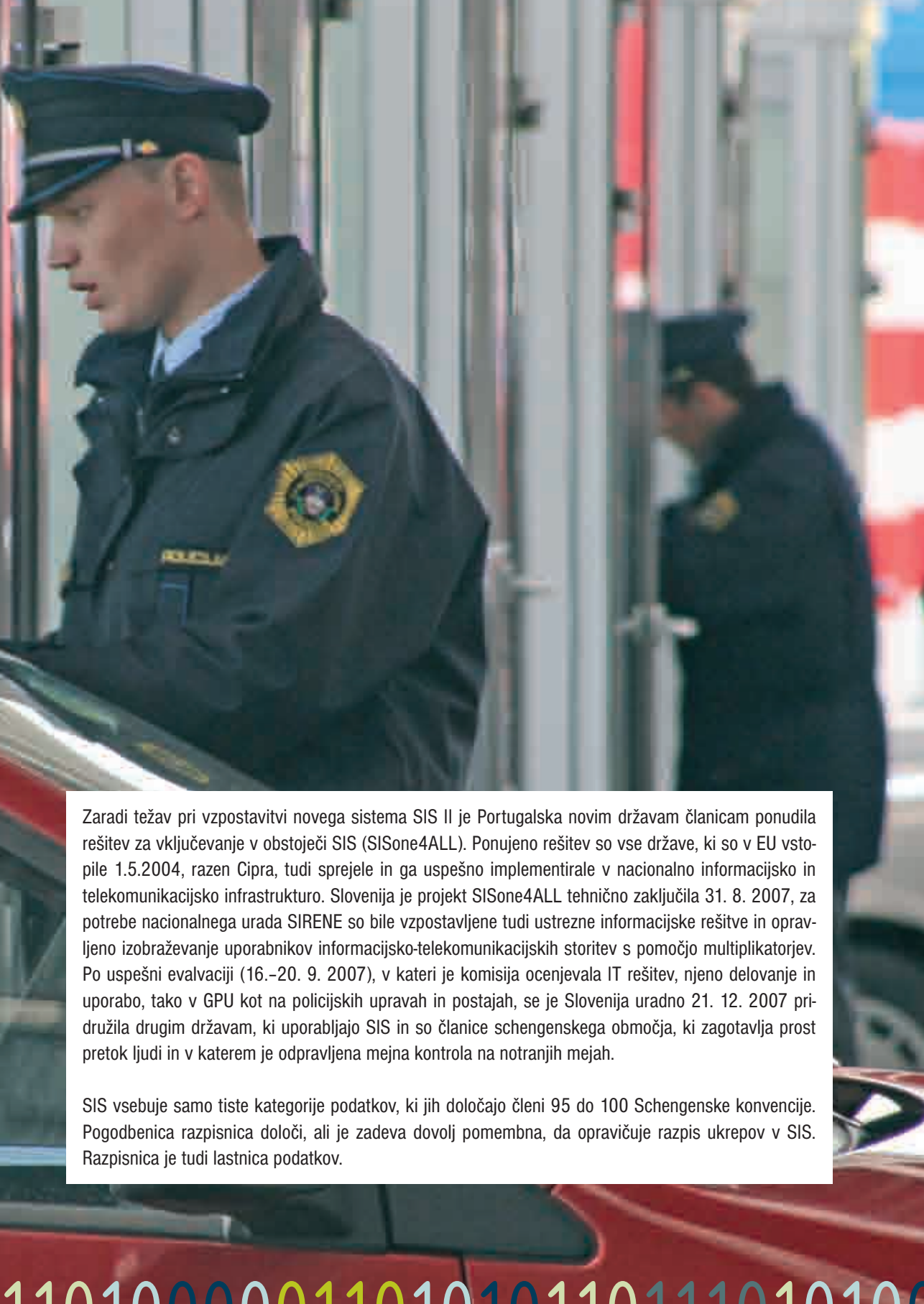
Države v schengenskem območju so Avstrija, Belgija, Danska, Finska, Francija, Grčija, Italija, Luksemburg, Nemčija, Nizozemska, Portugalska, Španija in Švedska ter pridruženi članici EU Islandija in Norveška, države, ki so se vključile 21. 12. 2007: Češka, Estonija, Latvija, Litva, Madžarska, Malta, Poljska, Slovaška in Slovenija. Ciper, Bolgarija in Romunija se na vstop v schengensko območje še pripravljajo.







01010111100010110110110101



Zaradi težav pri vzpostavitvi novega sistema SIS II je Portugalska novim državam članicam ponudila rešitev za vključevanje v obstoječi SIS (SISone4ALL). Ponujeno rešitev so vse države, ki so v EU vstopile 1.5.2004, razen Cipra, tudi sprejele in ga uspešno implementirale v nacionalno informacijsko in telekomunikacijsko infrastrukturo. Slovenija je projekt SISone4ALL tehnično zaključila 31. 8. 2007, za potrebe nacionalnega urada SIRENE so bile vzpostavljene tudi ustrezne informacijske rešitve in opravljeno izobraževanje uporabnikov informacijsko-telekomunikacijskih storitev s pomočjo multiplikatorjev. Po uspešni evalvaciji (16.-20. 9. 2007), v kateri je komisija ocenjevala IT rešitev, njeno delovanje in uporabo, tako v GPU kot na policijskih upravah in postajah, se je Slovenija uradno 21. 12. 2007 pridružila drugim državam, ki uporabljajo SIS in so članice schengenskega območja, ki zagotavlja prost pretok ljudi in v katerem je odpravljena mejna kontrola na notranjih mejah.

SIS vsebuje samo tiste kategorije podatkov, ki jih določajo člani 95 do 100 Schengenske konvencije. Pogodbenica razpisnica določi, ali je zadeva dovolj pomembna, da opravičuje razpis ukrepov v SIS. Razpisnica je tudi lastnica podatkov.

SIS sestavljata dva dela:

- centralni del (C.SIS) v Strasbourgu – vse podatke, ki jih države vnašajo preko svojih nacionalnih sistemov,
- nacionalni sistemi (N.SIS), preko katerih se izvajajo poizvedbe in vnašajo novi razpisi v skupni bazi podatkov.

Za upravljanje in podporo N.SIS v RS je odgovoren Urad za informatiko in telekomunikacije GPU MNZ<sup>18</sup>. Med C.SIS in N.SIS ves čas poteka posodabljanje, sinhronizacija podatkov pa poteka po posebej zaščitenem komunikacijskem omrežju.

SIS vsebuje podatke o osebah, ki jim je prepovedan vstop na schengensko območje in se iščejo zaradi aretacije ali izročitve, o pogrešanih osebah, o ukradenih vozilih in dokumentih, denarju, orožju itn. Po Schengenski konvenciji gre le za podatke o:

- osebah, za katere se zahteva prijetje zaradi predaje ali izročitve (95. člen Schengenske konvencije),
- osebah, ki niso državljani držav članic, za katere je razpisana zavrnitev vstopa v schengensko območje (96. člen),
- pogrešanih osebah ali osebah, ki potrebujejo začasno policijsko zaščito, predvsem mladoletniki (97. člen),
- pričah oziroma osebah, ki se morajo zaradi kazenskega postopka zglasiti na sodišču ali jim je potrebno vročiti sodbo ali vabilo na prestajanje kazni (98. člen) in
- osebah zaradi prikritega evidentiranja ali namenske kontrole (99. člen).

O osebah so lahko navedeni le naslednji podatki:

- priimek in ime, morebiten psevdonim, po potrebi v novem podatkovnem zapisu,
- morebitne fizične posebnosti, ki se ne spreminjajo,
- prva črka drugega imena,
- datum in kraj rojstva,
- spol,
- državljanstvo,
- ali je oseba oborožena,
- ali je oseba nasilna,
- predlagana oblika ukrepanja,
- razlog za razpis ukrepa.

Poleg navedenih osebnih podatkov pa SIS vsebuje tudi podatke o:

- vozilih, za katere se izvaja prikrito evidentiranje ali namenska kontrola (99. člen) in
- predmetih, ki se iščejo zaradi zasega ali za zagotovitev dokazov v kazenskih postopkih (100. člen).

Podatki o osebah veljajo kot osebni podatki in so skrbno varovani. Vsak posameznik ima pravico do vpogleda in seznanitve z lastnimi osebnimi podatki<sup>19</sup>, ki so vneseni v SIS, zahtevo pa lahko vloži v kateri koli schengenski državi, saj so vse nacionalne zbirke enake centralni zbirki v Strasbourg. Zahteva za seznanitev z lastnimi osebnimi podatki se v Sloveniji vloži pisno ali ustno na zapisnik pri Policiji. Vloga za seznanitev z lastnimi osebnimi podatki se lahko vloži tudi na vseh mejnih prehodih, upravnih enotah in diplomatsko-konzularnih predstavništvi Slovenije v tujini, vloga pa se v reševanje takoj posreduje Policiji. Poleg pravice do vpogleda v lastne osebne podatke v SIS, imajo državljani tudi pravico do popravka netočnih lastnih osebnih podatkov in do zahtevka za izbris nezakonito shranjenih lastnih osebnih podatkov v SIS.

Za nadzor tehničnega podpornega dela SIS je glede varstva osebnih podatkov pristojen skupni nadzorni organ. Poleg tega v skladu s Schengensko konvencijo vsaka pogodbenica imenuje nadzorni organ, ki je po nacionalni zakonodaji pristojen za neodvisni nadzor nad podatkovnimi zbirkami nacionalnega dela SIS in za preverjanje, da obdelava in uporaba podatkov, vnesenih v SIS, ne krši pravic oseb, na katere se podatki nanašajo. V Sloveniji je to informacijski pooblaščenec. Oblikovan je tudi skupni nadzorni organ za nadzor tehničnega podpornega dela SIS. Ta organ sestavljata po dva predstavnika vsakega nacionalnega nadzornega organa.

## Nove funkcije SIS

Zaradi povečevanja organiziranega kriminala in predvsem nevarnosti terorizma so bile za SIS predlagane nove funkcije:

- dostop do SIS za organe in podjetja, ki so odgovorni za izdajo prometnih dovoljenj in registrskih tablic za motorna vozila,
- dostop do SIS za Europol in Eurojust,
- vnos ponarejenih potnih listov v SIS in
- vnos biometričnih podatkov v SIS.

Novi SIS II bo tehnično posodobljen sistem in bo vključeval nove kategorije podatkov vključno z relacijami med njimi. Zaživel naj bi konec leta 2009. Omogočal bo razširitev in nove kategorije razpisov (letala, plovila, industrijska oprema, kontejnerji). Omogočal bo direktne povezave razpisov ter zajemal biometrične podatke.

---

19 30. člen Zakona o varstvu osebnih podatkov določa, da mora Policija, organ v sestavi Ministrstva za notranje zadeve, kot upravljavec nacionalnega dela SIS zbirke osebnih podatkov posamezniku na njegovo zahtevo:

- omogočiti vpogled v katalog SIS, potrditi, ali se podatki v zvezi z njim obdelujejo ali ne, in mu omogočiti vpogled v osebne podatke, ki so vsebovani v nacionalni zbirki SIS in se nanašajo nanj, ter njihovo prepisovanje ali kopiranje,
- posredovati izpis osebnih podatkov iz nacionalne zbirke SIS, ki se nanašajo nanj,
- posredovati seznam uporabnikov, ki so jim bili posredovani osebni podatki, kdaj, na kakšni podlagi in s kakšnim namenom,
- posredovati informacijo o virih, na katerih temeljijo zapisi, ki jih o posamezniku vsebuje SIS, in o metodi obdelave,
- posredovati informacije o namenu obdelave in vrsti osebnih podatkov, ki se obdelujejo v SIS, ter vsa potrebna pojasnila v zvezi s tem,
- pojasniti tehnične oziroma logično-tehnične postopke odločanja.

Na neformalnem zasedanju Sveta EU za pravosodje in notranje zadeve na Brdu (24. in 26. 1. 2008) so ministri izpostavili prednostne naloge EU pri vzpostavitvi druge generacije SIS II. Ta bo zagotavljal višje standarde ter uporabo najsodobnejših tehnologij za hitro in učinkovito kontrolo potnikov pri vstopu v Evropsko unijo. Poleg tega bo hitri in nemoteni dostop do podatkov pristojnim organom pregona v državah članicah omogočal učinkovito preprečevanje in preiskovanje vseh oblik kriminalitete, posebno organiziranega kriminala in terorizma.

## Sirene

Vsaka pogodbenica imenuje organ, ki je odgovoren za nacionalni del SIS, to so SIRENE (Supplementary Information Request at National Entry – zahteve po dodatnih informacijah pri nacionalnih vnosih). Vsaka pogodbenica izdaja svoje razpise ukrepov samo s pomočjo tega organa.

SIRENE so odgovorne za nemoteno delovanje nacionalnega dela SIS in sprejemajo potrebne ukrepe za zagotovitev upoštevanja določb te konvencije. Treba je poudariti, da je s SIS in njenim pomožnim elementom SIRENE doseženo zelo široko in dobro sodelovanje med policijami. S pomočjo teh tehničnih in operativnih sistemov namreč krožijo vse informacije, ki so v pomoč policistom pri opravljanju njihovih nalog. SIRENE so osnova za mednarodno policijsko sodelovanje na schengenskem območju (sistematično policijsko sodelovanje, ki temelji na medsebojni izmenjavi podatkov in razpisov za iskanje osebe in predmetov, ki jih države prosilke tekoče obnavljajo, po načelu medsebojnega zaupanja – enako, kot bi podatke obravnavali v nacionalnem sistemu). Celotno poslovanje med uradi SIRENE je poenoteno (standardizirano) na podlagi Priločnika SIRENE, ki se sprti popravlja in dopolnjuje.

Vse to pa ureja posebna aplikativna rešitev, ki je bila v celoti razvita z lastnim znanjem in lastnimi viri. Omogoča:

- prejemanje in pošiljanje posebej strukturiranih sporočil (SIRENE obrazci)
- prejemanje in pošiljanje nestrukturiranih sporočil (SISNET)
- samodejno obveščanje operaterjev SIRENE o vseh SIS zadetkih
- uvrščanje ter upravljanje vseh sporočil oz. dokumentov znotraj ustreznega dosjeja.

## Naloge in pristojnosti uradov Sirene

Osrednje naloge nacionalnih uradov SIRENE se nanašajo predvsem na izmenjavo dodatnih (supplementary) podatkov:

20 Pogodba med Kraljevino Belgijo, Zvezno republiko Nemčijo, Kraljevino Španijo, Francosko republiko, Velikim vojvodstvom Luksemburg, Kraljevino Nizozemsko in Republiko Avstrijo o poglobitvi čezmejnega sodelovanja, predvsem pri zatiranju terorizma, čezmejne kriminalitete in nezakonite migracije. Republika Slovenija je članica Prümške pogodbe od avgusta 2007.

Državni zbor Republike Slovenije je 9. 3. 2007 sprejel tako Prümško pogodbo kot skupno izjavo, 3. 4. 2007 pa sta bili obe objavljeni v Uradnem listu (Ur. l. RS, 30/2007). Listine o ratifikaciji in izjave so bile poslane depozitarju 4. 5. 2007 (vlada Zvezne republike Nemčije). Prümška pogodba je za Republiko Slovenijo začela veljati 8. 8. 2007. Skladno s 44. členom Prümške pogodbe pristojne službe pogodbenic na podlagi te pogodbe sklenejo sporazume, katerih cilj je upravno-pravna izpolnitev pogodbe, kar se kaže v izvedbenem sporazumu Prümške pogodbe, imenovanem ATIA.

- pred razpisom tiralice,
- sočasno oziroma vzporedno z razpisom tiralice,
- ob večkratnem razpisu tiralice,
- ob označitvi (opombi k) tiralice (flag),
- ob zadetku (hit),
- ob razpisu ukrepa »zavrnitev vstopa državljana tretje države«,
- o nezmožnosti izvajanja določenega ukrepa, ki je predviden ob zadetku,
- ob spremembi namena,
- ob nepravilnih podatkih,
- ob nezakonito shranjenih podatkih,
- o pravici vpogleda v lastne podatke in
- o pravici do poprave podatkov.

## Prümska pogodba

Prümska pogodba je večstranska mednarodna pogodba, s katero želijo pogodbenice<sup>20</sup> poglobiti medsebojno čezmejno policijsko sodelovanje, predvsem z izmenjavo informacij med državami članicami Evropske unije.

Prümska pogodba omogoča izmenjavo podatkov iz nacionalnih policijskih podatkovnih baz DNK profilov, podatkovnih baz odtisov papirarnih linij (prstnih odtisov, odtisov dlani ipd.), baz podatkov registriranih motornih vozil med državami podpisnicami ter izmenjavo podatkov pri varnostno tveganih mednarodnih prireditvah, za preprečevanje terorističnih kaznivih dejanj, čezmejne kriminalitete in za zatiranje nezakonitih migracij med državami podpisnicami.

Na podlagi določil Prümske pogodbe so države pogodbenice v okviru Prümskega partnerstva ustanovile skupno delovno skupino in tehnične delovne skupine. Skupna delovna skupina (Joint Working Group – JWG) je krovna delovna skupina, v okviru katere deluje pravna delovna skupine (Legal Working Group), za posamezna področja pa so ustanovljene tehnične delovne skupine (Technical Working Group – TWG), in sicer za DNK profile, za daktiloskopske podatke, za podatke o vozilih, za terorizem in velike prireditve, za ukrepe vračanja in za policijsko sodelovanje.

Urad za informatiko in telekomunikacije Generalne policijske uprave je postavil osnovno infrastrukturo, vzpostavil omrežje TESTA II (mednarodno omrežje, ki omogoča kriptiran prenos podatkov), pripravil Windows 2003 podatkovni in poštni strežnik z SQL serverjem 2005 in Lotus Dominom (SMTP in POP3), vzpostavil povezavo poštnega strežnika z omrežjem TESTA II preko HKOM omrežja in pripravil referenčne baze podatkov in osnovne aplikacije za preverjanje informacij o zadetkih (nezadetkih). Izmenjava DNK profilov z Avstrijo že poteka, pravkar pa poteka tudi testiranje z Nemčijo.

Posamezne podpisnice Prümske pogodbe bodo izmenjavo daktiloskopskih podatkov vzpostavile postopoma, in sicer večinoma do konca leta 2008 (Slovenije predvidoma v drugi polovici 2008). Do sedaj so strokovne službe Generalne policijske uprave vzpostavile omrežje TESTA II. Potekajo pa priprave za vzpostavitev in nadgradnje sistema AFIS (Automated Fingerprint Identification System).



7. Projele spremne za godišni  
izveštaj o ostvarenju ciljeva i  
obavljenoj radnji u skladu s  
godišnjim planom.

PC



0101010111100010110110110101

# POLICIJA

## Novi ISPP

Delavci UIT so v sodelovanju s policijskimi enotami zasnovali ISPP, ki ima svoje začetke že v letu 1991, leta 2007 pa je bil napisan povsem na novo. To je produkcijsko-programski paket, s katerim so policijske enote začele voditi pisarniško poslovanje (evidenco dokumentov in zadev), ter vse lokalne evidence, pomembne za policijsko postajo. Ta informacijski sistem, ki je bil pomemben zlasti za evidence na lokalni ravni, je bil najprej nadgrajen z informacijskim sistemom za področje prometa, imenovan ISPP-PROM, kasneje pa še za javni redi in mir (ISPP-JRM) ter mejne zadeve (ISPP-MEJA), je v tistem obdobju pomenil pravo revolucijo v spremembi filozofije pri zajemanju, obdelavi in uporabi podatkov. Prvič je bilo omogočeno povezovanje lokalnih evidenc na policijski postaji s centralnimi evidencami na tedanjemu MNZ. Aplikacija omogoča izdelavo različnih seznamov kršiteljev, po različnih kršitvah in v povezavi s krajem in časom storitve.

Seveda pa je informacijsko-tehnološki razvoj v zadnjem obdobju presegel rešitve, zasnovane v devetdesetih letih, ki so bile uporabne več kot deset let. V UIT so razvili Novi ISPP, ki je arhitekturno in tehnološko popolnoma nova aplikacija, vsebinsko pa zajema delovne procese na policijskih postajah. Zaradi velikih tehnoloških sprememb so nekateri procesi poenostavljeni, ponuja pa tudi nove možnosti za nadaljnjo racionalizacijo.

Za lažje poslovanje ter zmanjšanje podvajanja podatkov je aplikacija tesno povezana s policijskimi evidencaми (FIO).

Aplikacijo sestavljajo naslednji elementi:

- evidenca dokumentov in zadev
- poročilo dežurnega
- raspored dela in evidenca prisotnosti
- obračun ur in potnih stroškov.

Vse rešitve so delo lastnega kadra, ustrezajo pa tudi predpisom s področij, ki jih aplikacija zajema.

## Intranet Policije

Uspešnost spletne tehnologije je povzročila tudi razvoj zasebnega omrežja za interno izmenjavo vsebin. Tako ima lahko vsako podjetje in organizacija notranje razvejano ter predvsem varno in zasebno implementacijo interneta, ki ga imenujemo intranet<sup>21</sup>. Velika količina internih notranjih informacij, ki so se prej razširjale in objavljale preko pisnih medijev, je sedaj preko spletnih strani hitro in preprosto dostopna vsakemu uporabniku intraneta. Spletne informacije so lahko oblikovane tekstualno, grafično, slikovno, zvočno, nekatere pa vsebujejo celo video zapis. Intranet je bil v slovensko Policijo uveden leta 2000. Vzpodbuda za uvedbo spletne tehnologije v UIT oziroma za postavitve strežnika je bila predvsem možnost ponudbe informacijskega sistema IUS-INFO širšemu krogu delavcev Policije. Kasneje pa so snovalci oblikovali pestre vsebine policijskega portala.

Intranetne spletne strani so dostopne izključno notranjim (policijskim) uporabnikom in so namenjene obveščanju, medsebojnemu komuniciranju in sodelovanju ter posredovanju informacij in podatkov, ki so potrebni pri operativnem delu. Upravlja ga uredniški odbor za intranet in internet Policije, ki ga z odločbo imenuje generalni direktor Policije.

Intranet je sčasoma prerasel v pomemben sistem za interno obveščanje in sodelovanje. Dostop imajo praktično vsi zaposleni v Policiji. Osnovna stran je urejena kot portal, ki na enem mestu ponuja najnovejše informacije in sporočila. Na intranetu so tri vrste osnovnih storitev:

- statične spletne vsebine, ki jih v UIT večinoma objavljajo na zahtevo posameznih enot;
- zbirke dokumentov oz. vsebin: za vsako takšno zbirko je razvita posebna aplikacija, ki omogoča objavljanje vsakomur na podlagi njegovih pristojnosti. Zagotovljena je maksimalna ažurnost, poleg tega pa se vsebine objavljajo tam, kjer tudi nastajajo;
- podportali enot, ki posameznim enotam omogočajo objavo njihovih lokalnih vsebin.

---

21 Intranet je zasebno računalniško omrežje, ki deluje na TCP/IP protokolu in uporablja spletno tehnologijo. Nekateri ga poimenujejo tudi interni internet. Na intranetnih strežnikih se pojavljajo predvsem interne informacije in podatki, ki so lahko tudi zaupni. Intranet sestavljajo eden ali več strežnikov in odjemalci (spletni brskalniki).



Tehnične značilnosti:

- spletni strežnik IBM HTTP Server (powered by Apache)
- PHP Version 4.2.1 (serviranje dinamičnih strani)
- podatkovna baza MySQL 3.23.49
- iskalni mehanizem omogoča "Microsoft Index Service"
- aplikacijski strežnik IBM Lotus Domino Server 5.08

## Prenova fiksnega govornega omrežja Policije

Fiksno govorno omrežje zajema vse ravni MNZ in Policije, njegovo posodabljanje pa poteka v skladu z njuni strateškimi načrti. Star sistem je slonel na tehnologijah različnih proizvajalcev, zato ga je bilo potrebno tehnološko poenotiti. Policija je bila opremljena predvsem s sistemoma Alcatel OmniPCX Office in OmniPCX Enterprise. Sedaj je omrežje primerljivo z omrežji javnih operaterjev in jih v posameznih segmentih celo presega. Posodabljanje je najprej potekalo v lokalnih policijskih enotah (2002–2005), v zadnjem obdobju pa v MNZ, GPU in PU. Nadgradnja fiksnega govornega omrežja je slonela na ohranjanju obstoječe funkcionalnosti, ki je potrebna pri operativnem delu, in tudi na zagotavljanju novih storitev. Gre za zagotavljanje govorne komunikacije preko IP protokola (VOIP) – paketni prenos v sinergiji s TDM tehnologijo in ISDN protokoli. Tovrstna kombinacija tehnologij omogoča optimalno izkoriščanje obstoječe infrastrukture in optimizacijo stroškov komunikacij.

Posodobitev oziroma nadgradnjo fiksnega govornega omrežja Policije lahko razdelimo na:

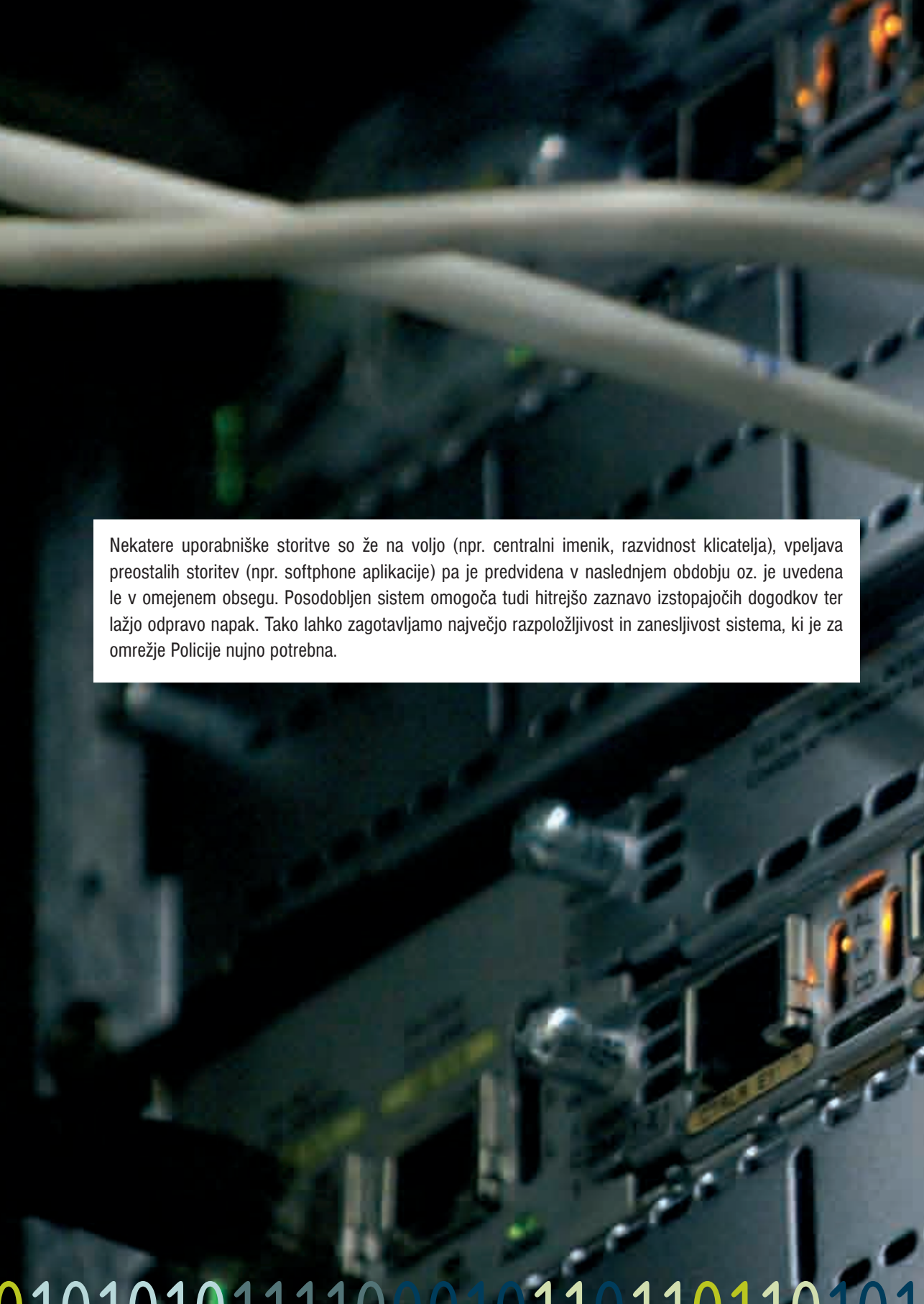
- sistemsko:

- IP platforma vozlišč,
- sinergija IP in TDM tehnologije,
- postopno uvajanje IP telefonije,
- poenotenje arhitekture vozlišč,
- povezava z računalniškim okoljem (CTI),
- optimalna povezljivost z drugimi sistemi ITSP,
- optimizacija pri izbiri javnih omrežij,
- večja sistemska zanesljivost, redundančnost,
- enotno in enostavnejše upravljanje,
- povečanje zanesljivosti, razpoložljivosti in varnosti;

- uporabniško:

- poenotenje oštevilčenja na vseh treh ravneh fiksnega govornega omrežja Policije,
- direktna dosegljivost vseh internih priključkov iz javnega omrežja,
- direktna medsebojna dosegljivost internih priključkov znotraj vseh treh ravni internega omrežja Policije,
- dostopnost javnega mobilnega omrežja za vse interne priključke,
- pridobitev dodatne funkcionalnosti in storitev naročniških priključkov.





Nekatere uporabniške storitve so že na voljo (npr. centralni imenik, razvidnost klicatelja), vpeljava preostalih storitev (npr. softphone aplikacije) pa je predvidena v naslednjem obdobju oz. je uvedena le v omejenem obsegu. Posodobljen sistem omogoča tudi hitrejšo zaznavo izstopajočih dogodkov ter lažjo odpravo napak. Tako lahko zagotavljamo največjo razpoložljivost in zanesljivost sistema, ki je za omrežje Policije nujno potrebna.

0101010111100010110110110101





1101000001101010110111010100



## Klicni centri 113

Klicni centri 113 sodijo med ključne elemente policijskega dela, po katerih javnost ocenjuje policijsko delo. Vsako leto evidentiramo milijon klicev občanov na interventno številko 113. Leta 2004 se je začela nadgradnja teh centrov, ki predvideva poenotenje sistemov, centralizacijo ter večjo varnost in zanesljivost shranjenih podatkov. Sistem so načrtovali strokovnjaki UIT v sodelovanju z delavci OKC, torej je plod lastnega znanja in izkušenj. Sedaj je to sodobni klicni center na telekomunikacijskem sistemu (Simens\_HiPath), za delovna mesta operaterjev je podprt s CTI aplikacijo in centralizirano bazo podatkov v glavnem računalniku.



Nadgradnja klicnih centrov 113 je prinesla naslednje bistvene pridobitve:

- Š Strojna telekomunikacijska in informacijska oprema je bila modernizirana in poenotena. Vključena je bila oprema, ki je tipizirana v ITSP in se ob morebitni okvari lahko takoj zamenja z rezervno opremo.
- S poenotenjem aplikativne programske opreme smo dosegli organizacijsko mobilnost policistov in pridobili funkcionalnost.
  - MS Access bazo je zamenjala zmogljivejša relacijska baza IBM DB2.
  - Za lažje vzdrževanje, večjo varnost in zanesljivost je bil izveden prehod s podatkovne baze na lokalnem strežniku na podatkovno bazo v centralnem računalniku (HOST).
  - S tem se je zmanjšala tudi količina informacijske strojne opreme. Obenem so operativni podatki, zbrani preko vstopnih točk 113, z implementacijo novih aplikacij na voljo tudi vsem drugim operativnim policijskim enotam.
  - Pridobljeno znanje omogoča, da osnovno vzdrževanje lahko izvajajo posamezne službe v Policiji (UIT GPU, OIT PU). S tem smo bistveno skrajšali odzivni čas ob prijavi okvare ter posledično čas za odpravo napake, obenem pa so se zmanjšali tudi stroški vzdrževanja sistema (zmanjšanje števila pogodb).

## Prenova komunikacijske infrastrukture

Vključevanje v globalne informacijsko-telekomunikacijske sisteme (Interpol, Europol, FADO ...) in SIS je pred slovensko Policijo postavil nove izzive za tehnološki razvoj, prenavo in posodabljanje informacijsko-telekomunikacijske infrastrukture. Številne tehnične rešitve so zagotovile ustrezne storitve in pogoje za delovanje novih, naprednejših in uporabnikom prijaznejših aplikacij. Novo integrirano širokopasovno omrežje temelji na tehnologiji navideznih zasebnih omrežij (VPN/MPLS – Virtual Private Networks over Multiprotocol Label Switching). Primarni ter sekundarni računalniški in komunikacijski center sta povezana preko DWDM sistemov (Dense Wavelength Multiplexing), z agregatno hitrostjo preko 10 Gb/s. Centra sta tudi vstopni točki za SIS.

Vse policijske enote se v omrežje vključujejo s hitrostjo od 1 Mb/s, 10/100 Mb/s in 1 Gb/s. Trenutno poteka vključevanje širokopasovnih redundantnih povezav do prioritarnih schengenskih lokacij.

## Digitalni mobilni radijski sistem

Državni organi Republike Slovenije so večinoma uporabljali analogne radijske sisteme, ki so po zasnovi zelo stari in ne omogočajo hitrega prenosa podatkov niti ne zagotavljajo kakovostne kriptozasčite ali povezovanja različnih skupin, frekvenčna koordinacija s sosednjimi državami pa je otežena. Zato je bil za MNZ - Policijo pripravljen projekt za digitalizacijo radijskih sistemov, ki ga je potrdila Vlada RS in so bili vanj vključeni tudi drugi državni organi. Projekt je bil zaradi novih zahtev in pogojev vključen tudi v Schengenski izvedbeni načrt (SIN), ki je bil medresorsko usklajen in nazadnje potrjen leta 2005. Vključitev v SIN je v tehničnem smislu pomenila tudi razširitev projekta, saj so bile pred UIT postavljene dodatne zahteve po delovanju omrežja. Določene in implementirane so bile tudi aktivnosti za digitalizacijo mobilnega radijskega sistema ob vključevanju Slovenije v schengenski prostor.

Kratica TETRA je prvotno pomenila Trans-European Trunked Radio (Vseevropski sistem snopovnih radijskih zvez). Ker pa se je ta tehnologija začela uporabljati tudi drugod po svetu, so jo preimenovali v Terrestrial Trunked Radio (Prizemeljske snopovne radijske zveze). Sistem je prvi pravi odprti digitalni standard za zasebna radijska omrežja, ki ga je določil ETSI – European Telecommunications Standards Institute (Evropski standardizacijski institut za telekomunikacije).

Podobno kot analogna omrežja za mobilno telefonijo (npr. NMT, TACS ...), ki se nadomeščajo z digitalnimi sistemi (GSM, UMTS), se tudi zasebna radijska modernizirajo – zamenjujejo z digitalnimi, ki pa so standardizirani, kar zagotavlja zaščito uporabnikov in tudi proizvajalcev.

Digitalizacija pomeni kakovosten preskok, kar se danes kaže tudi na drugih tehničnih področjih. Tudi pri TETRI pokrivanje geografskega območja z radijskim signalom omogoča celična tehnologija. Vse bazne postaje, ki pokrivajo določene celice, so povezane z glavnim centralnim kontrolorjem sistema (podobno funkcijo ima v mobilni telefoniji centrala). Ob vklopu radijske postaje se ta avtomatsko prijavi na domače omrežje in v kontrolorju se registrira v skladu z nastavitvami. Glede na zahteve se določeni postaji ali terminalu lahko onemogoči dostop in delo. Uporabnikom med gibanjem in preklopi med baznimi postajami ni potrebno predstavljati radijskih kanalov na napravah, ampak to poteka avtomatsko, podobno kot v mobilni telefoniji.





0101010111100010110110110110101



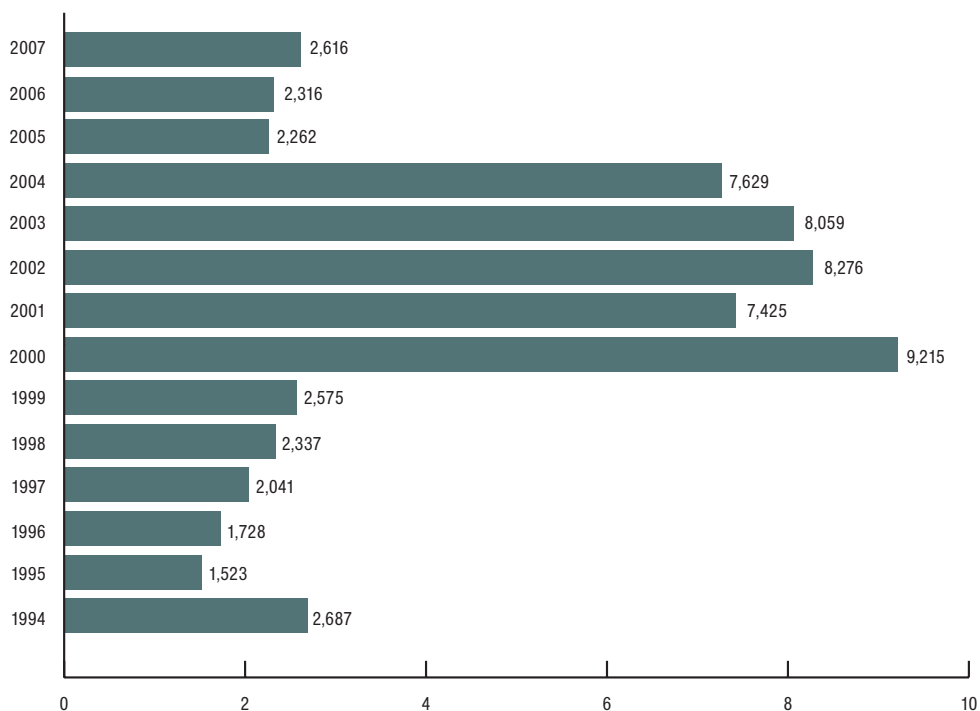
Predstavniki MNZ - Policije delujejo v posebnem delovnem telesu EU, ki je določilo tudi čezmejno policijsko sodelovanje pri radijskih zvezah. Opredeljujejo ga harmoniziran frekvenčni pas, omrežja TETRA in Tetrapol, na obmejnih območjih pa povezovanje radijskih omrežij z minimalnim številom storitev.

Predstavniki MNZ so sodelovali tudi v Twinning projektih (SL98/IB/JHA/01 in SL99/IB/JHA/02 – Vzpostavitev učinkovitega sistema za nadzor državne meje), v okviru katerih je bila pridobljena pomoč strokovnjakov Evropske unije. Tako so bili na področju radijskih zvez vzpostavljeni stiki s predstavniki notranjih ministrstev Avstrije, Nemčije, Nizozemske, Finske in Švedske.

## XII. INVESTICIJE V INFORMACIJSKO TELEKOMUNIKACIJSKA SREDSTVA POLICIJE

Slovenska policija oziroma UIT je za naložbe v informacijsko ter telekomunikacijsko opremo neposredno po osamosvojitvi Slovenije vlagala povprečno letno 2,3 milijona EUR. Za vse naložbe so bile izdelane strokovne podlage ter idejne zasnove, ki so bile opredeljene tudi v srednjeročnih planskih dokumentih Strategije razvoja informacijskega in telekomunikacijskega sistema policije. Naložbena aktivnost UIT je bila v preteklosti pretežno financirana iz lastnih proračunskih sredstev policije oziroma sredstev ministrstva. To je zahtevalo veliko naporov in odrekovanja tudi ostalih služb v Policiji. Investicijska sredstva v prvem obdobju so bila skromna in niso omogočila večji poseg v modernizacijo in posodobitev IT sistema. Šele z evroatlanskimi povezavami ter po sporazumu z vlado RS je ministrstvo oziroma policija prevzela tudi obvezo o zagotovitvi modernizacije in kompatibilnosti IT sistema policije s sistemom SIS. Ta odločitev je pomembno vplivala na prednost izvajanja načrta investicij. Po letu 2000 pa je država ter Evropa hitro razvijajoče IT sistem policije zaradi vključevanja v schengensko informacijsko okolje tudi finančno podprla v okviru Phare programa (s sredstvi iz evropskih skladov) ter na ta način omogočila prenovo oziroma izgradnjo ITK infrastrukture in hitro modernizacijo slovenske policije.

Investicije v ITS policije v posameznih letih v mil. EUR





## XIII. UIT – SKRBNIK EVIDENC

Na podlagi Zakona o varstvu osebnih podatkov je bil izdelan tudi prvi katalog zbirk osebnih podatkov<sup>22</sup> Ministrstva za notranje zadeve, ki je bil poslan takratnemu Ministrstvu za znanost in tehnologijo, pristojnemu za vodenje kataloga podatkov. Katalog je vseboval podatke za 52 zbirk osebnih podatkov. Z novim Zakonom o policiji je Policija postala organ v sestavi ministrstva, ki upravlja zbirke osebnih podatkov<sup>23</sup> (evidence) s svojega delovnega področja. Minister za notranje zadeve tudi podrobneje predpiše način vodenja evidenc<sup>24</sup>, določenih v Zakonu o policiji, Policija pa je s pravilnikom<sup>25</sup> natančneje uredila samo vzdrževanje, hranjenje evidenc in virov ter posredovanje podatkov iz evidenc. Evidence vsebujejo skupne osebne podatke, in sicer: osebno ime, rojstne podatke (dan, mesec, leto, kraj), EMŠO, spol, naslov stalnega oziroma začasnega prebivališča in državljanstvo. Poleg skupnih osebnih podatkov pa so v ZPol za vsako posamezno evidenco podrobno predpisani še drugi podatki.

V zvezi z izvajanjem policijskih pooblastil Policija vodi in vzdržuje naslednje evidence, katerih skrbnik je Urad za informatiko in telekomunikacije:

1. evidenco kaznivih dejanj
2. evidenco kršiteljev in prekrškov
3. evidenco iskanih oseb
4. evidenco identifikacij
5. (črtana)
6. evidenco operativnih informacij
7. evidenco oseb, zoper katere so bili izvedeni prikriti preiskovalni ukrepi iz zakona, ki ureja kazenski postopek
8. evidenco DNK preiskav
9. evidenco dogodkov
10. evidenco pridržanih in zadržanih oseb
11. evidenco varnostno preverjenih oseb
12. evidenco pritožb
13. evidenco uporabe prisilnih sredstev
14. evidenco daktiloskopiranih oseb
15. evidenco fotografiranih oseb
16. evidenco iskanih in najdenih predmetov
17. evidenco usmerjenega zbiranja obvestil o terorizmu in mednarodnem organiziranem kriminalu
18. evidenco vstopov in gibanja oseb v varovanih objektih Policije in okoliših teh objektov

22 Upravljalavec osebnih podatkov mora za vsako zbirko osebnih podatkov vzpostaviti in voditi katalog, ki mora biti točen in ažuren. V 26. členu ZVOP-1 je predpisanih trinajst skupin podatkov, ki pomenijo opis posamezne zbirke in jih mora vsebovati katalog. Namen takšnih katalogov je uveljavljanje pravice posameznika do seznanitve o namenu obdelave in vrstah osebnih podatkov, ki jih upravljalavec zbira.

23 Policija zbira osebne podatke in druge podatke zaradi opravljanja z zakonom določenih nalog.

24 57. člen Zakona o policiji (ZPol, uradno prečiščeno besedilo – UBP6, Ur. list RS, št. 107/2006, 17. 10. 2006).

25 Pravilnik o načinu vodenja policijskih evidenc (Ur. list, št. 121/2004, 11. 11. 2004).

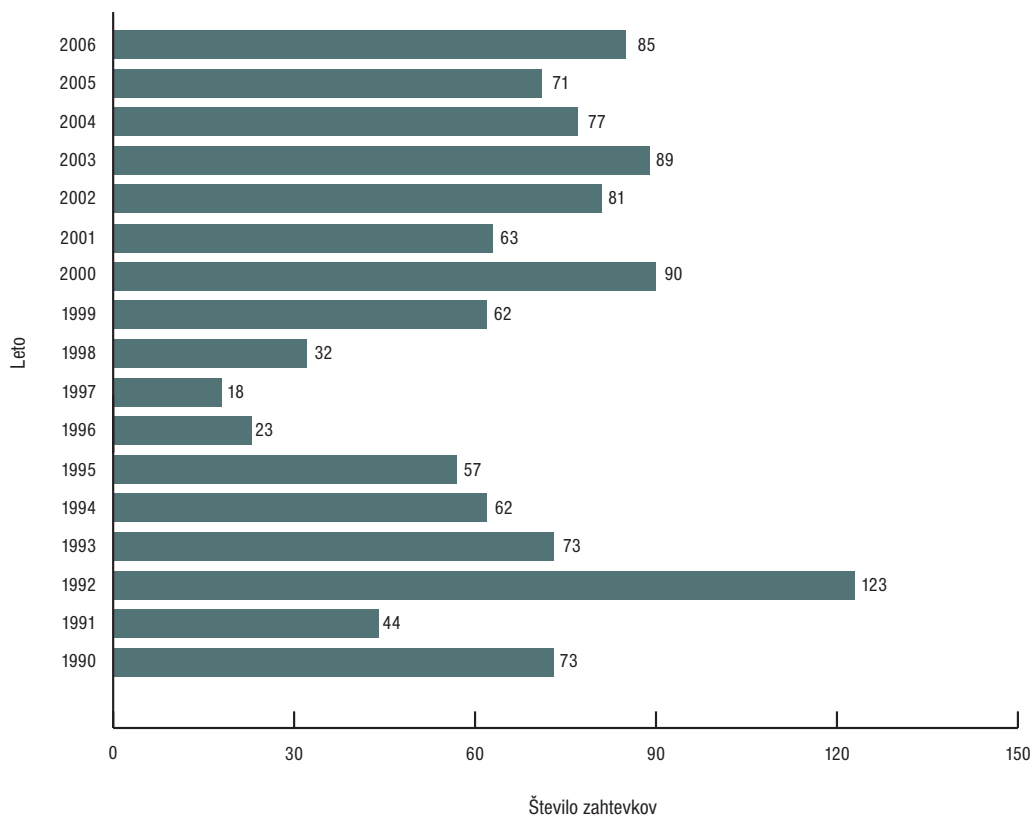


- 19. evidenco izdanih odredb za prepoved približevanja
- 20. evidenco prikritih evidentiranj in namenskih kontrol.

UIT je tudi lastnik in skrbnik evidence dovoljenj za obravnavanje tajnih podatkov.

Posameznik ima pravico do vpogleda v svoje podatke v evidencah<sup>26</sup>. V Policiji je ustanovljena tudi komisija<sup>27</sup> za varstvo osebnih podatkov, katere član je tudi delavec UIT. Komisija opravlja naloge v zvezi z uresničevanjem pravic posameznikov, ki jih Zakon o varstvu osebnih podatkov nalaga Policiji kot upravljavcu evidenc. Število zahtevkov za varstvo pravic iz ZVOP-1, ki so jih posamezniki naslovili na Policijo oziroma komisijo za varstvo osebnih podatkov v posameznih letih, je bilo zelo različno, odvisno je tudi od družbenih razmer, ki problematizirajo ter aktualizirajo varstvo osebnih podatkov ter morebitno izpostavljenost oseb v policijskih evidencah.

Število zahtevkov za varstvo pravic iz ZVOP-1 oziroma vpogledov v policijske evidence



26 62. člen Zpol-UBP6, Ur. list RS, št. 107/2006, 17.10.2006

27 Komisijo za varstvo osebnih podatkov (v nadaljevanju KVOP) na podlagi 5. člena Pravilnika o načinu vodenja policijskih evidenc imenuje generalni direktor policije. KVOP sestavljajo predsednik, po en predstavnik lastnikov evidenc in član iz CZP UIT GPU, ki opravlja tudi naloge tajnika KVOP. Tajnik KVOP je na predlog KVOP in na podlagi pooblastila generalnega direktorja policije pooblaščen tako za vodenje kot za odločanje v postopkih z delovnega področja KVOP. Odgovoren je tudi za hrambo gradiva KVOP. KVOP je tako operativno-tehnično telo, saj morajo člani dobro poznati vsebino evidenc in vse elemente obdelave podatkov, ki jih evidence vsebujejo (Arko: str.: 50, 2008).



## XIV. VIZIJA

Vizija Policije je, da se s svojim strokovnim znanjem in kakovostnimi storitvami uspešno sooča z varnostnimi izzivi in zagotavlja visoko stopnjo varnosti. Vizija UIT pa, da ji z ustreznimi IT rešitvami pri tem nudi vso potrebno podporo za učinkovito in uspešno delo. Tako želimo:

- še bolje prilagoditi IT rešitve poslovnim potrebam
- zgraditi podatkovno skladišče kot osnovo za statistično poročanje
- vzpostaviti elektronski arhiv
- vpeljati mobilne podatkovne rešitve in mobilno pisarno
- vpeljati satelitsko navigacijo GPS-AVL
- dokončati digitalizacijo radijskega omrežja na celotnem ozemlju RS
- dokončati širokopasovno WAN omrežje z vsemi obhodnimi potmi
- optimizirati fiksno in mobilno govorno omrežje
- uvesti tehnične sisteme za nadzor in zmanjšanje hitrosti na slovenskih cestah
- v uporabo vpeljati video sisteme za nadzor dogajanj ob meji in video nadzor ob varnostno pomembnih dogodkih ter daljinski nadzor z integracijo v WAN
- integracijo storitev na enotno IP tehnologijo
- vpeljavo informacijskega sistema za tajne podatke
- dokončati uvedbo sistema enotne prijave.

Glede na temeljne smernice Vlade RS, zakonske naloge oziroma planske dokumente Policije in projekte, ki se izvajajo, bo Urad za informatiko in telekomunikacije nadaljeval izgradnjo ITSP, zagotavljal nemoteno delovanje centralne informacijske infrastrukture ter njenega vzdrževanja, zagotavljal podporo uporabnikom standardnih programskih orodij in aplikacij ter zagotavljal implementacijo aplikativnih projektov in uvajal informacijske ter telekomunikacijske tehnologije v Policiji, izvajal strokovno usposabljanje in izobraževanje uporabnikov, razvijal informacijski sistem za podporo odločanja, skrbel za razvoj in vzpostavitev sistema varovanja in zaščite osebnih in tajnih podatkov Policije ter za nemoteno delovanje ITSP.



## XV. VODJE INFORMATIKE IN TELEKOMUNIKACIJ

Odkar je ta služba postala samostojna, so jo vodili: Edo KRANJČEVIČ (1979–1980), Herman SAVEC (1986–1990), Stanko ČUFAR (1990–1995), Bojan KOS (1995–1998), Bojan GLAVNIK (1999–2007), od leta 2007 pa jo vodi Andrej BRAČKO. Vsakdo s svojim osebnim prispevkom pomembno vplival na razvoj informatike in telekomunikacij v slovenski Policiji.

Pred ustanovitvijo samostojne organizacijske enote so oddelke oziroma sektorje ter centre za mehanografsko kot kasneje elektronsko oziroma avtomatsko obdelavo podatkov vodili:

- 1957:** Vida KULOVEC, vodja Službe za evidence in administracijo
- 1964:** Lovro ŠEFMAN, vodja Službe za operativne evidence, statistiko in administracijo
- 1970:** Martin VRANČIČ, vodja Službe za operativne evidence, statistiko in administracijo  
Janez MENART, vodja Sektorja AOP
- 1975:** Herman SAVEC, načelnik ERC-a



## VIRI

- Arko, S.: Varstvo osebnih pravic – pravna ureditev in naloge policije, diplomska naloga, 2008.
- Batis, R.: UIT, predstavitevna brošura, Ljubljana 1996.
- Bračko, A. : V boju proti hrošču, Varnost 1/2000.
- Bračko, A.: Schengenski informacijski sistem, Varnost, 4/2007.
- Bogataj, I. : Medresorska skupina Tetra, poročilo, 2007.
- Brvar, B.: 40 let informacijskega sistema organov za notranje zadeve, Ljubljana 1997.
- Brenčič, A.: Stanje računalništva v RSNZ in predviden razvoj, Varnost – strokovni bilten, Ljubljana 1979.
- Berlec, B., Koblar, M., Cizel, A.: Prenova fiksnega govornega omrežja policije, poročilo, 2008
- Lenarčič, I.: Fonetični indeks oseb, Ljubljana 2002.
- Radulovič, D.: letna poročila o izobraževanju in usposabljanju zaposlenih v UIT.
- Vidmar, P.: Širjenje informatike v ONZ SRS, Varnost – strokovni bilten, Ljubljana 1981.
- Vučko, I. : Nove spletne strani policije, Varnost, 2-3/2001.
- Vučko, I. : Intranet v Policiji, Varnost, junij 2001.
- Vučko, I.: Nova EPP in ISPP, poročilo, 2007.
- Letna poročila MNZ GPU in UIT.
- Strategija razvoja ITS Policije v obdobju 2004–2007, Ljubljana 2004.
- Pregledi, interni časopis UIT, Ljubljana 1996.





0101010111100010110110110110101



1101000001101010110111010100





