Univerza v Mariboru

Fakulteta za varnostne vede

**DIPLOMSKO DELO**

# Kazniva dejanja na področju informacijske varnosti v Sloveniji

December, 2013

Roman Krajnc

Univerza v Mariboru

Fakulteta za varnostne vede

**DIPLOMSKO DELO VISOKOŠOLSKEGA STROKOVNEGA ŠTUDIJA**

**Varstvoslovje**

# Kazniva dejanja na področju informacijske varnosti v Sloveniji

December, 2013

Roman Krajnc

Mentor: doc. dr. Igor Bernik

## ZAHVALA

*Zahvaljujem se moji družini in vsem ostalim, ki so me spodbujali in mi na kakršenkoli način pomagali pri nastajanju diplomskega dela.*

*Zahvaljujem se svojemu mentorju doc. dr. Igorju Berniku za strokovno pomoč, usmerjanje in podporo tekom izdelave diplomskega dela.*

*Hvala!*

**Kazalo vsebine**

**Kazalo tabel**

**Kratice in akronimi**

| | |
|---|---|
| CERT | Center za posredovanje pri internetnih incidentih |
| CSIRT | je kratica za Skupino za reševanje varnostnih incidentov |
| ISMS | information security management system |
| RS | Republika Slovenija |
| SUIV | sistem za upravljanje informacijske varnosti |
| VNC | varnostno-nadzorni center |
| ZEKom | Zakon o elektronskih komunikacijah |
| ZEPT | Zakon o elektronskem poslovanju na trgu |
| ZEPEP | Zakon o elektronskem poslovanju in elektronskem podpisu |

# Povzetek

Živimo v svetu v katerem je informacija iz dneva v dan pomembnejša. Z razvojem informacijske tehnologije je tudi dostop do informacije vse lažji in hitrejši. Da bi naprave nemoteno delovale jih moramo tudi dobro spoznati, da lahko nemoteno delujejo pred različnimi grožnjami.

V diplomskem delu smo obravnavali kazniva dejanja, ki se pojavljajo na področju informacijske varnosti v Sloveniji. V teoretičnem delu smo proučili kazniva dejanja kibernetske kriminalitete, proučili kakšno je področje informacijske varnosti v Sloveniji, kibernetsko kriminaliteto in z njo povezane osnove, dotaknili smo se zakonodaje na področju informacijske varnosti v Sloveniji in predstavili katere so še drugi možni vidiki zaščite uporabnikov informacijskih sistemov. V praktičnem delu naloge smo na področju analize analizirali kazniva dejanja na področju informacijske varnosti v Sloveniji v obdobju od leta 2005 pa vse do leta 2010. Na podlagi proučenega in analiziranega smo podali zaključek.

Ključne besede: kazniva dejanja, kibernetska kriminaliteta, kibernetski prostor, kazenski zakonik, informacijska varnost, analiza rezultatov

# Offences in Information security in Slovenia

## Summary

In this thesis we deal with crimes that occur in the field of information security in Slovenia. The thesis is theoretical and practical. In the theoretical part we investigate crimes cyber crime, explore how the field of information security in Slovenia, cyber crime and related base, we touched on the legislation in the field of information security in Slovenia, and present what are other possible aspects of the protection of users of information systems. In the practical part of the paper we analyze the analysis of crimes in the area of information security in Slovenia in the period from 2005 until 2010. Based on studied and analyzed, we made a conclusion.

Key words: crime, cyber crime, cyber space, Penal Code, information security, analysis of the results

# 1 Uvod

Dandanes je poslovanje v organizacijah v veliki meri podprto z informacijskimi sistemi in osnova za nemoteno delovanje. Učinkovitost izvedbe poslovnih procesov je pogojena z zadovoljnim delovanjem informacijskega sistema, saj njegovo nedelovanje ali okrnjeno delovanje pogosto vodi v prekinitev izvajanja ključnih poslovnih procesov v organizacije. Informacijski sistemi so v različnih organizacijah izpostavljeni različnim tveganjem s stališča varnosti.

Lukman (2008) pravi, da statistični rezultati ne predstavljajo absolutnega sodila o lastnostih storilcev kibernetskega kriminala, saj je potrebno na področju kibernetske kriminalitete upoštevati veliko polje neidentificiranih kaznivih dejanj ter izredno selektivno prijavo zaznanih kaznivih dejanj s strani oškodovancev. Prav tako pravi, da nekateri avtorji navajajo na en prijavljen incident celo 4000 poizkusov napadov na informacijske sisteme.

V nalogi nameravamo proučiti kazniva dejanja na področju informacijske varnosti v Sloveniji v obdobju od leta 2005 do 2010. To obdobje smo si izbrali zaradi tega, da bomo lažje primerjali število kaznivih dejanj, ker predvidevamo, da se število iz leta v leto povečuje.

## *1.1 Namen in cilj*

Namen diplomskega dela je proučiti kazniva dejanja na področju informacijske varnosti v Sloveniji. Prav tako bom proučil najpogostejšo kibernetsko kriminaliteto, povezano z informacijsko varnostjo.

Cilj diplomskega dela je:

- Ugotoviti in proučiti najpogostejšo kibernetsko kriminaliteto,
- Ugotoviti in proučiti vrste kibernetske kriminalitete,

- Proučiti zakonodajo na področju informacijske varnosti v Sloveniji,
- Podati zaključke glede na proučeno tematiko.

## *1.2 Opredelitev predpostavk*

V diplomskem delu smo potrdili oz. ovrgli naslednje hipoteze:

H1 – Informacijska varnost v Sloveniji je neustrezna saj posvečamo temu premalo pozornosti oziroma nismo dovolj ozaveščeni kakšna nevarnost nam preti na svetovnem spletu.

H2 – Najpogostejša računalniška kriminaliteta je vdor v informacijski sistem saj je povezan z velikim številom kaznivih dejanj kot so tatvine premoženja, zloraba osebnih podatkov, goljufije, zlorabe poslovnih skrivnosti. Pri tem pa v večini primerih storilčeva identiteta ostane zelo dobro prikrita.

H3 – Število kaznivih dejanje se iz leta v leto povečuje saj je računalnik postal nujno delovno sredstvo v delovnih procesih, katerega uporablja vse več ljudi. Pri tem se iz leta v leto znanje iz področja informatike vse bolj izboljšuje, kar pa nekateri zlorabijo za dosego svojih lastnih nelegalnih interesov.

## *1.3 Metoda dela*

V diplomskem delu nameravamo uporabiti deskriptivni pristop in naslednje raziskovalne metode:

- metodo deskripcije ali opisovanja,
- metodo kompilacije oziroma pridobivanja informacij iz strokovne literature različnih avtorjev,
- metodo komparacije, ki jo bomo uporabili pri spoznanju, stališčih in mnenjih drugih avtorjev,
- statistično metodo s katero bomo analizirali podatke o kaznivih dejanjih na področju informacijske varnosti v Sloveniji v obdobju 2005-2010.

# 2 Kazniva dejanja na področju informacijske varnosti

Informacijski varnosti v Sloveniji in svetu ne posvečamo dovolj pozornosti, saj se ne zavedamo pomembnosti le te. Uporabniki so prepričani, da jim pri uporabi svojih mobilnih telefonov, prenosnikov, dlančnikov, računalnikov ne proti nobena grožnja, zato jih zaščitijo z slabimi gesli ali pustijo nenadzorovane.

Kazniva dejanja ki so povezana z informacijskimi sistemi in kibernetsko kriminaliteto ne moremo metati v isti koš. Pri Informacijski komunikacijski tehnologiji (IKT) kot mobilni telefon lahko storilec zlorabi osebne podatke ali preko IKT sistemov prihaja do raznih goljufij ali zlorab.

Z uporabo informacijskih sistemov (IS) kot so prenosnik ali računalnik, ki sta povezana z internetom kot množičnim medijem in je del kibernetskega prostora in ga storilec lahko zlorabi iz velike razdalje ob hitrem pretoku informacij.

Ko se je začela informacijska tehnologija razvijati, z razmejitvijo kibernetsko kriminaliteto ni bilo kakšnega problema, kar danes ne drži več. Z razvojem na tem področju se pojavlja vedno več vrst kaznivih dejanj, ki pa seveda iz dneva v dan spreminjajo svojo obliko. Zato je potrebno svoje informacije ustrezno zavarovati, tako informacijsko komunikacijsko tehnologijo, kot informacijske sisteme.

Kazniva dejanja se razlikujejo po tem, proti komu so naperjena, v kakšni obliki se pojavljajo in po specifiki kaznivega dejanja, ki je bila storjena. Te razmejitve niso pomembne le za lažje razumevanje ampak tudi za to, da se za vsako specifično pojavno obliko in vrsto kibernetske kriminalitete v pravnih aktih določijo sankcije in načini pregona. Pojavi pa se problem, saj je treba za vsako pojavno obliko izobraziti organe pregona za uspešno zoperstavljenje storilcem kaznivih dejanj.

# 3 Informacijska varnost v Sloveniji

Informacijska varnost se ukvarja z varovanjem podatkov in informacijskih sistemov pred nezakonitim dostopom, uporabo, razkritjem, ločitvijo, spremembo ali uničenjem. Izrazi informacijska varnost, računalniška varnost in varnost informacij se pogosto uporabljajo kot sinonimi. Kljub temu, da so ta področja v medsebojnem odnosu in si delijo skupne cilje varstva zaupnosti, neokrnjenosti in razpoložljivosti informacij, obstajajo med njimi komaj opazne razlike glede vidika, s katerega pristopajo k tem ciljem in glede načinov zagotavljanja le-teh (Lušenc, 2010).

Informacijska varnost je sistem zagotavljanja varnosti vseh informacij ne glede na njihovo obliko (na papirju, v elektronski obliki ali v glavah zaposlenih). Varnost informacij pomeni, da so celovite in pravilne ter te dostopne samo pooblaščenim uporabnikom. Zato pomeni varstvo pred izgubo (naravna nesreča, okvara, nenamerno uničenje) in nepooblaščeno spremembo ali dostopom (vdorom).

Belič (1999) informacijsko varnost opredeljuje kot stanje, v katerem so podatek, informacija in znanje, shranjeni v informacijskem sistemu, varni pred nepooblaščenimi dostopi, izgubo ali spremembo.

## *3.1 Sistem za upravljanje informacijske varnosti*

Organizacija, ki želi v svojem okolju vzpostaviti želen nivo informacijske varnosti, mora vzpostaviti ustrezen *sistem za upravljanje informacijske varnosti* – SUIV, (angl. information security management system – ISMS). SUIV v organizaciji mora temeljiti na procesnem pristopu »planiraj-uvedi-kontroliraj-korigiraj«, ki ga uvaja standard ISO/IEC 27001.

## *3.2 Vzpostavitev sistema upravljanje informacijske varnosti v organizaciji*

Dandanes je poslovanje v organizacijah v veliki meri podprto z informacijskim sistemom. Učinkovitost izvede poslovnih procesov je pogojena z zadovoljivim

delovanjem informacijskega sistema, saj njegovo nedelovanje ali okrnjeno delovanje pogosto vodi v prekinitev izvajanja ključnih poslovnih procesov organizacije. Posledice tega dogodka so lahko za organizacijo kritične in povezane z visokimi stroški. Organizacija, ki želi zagotoviti kontinuirano in ekonomično izvajanje svojih poslovnih procesov, je primorana poskrbeti za ustrezen nivo varnosti informacijskega sistema. Zagotavljanje varnosti informacijskega sistema v organizaciji je kompleksna aktivnost, ki zahteva sistematičen pristop. Definirati in vzpostaviti je potrebno SUIV[1], ki mora temeljiti na procesnem pristopu »planiraj-uvedi-kontroliraj-korigiraj«. Vzpostavitev SUIV sestoji iz več faz, pri čemer je potrebno za vsako fazo proučiti aktivnosti, ki jih je potrebno izvesti na različnih nivojih v organizaciji. Cilj uvedbe SUIV je v čim večji meri zmanjšati varnostna tveganja, ki jim je informacijski sistem v organizaciji izpostavljen, in s tem zagotoviti učinkovito poslovanja organizacije.

V skladu s tem procesnim pristopom sestoji vzpostavitev SUIV v organizaciji iz štirih faz:

- *faza: načrt vzpostavitve SUIV,*
- *faza: uvedba SUIV,*
- *faza: vzpostavitev sistema kontrol in nadzorstev nad delovanjem SUIV,*
- *faza: analiza odstopanj SUIV in izvajanje korektivnih ukrepov.*

V nadaljevanju so posamezne faze vzpostavitve SUIV v organizaciji podrobneje opisane. V okviru opisa posamezne faze so podane tudi nekatere smernice in priporočila na podlagi izkušenj iz prakse, ki lahko organizacijam služijo v pomoč za uspešnejšo izvedbo posamezne faze vzpostavitve SUIV.

**Načrt vzpostavitev SUIV**

V tej fazi je potrebno zagotoviti jasno definiranje ciljev in zahtevanega nivoja

[1] Sistem za upravljanje informacijske varnosti

informacijske varnosti. Izhajati je potrebno iz osnovne zahteve, da mora informacijski sistem zagotavljati in podpirati učinkovito izvajanje vseh in še posebej ključnih poslovnih procesov v organizaciji. Natančno in jasno je potrebno opredeliti varnostna tveganja z namenom preprečiti nedelovanje oziroma okrnjeno delovanje informacijskega sistema. Izvedba analize in ocene tveganj je osnova za določitev okvira SUIV. Le-ta je v vsaki organizaciji drugačen.

glede na njeno specifičnost, pomembnost in odvisnost informacijskega sistema za izvajanje poslovnih procesov. Ključni del prve faze vzpostavitve SUIV je izdelava načrta vzpostavitve in, kar je najpomembneje, sprejem in potrditev načrta s strani najvišjega vodstva organizacije.

**Uvedba SUIV**

Na osnovi sprejetega načrta vzpostavitve SUIV sledi njegova uvedba. Krovni dokument izvedbe celotnega projekta vzpostavitve SUIV in vodilo za njegovo uvedbo je politika varovanja podatkov in informacij, ki jo sprejema in potrjuje najvišje vodstvo organizacije. Ker je politika okviren dokument, je potrebno izdelati in potrditi izvedbene dokumente na več nivojih, do najnižjega nivoja, ki zagotavlja operativno izvajanje vseh potrebnih aktivnosti za doseganje želenega nivoja informacijske varnosti. Izvedbeni dokumenti sprejeti na podlagi načrta so osnova za aktivnosti uvajanja SUIV in pomeni informiranje ter izobraževanje vseh zaposlenih kot tudi zunanjih sodelavcev in pogodbenih partnerjev organizacije (Brezavšček in Moškon, 2008).

Uvedba SUIV vključuje naslednje aktivnosti:

- izdelava krovne politike varovanja podatkov in informacij in njena potrditev s strani najvišjega vodstva organizacije,
- izdelava, potrditev in sprejem izvedbenih dokumentov SUIV,
- uvedba SUIV (krovne politike in izvedbenih dokumentov),
- seznanjanje in izobraževanje vseh zaposlenih, zunanjih sodelavcev in pogodbenih partnerjev organizacije, ki pri svojem delu uporabljajo IKT.

**Vzpostavitve sistema kontrol in nadzorstev nad delovanjem SUIV**

Z načrtovanjem kontrol in kontrolnega okolja SUIV je potrebno začeti že v prvi fazi vzpostavitve SUIV. Poleg tega je potrebno skozi celotno strukturo dokumentov, ki obravnavajo zagotavljane informacijske varnosti, definirati kontrole in kontrolno okolje za nadzor nad delovanjem SUIV. Poleg tega je potrebno določiti postopke in odgovorne osebe za izvajanje teh kontrol, kakor tudi nadzor nad delovanjem teh oseb ter zaposlene skozi proces informiranja in usposabljanja s temi kontrolami seznanjati.

**Analiza odstopanj SUIV in izvajanje korektivnih ukrepov**

Zadnja faza vzpostavitve SUIV v organizaciji je analiza odstopanj in izvajanje korektivnih ukrepov. V primeru, da analiza odstopanj pokaže, da v poslovnih procesih organizacije niso ustrezno seznanjeni z zahtevami SUIV, jih ne razumejo ali se ne zavedajo posledic njihovega nespoštovanja, jim je potrebno zagotoviti ustreznejši način informiranja ali dodatno usposabljanje ter določiti postopek za izvedbo sprememb, v kolikor analize pokažejo tako.

Dejstvo je, da si informacijski sistemi v različnih organizacijah izpostavljeni različnim tveganjem s stališča varnosti. S tega vidika mora biti SUIV v organizaciji prilagojen specifičnim zahtevam posamezne organizacije. Po drugi strani pa menimo, da so faze, ki so potrebne za vzpostavitev SUIV v organizaciji, podobne ne glede na velikost in dejavnost organizacije (Brezavšček in Moškon, 2008).

## *3.3 Varnostno nadzorni centri*

VNC[2] je najobčutljivejši in najpomembnejši člen v sistemu tehničnega varovanja, kamor se stekajo alarmna sporočila iz priklopljenih alarmnih sistemov, kjer se jih obdela in shrani ter obvešča ustrezne intervencijske in varnostne službe. Zato je nujno potrebna njegova tehnična dovršenost, varnostna brezhibnost in organizacijska učinkovitost.

Institut za standardizacijo RS je na podlagi pobude SIST TC EAL leta 2005 razglasil slovenski prevod BS 5979:2000 za slovenski standard (Fefer, 2008). Britanski standard je napisan v obliki smernic in priporočil poklicnega kodeksa. V tem poklicnem kodeksu standarda so priporočila za načrtovanje, izgradnjo in opremo kadrovsko zasedenih in nezasedenih VNC-jev, kot tudi za delovanje centrov za sprejem alarma v povezavi s protivlomnimi in protipožarnimi sistemi, video nadzorom, socialnih alarmov, alarmni sistemi za varovanje oseb ter ostalimi nadzornimi službami.

VNC so razdeljeni glede na tip alarmnega signala, kjer se postavitev kvalitetnega VNC že začne pri njegovem načrtovanju, iz česar je razvidna njegova namembnost zgradbe, komunikacij, opreme, delovanja in informacij (Fefer, 2008). Kot so različni tipi stavb za VNC-je, tako tudi ni mogoče določiti vseh potencialnih rešitev. Zatorej so priporočila poklicnega kodeksa le okvirna.

Zakon o zasebnem varovanju, 2003 je stopil v veljavo 2.1.2004 in uvaja, da so slovenski standardi, ki urejajo problematiko VNC-jev. Upravljanje z VNC-jem (2. čl. tega zakona) je upravljanje in stalen fizičen nadzor nad vgrajenimi tehničnimi sistemi in napravami za varovanje premoženja, območja ali varovane osebe, in nadzor s telekomunikacijskimi potmi prenosa alarmnih signalov, ki se opravlja v VNC-ju.

[2] Varnostno nadzorni center

V Sloveniji je bilo 31.3.2008 sedemnajst VNC-jev, ki so pridobili, oziroma so v postopku pridobitve licence za upravljanje z varnostno nadzornim centrom. Pri revizijskem pregledu centrov je bilo ugotovljeno, da dvanajst VNC-jev izpolnjuje vse bistvene zahteve SIST BS5979:2005. Tu in tam sicer obstajajo manjša odstopanja od zahtev standarda, ki pa niso bistvena za delovanje VNC-ja. Pet VNC-jev pa ni imelo ustreznih »backup centrov«, torej ni izpolnjevalo 8.4 člena standarda SIST BS 5979:2005 (Fefer, 2008).

## *3.4 Mehanizmi informacijske varnosti v Sloveniji*

Po mnenju Dunn (2004) lahko k varovanju informacijske infrastrukture in zagotavljanju varnosti pristopimo z več vidikov:

- tehnični: zagotavlja se na tehnični ravni s poudarkom na omrežni varnosti. V tem pogledu se z grožnjami soočimo s tehničnimi sredstvi, kot so požarne pregrade, protivirusna programska oprema, avtentikacijski mehanizmi in ustanovitev CERT[3] in CSIRT[4] skupin. Požarne pregrade si lahko razlagamo kot varnostnika na vratih, kjer ta prepušča le koristen podatkovni promet. Funkcija požarne pregrade je zavračanje in sprejemanje določenega podatkovnega prometa, naloge CERT in CSIRT pa preventivno delovanje,

- na ravni podjetja: informacijsko varnost se tukaj razume predvsem kot zagotavljanje stalnega delovanja, kar pomeni stalen dostop do informacijske infrastrukture in stalno delovanje poslovnih procesov, da bi se doseglo zadovoljivo poslovno delovanje. Sredstva za dosego teh ciljev poleg organizacijskih in človeških dejavnikov vključujejo tudi tiste, ki so bili našteti v zgornji alineji,

- vidik organov pregona: organi pregona vidijo varovanje kritične informacijske infrastrukture predvsem v preganjanju kibernetskega kriminala, kar pokrije zelo širok razpon kaznivih dejanj. Vključuje kršitve avtorskih pravic, računalniške prevare, otroško pornografijo in kršitve mrežne varnosti. Proti

[3] Nacionalni odzivni center za obravnavo incidentov s področja varnosti elektronskih omrežij in informacij
[4] Computer Security Incident Response Team

takšni obliki kriminala se bori na klasičen način, še posebej s sprejemanjem nove zakonodaje in spodbujanjem mednarodnega sodelovanja,

- nacionalno-varnostni: celotna družba je videna kot ogrožena, deluje se na več ravneh (tehnični, zakonodajni, organizacijski ali mednarodni). Akterji vključujejo državne uslužbence različnih organov ter predstavnike zasebnega sektorja in javnosti. Glede na spremenjeno varnostno okolje, po 11. Septembru 2001 se je predlagala vzpostavitev državnih organov, ki so se ukvarjali s problematiko informacijske varnosti, kot so to naredili v več državah (Dunn, 2005).

To so tudi vse države, ki so ustanovile specializirane organe bodisi za varovanje kritične infrastrukture bodisi za informacijsko varovanje. Druge države urejajo to področje tako, da naloge zagotavljanja varnosti vključijo v sklop delovnih nalog že obstoječih ministrstev. Razlog, ki govori v prid vzpostavitvi centralnega organa, je tudi, da je kritična infrastruktura razdeljena med zelo različne akterje, podjetja iz različnih sektorjev in državne institucije. Komunikacija med temi akterji bi bila olajšana, hkrati pa bi ta državna institucija delovala kot povezovalni element (Simčič, 2007).

# 4 Kibernetska kriminaliteta

Kibernetska kriminaliteta je gotovo ena najkompleksnejših oblik kriminala, ki pa se stalno razvija in napreduje, saj je svet postal povsem odvisen od dostopa in izmenjave informacij prek svetovnega spleta, v zadnjih letih pa so se temu pridružila tudi razna socialna omrežja, ki povezujejo prebivalstvo v kibernetskem prostoru. Z novimi možnostmi povezovanja pa so se pojavile tudi nove oblike groženj, ki vplivajo na varnost uporabnika.

Kot navajata Bernik in Prislan (2012) besedna zveza kibernetska kriminaliteta pomeni različne tipe kriminalnih dejanj, med katerimi je večina zares kaznivih, vendar pa prištevamo sem tudi nekatera dejanja, storjena v kibernetskem prostoru, ki (še) niso kazniva po kazenskem zakoniku ali mednarodnih pravnih aktih.

## *4.1 Opredelitev in pojem*

Izraz kibernetska kriminaliteta se uporablja za opis različnih kaznivih dejanj, vključno s kaznivimi dejanji, povezanimi s podatki in računalniškimi sistemi (hekanje); s ponarejanjem in goljufijami (phishing), storjenimi s pomočjo računalnikov; kaznivimi dejanji razpečevanja nedovoljenih vsebin (širjenje otroške pornografije); in s kršenjem avtorskih pravic (razpečevanje piratskih vsebin) (UNODC, Cybercrime, 2010).

Pojem računalniška kriminaliteta je izraz, ki se je najprej pojavljal v normodajnih aktih. Vsa prepovedana dejanja kibernetične kriminalitete so res povezana z računalniki, saj brez računalnika oziroma vsaj dveh računalnikov ni mogoče vzpostaviti njune povezave in s tem generiranja novega polja – virtualnega oziroma kibernetičnega prostora. Kljub temu pa je navedeni termin iz vsebinski in formalnih razlogov neustrezen. Zlasti gre za poimenovanje te vrste kriminalitete po uporabljenem sredstvu, kar običajno ni bila praksa. Kazenskopravna teorija predlaga uporabo pojma kriminaliteta v zvezi z računalniki (*computer-related crime*), ki upošteva dejstvo, da je računalnik »samo orodje v človekovih rokah«, vanjo pa

uvršča vsa kazniva dejanja, pri katerih računalnik nastopa kot orodje ali kot predmet napada, za izvršitev ali poskus izvršitve kaznivega dejanja pa je potrebno določeno znanje iz računalništva ali informatike. Glede na pogoj, da ima storilec določeno znanje iz računalništva (tehnika informatike) ali informatike (uporabna informatika) nekateri predlagajo tudi uporabo pojma kriminaliteta v informatiki.

Najprimernejši pojem za poimenovanje kaznivih dejanj v zvezi z računalniki in njihovimi mrežami je po našem mnenju pojem kibernetična kriminaliteta. Ta pojem upošteva, da gre za kriminaliteto v zvezi z računalniki, ki je storjena v kiber-kulturnem kontekstu (*cyberspace*). Druga pojma, ki se uporabljata za poimenovanje kibernetične kriminalitete sta še internetna kriminaliteta in virtualna kriminaliteta. Prvi pojem se nanaša na globalni internet oziroma medmrežje (www – *world wide web*), drugi pa na nov prostor, nastal s povezavo dveh ali več računalnikov. Pojma sta v uporabi v družboslovnih refleksijah, za uporabo na pravnem področju, zlasti kazenskem, na katerem velja poostroženo načelo zakonitosti (*lex certa*), pa zaradi nedoločnosti nista primerna. Pojem informacijska kriminaliteta je širši od kibernetične kriminalitete, saj poleg računalniške kriminalitete zajema tudi področja brez računalnikov.

Torej lahko kibernetsko kriminaliteto pojmujemo kot kriminaliteto, ki jo sestavljajo kazniva dejanja, pri katerih se informacijska tehnologija (računalnik, tablica, mobilnik) pojavlja kot orodje ali kot predmet napada, za izvršitev ali poskus izvršitve kaznivega dejanja pa je potrebno določeno znanje računalništva ali informatike. »Izraz kibernetska kriminaliteta se nanaša na dejanja, ki so storjena s pomočjo elektronske opreme za obdelavo podatkov in ki povzročijo neželene posledice. Gre za kakršno koli protipravno dejavnost, ki zajema kopiranje, odstranitev, vmešavanje, vdor, uničenje ali drugo manipulacijo z računalniškim sistemom, računalnikom, podatki ali računalniškimi programi« (Završnik v Bernik in Prislan, 2012).

## *4.2 Preiskovanje kibernetskega kriminala*

Podatki v elektronski obliki so dodaten vir dokazov, ki lahko predstavljajo kaznivo dejanje sami po sebi, ali pa so le podaljšek kaznivega dejanja, storjenega v fizičnem svetu (Hinde v Bernik in Prislan, 2012).

To organom pregona prinaša nove izzive pri zaseganju, izločevanju in ravnanju s tovrstnimi podatki oz. dokazi. Storilci za seboj puščajo digitalne sledi, ki pa lahko vodijo v slepo ulico, prav tako je z njimi lahko manipulirati z namenom oviranja preiskave. Zato predstavljajo forenzične preiskave naprav, ki hranijo digitalne podatke, čedalje pomembnejši člen pri preiskavah kaznivih dejanj tako s področja kibernetske kriminalitete kot tudi drugih, klasičnih oblik kriminalitete (Mohay, Byron, De Vel in McKemish v Bernik in Prislan 2012).

Dokazna teorija je predvsem dobro razvita v anglosaškem pravnem prostoru, kjer se pravila o sprejemljivosti dokazov v pravnih postopkih urejata predvsem zakon o pravdnem postopku za civilno pravo ter zakon o kazenskem postopku za kazensko pravo. Posebna podzvrst dokaznega prava so računalniški dokazi oziroma računalniška forenzika.

Berčič (2003) pravi, da je v anglosaškem pravu forenzika razvita kot posebna disciplina, podprta s pravnimi viri, razvoj pri nas na tem področju zaostaja. Razen nekaj določb Zakona o elektronskem poslovanju in elektronskem podpisu, ki govorijo o načelu nediskriminacije elektronskih dokumentov v pravnem prometu (4. čl.) je siceršnja dokazna vrednost elektronskih dokumentov in drugih podatkov na splošno urejena v zakonih o kazenskem in pravdnem postopku. Na splošno velja v celinskem pravu načelo proste presoje dokazov. Gre za splošno načelo, ki sodniku omogoča, ob upoštevanju mnenj izvedencev posamezne stroke, ustvarjalno interpretacijo sprejemljivosti nekega dokaza.

Pri računalniških zapisih ki pa jih je ustvaril človek, bo, podobno kot pri pisnih listinah, sam pri sebi takšen dokaz nespremenljiv, če pa bo avtor zapisa pričal pred

sodiščem in potrdil avtentičnost ter vsebino zapisa ter bil na voljo za navzkrižno zaslišanje, pa bo veljaven. Pri računalniško generiranih zapisih pa se bo postavilo vprašanje njihove zanesljivosti v smislu pravilnega delovanja računalniškega sistema od trenutka njihovega nastanka naprej. Ker so tudi računalniški zapis, ki jih ustvari človek, podvrženi kontaminaciji z možnimi napakami v delovanju sistemske aplikativne programske opreme, je treba pri njih, poleg že zgoraj omenjene nesprejemljivosti gledati tudi na pravilno delovanje sistemske ali aplikativne opreme ves čas njihovega obstoja, od nastanka do uporabe na sodišču (Berčič, 2003).

V kazenskem zakoniku (KZ-1, 2008) so kot kazniva dejanja, ki bi jih lahko šteli med tako imenovana računalniška kazniva dejanja oziroma kazniva dejanja, ki jih je mogoče izvesti s pomočjo računalnika oziroma informacijske tehnologije, opredeljena naslednja ravnanja:

- neupravičeno prisluškovanje in zvočno snemanje (148. člen Kazenskega zakonika, v osnovi ne gre za tako imenovano »računalniško kaznivo dejanje«),
- neupravičeno slikovno snemanje (149. člen Kazenskega zakonika, v osnovi ne gre za tako imenovano »računalniško kaznivo dejanje«),
- kršitev tajnosti občil (2. točka 2. odstavka 150. člena Kazenskega zakonika, v osnovi ne gre za tako imenovano »računalniško kaznivo dejanje«),
- nedovoljena objava zasebnih pisanj (151. člen Kazenskega zakonika, v osnovi ne gre za tako imenovano »računalniško kaznivo dejanje«),
- zloraba osebnih podatkov (drugi odstavek 154. člena Kazenskega zakonika),
- kršitev avtorske pravice (drugi odstavek 158. člena Kazenskega zakonika),
- neupravičena uporaba (prej: izkoriščanje) avtorskega dela (159. člena Kazenskega zakonika),
- kršitev avtorskih in sorodnih pravic (160. člen Kazenskega zakonika, v osnovi ne gre za tako imenovano »računalniško kaznivo dejanje«),
- neupravičen vstop v informacijski sistem (242. člen Kazenskega zakonika),
- izdelovanje in pridobivanje orožja in pripomočkov, namenjenih za kaznivo dejanje (tretji odstavek 309. člena Kazenskega zakonika).

## *4.3 Ovire organov pregona pri preiskovanju kibernetskega kriminala*

Organi pregona se spopadajo z velikimi težavami in izzivi, ki jih povzročajo novi načini komunikacije, naraščajoča sofisticiranost in hiter napredek tehnologije. Tako lahko komunikacijski kanali, ki jih uporabljajo storilci, potekajo po številnih in raznovrstnih tehnologijah, kot so fiksna telefonija, lokalni ali mednarodni ponudniki teh tehnologij, brezžične in satelitske povezave. Prav tako lahko potekajo skozi številne države z različnimi časovnimi območji in pravnimi sistemi. Vse te možnosti ovirajo organe pregona pri sledenju in odkrivanju storilcev. Storilci lahko uporabljajo kar nekaj poti, da zakrijejo svojo identiteto in zmanjšajo možnost odkritja. Nekatere metode zahtevajo dokaj visoko stopnjo znanja in tehničnih spretnosti, z večino pa se storilci lahko seznanijo med viri, ki so prosto dostopni na internetu. Nekatere pogoste metode so posredovanje izmišljenih ali ukradenih osebnih podatkov ob registraciji pri ponudniku priklopa v internet, uporaba anonimne elektronske pošte, predhoden vdor v enega ali več strežnikov, iz katerih nato opravljajo svoje dejavnosti, uporaba anonimnih strežnikov, ki ne posredujejo naprej podatkov o uporabniku (predvsem naslovov IP) in ponareditev podatkov o naslovu IP, elektronski pošti, spletni strani. V kibernetski kriminaliteti danes govorimo o virtualnih lokacijah, med katerimi se selijo storilci in s tem izogibajo pravnim sankcijam in ukrepanju organov pregona (Završnik, 2005).

Spletne strani, na katerih opravljajo svoje protipravne dejavnosti (razširjanje otroške pornografije, nelegalna prodaja avtorskih del idr.) največkrat postavijo na strežnike v državah s pomanjkljivo zakonodajo, brez mednarodnih sporazumov in z manj usposobljenimi organi pregona. Takšna problematična območja so predvsem Južna Amerika, Afrika ter še nekatere slabše razvite države vzhodne Evrope in nekdanje Sovjetske zveze (Bernik in Prislan, 2012).

Od leta 1995 deluje vladni center za obveščanje, spremljanje in ukrepanje v okviru javnega zavoda Arnes[5], ki opravlja vlogo nacionalnega centra CERT. SI-CERT sprejema prijave incidentov za vsa omrežja v Sloveniji in pri razreševanju sodeluje tako z

[5] Akademska in raziskovalna mreža Slovenije

operaterji, ponudniki informacijskih storitev in policijo. Omrežje za sisteme v javni upravi je na drugi strani posebej pomemben del informacijske strukture države, ki zahteva posebno načrtovanje in upravljanje, zato je smiselno ustanoviti ločeno službo, ki se bo lahko učinkovito spopadla z obravnavo varnostnih incidentov na tej infrastrukturi. Večletni program Evropske unije z naslovom »Odprta in varna Evropa, ki služi državljanom in jih varuje« (tako imenovani Stockholmski program, UL C št. 115 z dne 4. maja 2010, str. 1) v poglavju 4.4.4 na str. 47 poziva države članice, naj »v celoti podpirajo nacionalne portale za obveščanje, ki delujejo na področju boja proti kibernetski kriminaliteti,« ter poudarja, da je »treba sodelovati z državami zunaj Evropske unije«. Hkrati opredeljuje, da bi morala »Unija spodbujati politike in zakonodajo, ki zagotavljajo zelo visoko raven varnosti omrežja in omogočajo hitrejši odziv v primeru kibernetskih motenj ali kibernetskega napada«. Prav tako je Evropski svet na zasedanju 25. in 26. marca 2010 sprejel Strategijo o notranji varnosti EU; v njej je na strani 14 kot grožnja notranji varnosti opredeljen tudi kibernetski kriminal. Na podlagi tega je Evropska komisija pripravila akcijski načrt za izvajanje strategije notranje varnosti EU (stran 9 priloženega dokumenta), v katerem so določeni nosilci v EU in roki za izvedbo. Ključni deli tega akcijskega načrta so:

- da bo EU do leta 2013 ustanovila center za kibernetsko kriminaliteto, države pa bodo morale do leta 2013 vzpostaviti svoje centre na nacionalni ravni ali v partnerstvu z drugimi državami članicami. Ti centri naj bi med drugim tesno sodelovali tudi z akademskimi krogi in industrijo,

- države članice bi morale zagotoviti, da državljani enostavno dostopajo do navodil v zvezi s kibernetskimi grožnjami in osnovnimi varnostnimi ukrepi, ki jih je treba izvesti. Ta navodila bi morala vsebovati informacije o tem, kako zavarovati svojo zasebnost na spletu, kako odkrivati in sporočati primere navezovanja stikov, kako na računalnike namestiti osnovno protivirusno programsko opremo in požarne zidove, kako upravljati gesla ter odkrivati lažno predstavljanje (phishing), zvabljanje (pharming) in druge napade,

- sodelovanje med javnim in zasebnim sektorjem je na evropski ravni treba okrepiti in razvijati inovativne ukrepe in instrumente za izboljšanje varnosti, tudi v zvezi s kritično infrastrukturo, ter odpornost omrežne in informacijske infrastrukture. Evropsko javno-zasebno partnerstvo za odpornost bi moralo sodelovati tudi z mednarodnimi partnerji, da se izboljša svetovno obvladovanje tveganj v omrežjih IT,

- proti nezakonitim internetnim vsebinam – vključno s spodbujanjem k terorizmu – bi bilo treba ukrepati s smernicami za sodelovanje na podlagi postopkov za prijavo in odstranjevanje, skupaj s ponudniki internetnih storitev, organi kazenskega pregona in neprofitnimi organizacijami,

- za krepitev stikov in interakcij med navedenimi zainteresiranimi stranmi bo Evropska komisija spodbujala uporabo spletne platforme proti kibernetski kriminaliteti za industrijo in kazenski pregon,

- za izboljšanje preprečevanja in odkrivanja kibernetskih napadov ali motenj ter hitro reagiranje nanje bi vsaka država članica morala vzpostaviti dobro delujočo skupino za odzivanje na računalniške grožnje. Ta skupina bi sodelovala z organi kazenskega pregona pri preprečevanju in odzivanju. Države članice bi morale povezati svoje nacionalne/vladne skupine za odzivanje na računalniške grožnje. To bo ključnega pomena pri razvoju evropskega sistema za izmenjavo informacij in opozarjanje (EISAS) širše javnosti do leta 2013 ob podpori Komisije in Evropske agencije za varnost omrežij in informacij (ENISA) ter pri vzpostavitvi mreže kontaktnih točk med zadevnimi organi in državami članicami. Države članice bi morale pripraviti nacionalne načrte ukrepov ter na nacionalni in evropski ravni redno izvajati vaje za odzivanje na incidente in za odpravo posledic.

Prav tako bodo na Svetu Evrope sprejete prednostne naloge EU v boju proti organiziranemu kriminalu 2011–2013 (Sklepi Sveta o določitvi prednostnih nalog EU v boju proti organiziranemu kriminalu za obdobje med letoma 2011 in 2013), na podlagi katerih bodo države članice okrepile svoje dejavnosti v boju proti kibernetski kriminaliteti in kriminalni zlorabi intraneta s strani organiziranih kriminalnih skupin. V ta namen namerava Europol leta 2013 vzpostavil Center za kibernetsko kriminaliteto (Resolucija o nacionalnem programu preprečevanja in zatiranja kriminalitete, 2012).

# 5 Zakonodaja za področje informacijske varnosti v Sloveniji

Vidike omrežne in informacijske varnosti obravnavajo različni zakoni. Slovenija kot pravna država pri obravnavi kaznivih dejanj s področja informacijskih sistemov nikakor ne more mimo pravne ureditve sprejete v Evropski uniji in pravne ureditve sprejete v Republiki Sloveniji. Slovenija je z vstopom v Evropsko unijo zraven svoje pravne ureditve sprejela tudi evropsko, Konvencijo o kibernetskem kriminalu, ki obravnava kazniva dejanja na področju informacijskih sistemov.

Kazenski zakonik (2008) recimo opredeljuje kazniva dejanja (kot je recimo vdor v poslovni informacijski sistem), Zakon o elektronskih komunikacijah (2004) definira dolžnosti in nadzor nad delom operaterjev, medtem ko Zakon o elektronskem poslovanju na trgu (2006) širše opredeljuje delovanje vseh ponudnikov storitev. Zakon o elektronskem poslovanju in elektronskem podpisu (2000) opredeljuje, kdaj so elektronsko podpisani dokumenti enakovredni ročno podpisanim pogodbam in vloge overiteljev.

## *5.1 Kazenski zakonik (KZ-1) RS*

Na tem področju kazenski zakonik ureja: **Zlorabo osebnih podatkov, 143. člen (KZ-1, 2008)**

1. Kdor uporabi osebne podatke (Zloraba osebnih podatkov, 143. člen Kazenskega zakonika), ki se obdelujejo na podlagi zakona, v neskladju z namenom njihovega zbiranja ali brez osebne privolitve osebe, na katero se osebni podatki nanašajo, se kaznuje z denarno kaznijo ali zaporom do enega leta.
2. Enako se kaznuje, kdor vdre ali nepooblaščeno vstopi v računalniško vodeno zbirko podatkov z namenom, da bi sebi ali komu drugemu pridobil kakšen osebni podatek.

3. Kdor na svetovnem medmrežju objavi ali omogoči drugemu objavo osebnih podatkov žrtev kaznivih dejanj, žrtev kršitev pravic ali svoboščin, zaščitenih prič, ki se nahajajo v sodnih spisih sodnih postopkov, kjer po zakonu ali po odločitvi sodišča ni dovoljena prisotnost javnosti ali identifikacija žrtev ali zaščitenih prič ter osebnih zapisov o njih v zvezi s sodnim postopkom, na podlagi katerih se te osebe lahko določi ali so določljive, se kaznuje z zaporom do treh let.

4. Kdor prevzame identiteto druge osebe in pod njenim imenom izkorišča njene pravice, si na njen račun pridobiva premoženjsko korist ali prizadene njeno osebno dostojanstvo, se kaznuje z zaporom od treh mesecev do treh let.

5. Če stori dejanje iz prejšnjih odstavkov tega člena uradna oseba z zlorabo uradnega položaja ali uradnih pravic, se kaznuje z zaporom do petih let.

6. Pregon iz tretjega odstavka tega člena se začne na predlog (KZ-1, 2008).

Varstvo osebnih podatkov je zagotovljeno že v Ustavi Republike Slovenije (1991), ki v 38. členu prepoveduje uporabo osebnih podatkov v nasprotju z namenom njihovega zbiranja ter določa, da zbiranje, obdelovanje, namen uporabe, nadzor in varstvo tajnosti osebnih podatkov določa zakon. Določeno je tudi, da ima vsakdo pravico seznaniti se z osebnimi podatki, ki se nanašajo nanj in pravico do sodnega varstva ob njihovi zlorabi.

Z Zakonom o varstvu osebnih podatkov (ZVOP-1-UPB-1, 2004) se določajo pravice, obveznosti, načela in ukrepi, s katerimi se preprečujejo neustavni, nezakoniti in neupravičeni posegi v zasebnost in dostojanstvo posameznika oziroma posameznice (v nadaljnjem besedilu: posameznik) pri obdelavi osebnih podatkov.

Pomen izrazov je opredeljen v 3. točki 6. čl. tega zakona, ki pravi:

da obdelava osebnih podatkov pomeni kakršnokoli delovanje ali niz delovanja, ki se izvaja z osebnimi podatki, ki so avtomatizirano obdelani ali ki so pri ročni obdelavi del zbirke osebnih podatkov ali so namenjeni vključitvi v zbirko osebnih podatkov, zlasti zbiranje, pridobivanje, vpis, urejanje, shranjevanje, prilagajanje ali

spreminjanje, priklicanje, vpogled, uporaba, razkritje s prenosom, sporočanje, širjenje ali drugo dajanje na razpolago, razvrstitev ali povezovanje, blokiranje, anonimiziranje, izbris ali uničenje; obdelava je lahko ročna ali avtomatizirana (sredstva obdelave). Zakon ne določa »numerus clausus« dejanj, ki pomenijo obdelovanje osebnih podatkov, pač pa z uporabo besede »zlasti« le primeroma našteva možne oblike obdelovanja, tako da tudi kakršno koli drugo ravnanje z osebnimi podatki, pomeni njihovo obdelovanje. Tako se šteje, da je tudi nepooblaščen vstop v zbirko podatkov in njihovo kopiranje obdelava osebnih podatkov.

Splošna pravila o odgovornosti so opisana v 8. čl. tega zakona, ki pravi:

- Osebni podatki se lahko obdelujejo le, če obdelavo osebnih podatkov in osebne podatke, ki se obdelujejo, določa zakon ali če je za obdelavo določenih osebnih podatkov podana osebna privolitev posameznika.
- Namen obdelave osebnih podatkov mora biti določen v zakonu, v primeru obdelave na podlagi osebne privolitve posameznika pa mora biti posameznik predhodno pisno ali na drug ustrezen način seznanjen z namenom obdelave osebnih podatkov.

Ker je v skladu z 19. čl. ZVOP-1 dolžnost upravljavca osebnih podatkov, da posameznika obvešča o obdelavi osebnih podatkov, ga je seveda potrebno obveščati tudi v primeru, če je osebne podatke obdelovala nepooblaščena oseba. Navedeno izhaja tudi 5. točke 24. čl. in iz 3. odst. 22. čl. ZVOP-1, ki upravljavcu osebnih podatkov nalaga, da mora za vsako posredovanje osebnih podatkov zagotavljati t.i. sledljivost. To pomeni, da mora zagotoviti, da je mogoče pozneje ugotoviti, kateri osebni podatki so bili posredovani, komu, kdaj in na kakšni podlagi, in sicer za obdobje, ko je mogoče zakonsko varstvo pravice posameznika zaradi nedopustnega posredovanja osebnih podatkov.

Na tem področju kazenski zakonik ureja: **Napad na informacijski sistem, 221. člen (KZ-1, 2008)**

1. Kdor vdre v informacijski sistem ali kdor neupravičeno prestreže podatek ob nejavnem prenosu v informacijski sistem ali iz njega (Napad na informacijski sistem, 221. člen Kazenskega zakonika), se kaznuje z zaporom do enega leta.

2. Kdor podatke v informacijskem sistemu neupravičeno uporabi, spremeni, preslika, prenaša, uniči ali v informacijski sistem neupravičeno vnese kakšen podatek, ovira prenos podatkov ali delovanje informacijskega sistema, se kaznuje za zaporom do dveh let.

3. Poskus dejanja iz prejšnjega odstavka je kazniv.

4. Če je z dejanjem iz drugega odstavka tega člena povzročena velika škoda, se storilec kaznuje z zaporom od treh mesecev do petih let.

**Vdor v poslovni informacijski sistem, 237. člen (KZ-1, 2008)**

1. Kdor pri gospodarskem poslovanju neupravičeno uporabi, spremeni, preslika, prenaša, uniči ali v informacijski sistem vnese kakšen svoj podatek, ovira prenos podatkov ali delovanje informacijskega sistema ali kako drugače vdre v informacijski sistem (Vdor v poslovni informacijski sistem, 237. člen Kazenskega zakonika), da bi sebi ali komu drugemu pridobil protipravno premoženjsko korist ali drugemu povzročil premoženjsko škodo, se kaznuje z zaporom do treh let.

2. Če je bila z dejanjem iz prejšnjega odstavka pridobljena velika premoženjska korist ali povzročena velika premoženjska škoda in je storilec hotel sebi ali komu drugemu pridobiti tako premoženjsko korist ali drugemu povzročiti tako premoženjsko škodo, se kaznuje z zaporom do petih let.

**Izdelovanje in pridobivanje orožja in pripomočkov, namenjenih za kaznivo dejanje, 306. člen (KZ-1, 2008)**

1. Kdor orožje, razstrelilne snovi ali pripomočke, s katerimi se lahko napravijo, ali strupe, za katere ve, da so namenjeni za kaznivo dejanje, izdela ali si jih pridobi ali jih hrani ali komu omogoči, da pride do njih (Izdelovanje in pridobivanje orožja in pripomočkov, namenjenih za kaznivo dejanje, 306. člen Kazenskega zakonika), se kaznuje z zaporom do treh let.

2. Kdor napravi ali komu odstopi ponarejen ključ, odpirač ali kakšen drug pripomoček za vlom, čeprav ve, da je namenjen za kaznivo dejanje, se kaznuje z zaporom do enega leta.

3. Enako kot v prejšnjem odstavku se kaznuje, kdor z namenom storitve kaznivega dejanja poseduje, izdeluje, prodaja, daje v uporabo, uvaža, izvaža ali kako drugače zagotavlja pripomočke za vdor ali neupravičen vstop v informacijski sistem.

### 5.1.1 Zakon o elektronskih komunikacijah

Zakon o elektronskih komunikacijah (ZEKom-UPB1-1, 2007) med drugim opredeljuje dolžnosti operaterjev, ki zagotavljajo delovanje komunikacijskih omrežij. ZEKom-UPB-1 v X. poglavju in ZEKom-1 v XII. in XIII. poglavju obravnavajo »zaščito tajnosti, zaupnosti in varnosti elektronskih komunikacij ter hrambo podatkov o prometu«. Zakon določa, da mora operater ustrezno skrbeti za varnost omrežja in storitev, kako mora skrbeti za zaupnost komunikacij, katere prometne podatke mora hraniti in na kakšen način ter kdaj in pod kakšnimi pogoji mora omogočiti prestrezanje komunikacije.

### 5.1.2 Zakon o elektronskem poslovanju na trgu

ZEPT (2006) »določa način in obseg elektronskega poslovanja na trgu,« s stališča informacijske varnosti pa so v njem pomembni členi, ki opredeljujejo odgovornost ponudnika storitve ali gostiteljstva za podatke, ki so preko omrežja dostopni.

Splošna pravila o odgovornosti ponudnikov posredovalnih storitev so opisana v 8. čl. tega zakonika, ki pravi:

- Ponudnik storitev odgovarja za podatke, ki jih zagotovi prejemnik njegove storitve, po določbah tega zakona.

- Ponudnik storitev odgovarja za podatke, ki jih za opravljanje storitve informacijske družbe zagotovi sam, po splošnih pravilih obligacijskega in kazenskega prava.

- Ponudnik storitev ni dolžan nadzirati ali hraniti podatkov, ki jih pošilja ali hrani, ali dejavno raziskovati okoliščin, nakazujočih na protipravnost podatkov, ki jih zagotavlja prejemnik storitve.

- Ponudniki storitev morajo vsem pristojnim organom na njihovo zahtevo najkasneje v roku treh dni od njenega prejema sporočiti podatke, na podlagi katerih je mogoče identificirati prejemnike njihove storitve (ime in priimek, naslov, firma, elektronski naslov). Navedene podatke morajo ponudniki storitev sporočiti zaradi odkrivanja in preprečevanja kaznivih dejanj na podlagi odredbe sodišča, brez odredbe sodišča pa, če tako določa področni zakon.

Odgovornost ponudnika storitev izključnega prenosa je opisana v 9. čl., ki pravi:

- Kadar se storitev informacijske družbe nanaša na prenos podatkov v komunikacijskem omrežju, ki jih zagotovi prejemnik storitve, ali zagotovitev dostopa do komunikacijskega omrežja prejemniku storitve, ponudnik storitev ni odgovoren za poslane podatke, če:

  - ne sproži prenosa podatkov
  - ne izbere naslovnika in
  - podatkov, ki jih prenaša, ne izbere ali spremeni.

- Prenos in zagotovitev dostopa iz prejšnjega odstavka vključujeta samodejno, vmesno in prehodno shranjevanje poslanih podatkov, če je namenjeno samo izvajanju prenosa v komunikacijskem omrežju in če se podatki ne shranijo za daljši čas, kolikor je za njihov prenos upravičeno potrebno.

- Sodišče lahko ponudniku storitve naloži ustavitev ali preprečitev kršitve. Ne glede na izključitev odgovornosti ponudnikov storitev iz prvega odstavka tega člena, pa jim lahko sodišče odredi odstranitev nezakonitih vsebin ali onemogočanje dostopa do njih zaradi odkrivanja in preprečevanja kaznivih dejanj, varstva zasebnosti, varovanja tajnih podatkov in poslovne tajnosti. Takšen predlog lahko sodišču v javnem interesu posredujejo tudi za nadzor pristojni upravni organi, skladno s področno zakonodajo.

Zakon v 10. čl. govori o odgovornosti ponudnika storitev shranjevanja v predpomnilniku in navaja:

- Kadar se storitev informacijske družbe nanaša na prenos podatkov v komunikacijskem omrežju, ki jih zagotovi prejemnik storitve, ponudnik storitev ni odgovoren za samodejno, vmesno in prehodno shranjevanje teh podatkov, če je namenjeno izključno učinkovitejšemu posredovanju podatka drugim prejemnikom storitve na njihovo zahtevo, pod pogojem, da ponudnik storitev:
  - podatkov ne spremeni,
  - ravna v skladu s pogoji za dostop do podatkov,
  - ravna v skladu s pogoji o sprotnem dopolnjevanju podatkov, ki so določeni v splošno priznanih in uporabljenih industrijskih standardih,
  - ne posega v zakonito uporabo tehnologij za pridobivanje informacij o rabi podatkov, ki so določene v splošno priznanih in uporabljenih industrijskih standardih in
  - brez odlašanja odstrani ali onemogoči dostop do podatka, ki ga hrani, takoj ko je obveščen, da je bil vir podatka odstranjen iz omrežja ali da je bil dostop do njega onemogočen ali da je sodišče ali upravni organ odredil njegovo odstranitev ali omejitev.
- Sodišče lahko ponudniku storitve naloži ustavitev ali preprečitev kršitve. Ne glede na izključitev odgovornosti ponudnikov storitev iz prejšnjega odstavka, pa jim lahko sodišče odredi odstranitev nezakonitih vsebin ali onemogočanje dostopa do njih zaradi odkrivanja in preprečevanja kaznivih dejanj, varstva zasebnosti, varovanja tajnih podatkov in poslovne tajnosti. Takšen predlog lahko sodišču v javnem interesu posredujejo tudi za nadzor pristojni upravni organi, skladno s področno zakonodajo.

Zakon v svojem 11. čl. obravnava odgovornost ponudnika storitev gostiteljstva:

- Kadar se storitev informacijske družbe nanaša na shranjevanje podatkov, ki jih zagotovi prejemnik storitve, ponudnik storitev ni odgovoren za podatke, ki

jih je shranil na zahtevo prejemnika storitve, ki ne deluje v okviru njegovih pooblastil ali pod njegovim nadzorom, pod pogojem, da ponudnik storitev:

- ne ve za protipravno dejavnost ali podatek in mu v zvezi z odškodninsko odgovornostjo niso znana dejstva ali okoliščine, iz katerih izhaja protipravnost, ali
- nemudoma, ko mu je protipravnost znana, ukrepa tako, da podatke odstrani ali onemogoči dostop do njih.
- Sodišče lahko ponudniku storitve naloži ustavitev ali preprečitev kršitve. Ne glede na izključitev odgovornosti ponudnikov storitev iz prejšnjega odstavka, pa jim lahko sodišče odredi odstranitev nezakonitih vsebin ali onemogočanje dostopa do njih zaradi odkrivanja in preprečevanja kaznivih dejanj, varstva zasebnosti, varovanja tajnih podatkov in poslovne tajnosti. Takšen predlog lahko sodišču v javnem interesu posredujejo tudi za nadzor pristojni upravni organi, skladno s področno zakonodajo.

### 5.1.3 Zakon o elektronskem poslovanju in elektronskem podpisu

ZEPEP (2000 ) ureja elektronsko poslovanje, ki zajema poslovanje v elektronski obliki z uporabo informacijske in komunikacijske tehnologije in uporabo elektronskega podpisa v pravnem prometu, kar vključuje tudi elektronsko poslovanje v sodnih, upravnih in drugih podobnih postopkih. S tem zakonom se uvaja enakovrednost elektronskega in lastnoročnega podpisa na dokumentih, kadar so izpolnjeni nekateri pogoji.

Elektronskemu podpisu se ne sme odreči veljavnosti ali dokazne vrednosti samo zaradi elektronske oblike, ali ker ne temelji na kvalificiranem potrdilu ali potrdilu akreditiranega overitelja, ali ker ni oblikovan s sredstvom za varno elektronsko podpisovanje (14. čl. ZEPEP).

Varen elektronski podpis, overjen s kvalificiranim potrdilom, je glede podatkov v elektronski obliki enakovreden lastnoročnemu podpisu ter ima zato enako veljavnost in dokazno vrednost (15. čl. ZEPEP).

## *5.2 Konvencija o kibernetski kriminaliteti*

V Sloveniji je Konvencija o kibernetski kriminaliteti eden od normativnih aktov, ki se nanaša na področje boja proti kibernetski kriminaliteti. Na nivoju države pa to področje urejajo Zakon o kazenskem postopku in njegove spremembe ter dopolnitve, Kazenski zakonik RS, Zakon o varstvu osebnih podatkov in Zakon o elektronskem poslovanju. Težava konvencije in Kazenskega zakonika je pomanjkljivost, da ob dokumenta opredeljujeta posamezne oblike kibernetske kriminalitete, medtem ko povezanih napadov ne predvidevata (Bernik in Prislan, 2011).

Konvencijo o kibernetski kriminaliteti je 8.11.2001 sprejel Svet Evrope (konvencijo in poročilo Explanatory Report, v katerem so razloženi posamezni pojmi, ki jih vsebuje konvencija). Slovenija je ratificirala konvencijo in pripadajoče dokumente, na osnovi katerih je potem državni zbor sprejel novo dikcijo kaznivega dejanja neupravičenega vstopa v informacijski sistem.

Omenjena konvencija je prvi mednarodni pravni akt, ki sodobno kibernetsko kriminaliteto obravnava z vidika priporočil, ki naj jih podpisnice upoštevajo pri oblikovanju in reformi svojega notranjega prava, in je vir strategij za boj proti kibernetski kriminaliteti.

Namen konvencije je bil (Council of Europe, 2001):

- harmonizirati nacionalne kazenskopravne zakonodaje,
- ponuditi kazensko procesna pooblastila, ki so potrebna za odkrivanje in pregon tovrstne kriminalitete,
- vzpostaviti hiter in učinkovit režim mednarodnega sodelovanja, kar je razvidno tudi iz same strukture.

Konvencija obsega štiri poglavja:

1. v prvem poglavju so opredeljeni osnovni izrazi, kot so računalniški sistem, računalniški podatki, ponudnik storitev in podatki o prometu,

2. drugo poglavje opredeljuje ukrepe, ki jih je treba sprejeti na državni ravni, in v prvem oddelku nastavlja kazensko materialno pravo, kjer opredeljujejo vrsto kibernetičnih kaznivih dejanj ter jih razvršča v štiri skupine:

   - v prvi skupini kaznivih dejanj zoper zaupnost, celovitost in dostopnost računalniških podatkov in sistemov so kazniva dejanja (protipravnega dostopa, protipravnega prestrezanja, motenja podatkov, motenja sistemov in zlorabe naprav),

   - drugo skupino sestavljata dejanji, povezani z računalnikom. To sta: računalniško ponarejanje in računalniške goljufije,

   - tretja skupina je namenjena za kazniva dejanja, povezana s sporno vsebino. Gre za: kazniva dejanja povezana z otroško pornografijo, kazniva dejanja razširjanja rasističnega in ksenofobičnega gradiva v računalniških sistemih, rasistične in ksenofobične žalitve ter zanikanja, hujša zmanjševanja pomena, odobravanja ali zagovarjanja genocida ali hudodelstev zoper človečnost,

   - četrto skupino sestavljajo kazniva dejanja, povezana s kršitvijo avtorske in sorodnih pravic. Sem spadajo kazniva dejanja, povezana s kršitvijo avtorske in sorodnih pravic.

Drugi odstavek drugega poglavja opisuje določene proceduralne ukrepe, ki jih morajo uvesti nacionalne države za učinkovito zaščito, odkrivanje in pregon storilcev kibernetične kriminalitete, tretji oddelek pa govori o sodni pristojnosti oziroma ureja vprašanje jurisdikcije (Council of Europe, 2001):

3. tretje poglavje vsebuje vrsto določb, ki se nanašajo na mednarodno sodelovanje (izročitev in medsebojno pomoč),

4. v četrtem poglavju so končne določbe.

# 6 Rezultati raziskave

V uvodnem delu sem si zastavil tudi tri raziskovalne hipoteze, ki jih sedaj na podlagi analize in proučenosti lahko potrdim ali zavržem.

**H1 - Informacijska varnost v Sloveniji je neustrezna.**

Hipotezo 1, da je informacijska varnost v Sloveniji neustrezna lahko potrdim, saj uporabniki internetnih storitev niso ozaveščeni kakšne nevarnosti prežijo pri uporabi le-tega, prav tako se pa število uporabnikov povečuje.

**H2 - Najpogostejša računalniška kriminaliteta je vdor v informacijski sistem**

Hipotezo 2, da je najpogostejša računalniška kriminaliteta vdor v informacijski sistem lahko potrdim, saj danes poslovanje brez uporabe interneta ni več mogoča, kar pa storilci izrabljajo za izvajanje svojih dejavnosti, katerih edini cilj pa je pridobitev protipravnega premoženja.

**H3 – Število kaznivih dejanje se iz leta v leto povečuje**

Hipotezo 3, da se število kaznivih dejanj iz leta v leto povečuje lahko potrdim, saj vedno več uporabnikov internetnih storitev, ki računalnik uporabijo kot sredstvo za storitev kaznivih dejanj in s katerim želijo priti do hitrega zaslužka. Prav tako je z uporabo interneta mogoč zelo hiter dostop do informacij in prenos le-teh. K temu je pa bistveno pripomogla svetovna kriza, saj je vedno več nezaposlenih, ki se posledično odločijo za tako dejavnost in splošne dostopnosti orodij ter znanja.

## *6.1 Zbiranje podatkov*

Podatke za statistično obdelavo podatkov sem pridobil preko letnih poročil Policije za proučena leta.

V teoretičnem delu diplomskega dela posamezni članki in raziskave potrjujejo hipotezo, ki pravi, da je Neupravičen vstop v informacijski sistem oz. Napad na informacijski sistem ena od najpogostejših oblik kibernetskega kriminala. Potencialne

nevarnosti se stopnjujejo, saj bliskoviti razvoj tehnologije in lahka dostopnost do informacij omogoča tudi druge vrste kibernetske kriminalitete. V zadnjih letih je k porastu tovrstnih kaznivih dejanj pripomogla tudi svetovna kriza, saj se vse več izobraženih ljudi odloča za takšna dejanja, bodisi zaradi nezaposlenosti ali premajhnega plačila za svoje delo.

## *6.2 Statistična obdelava podatkov*

**Tabela 1: Kazniva dejanja na področju računalniške kriminalitete za leto 2005 in 2006**

| | Vrsta kaznivega dejanja | Število kaznivih dejanj | | Št. ovadenih osumljencev | |
|---|---|---|---|---|---|
| | | 2005 | 2006 | 2005 | 2006 |
| Računalniška kriminaliteta | Neupravičen vstop v informacijski sistem | 30 | 24 | 21 | 10 |
| | Vdor v računalniški sistem | 5 | 6 | 3 | 2 |
| | Neupravičena uporaba avtorskega dela in | 17 | 6 | 17 | 5 |
| | SKUPAJ | 52 | 36 | 41 | 17 |

Vir: Policija, 2006

S področja računalniške kriminalitete je bilo obravnavanih 36 (52) kaznivih dejanj, med katerimi so prevladovala kazniva dejanja neupravičenega vstopa v informacijski sistem. Preiskovanje teh kaznivih dejanj je postalo zahtevnejše in dolgotrajnejše, ker je bilo storilce vse težje odkriti, poleg tega pa se je policija pri preiskovanju soočala s čedalje večjo količino podatkov.

**Tabela 2: Kazniva dejanja na področju računalniške kriminalitete za leto 2006 in 2007**

| | Vrsta kaznivega dejanja | Število kaznivih dejanj | | Št. ovadenih osumljencev | |
|---|---|---|---|---|---|
| | | 2006 | 2007 | 2006 | 2007 |
| Računalniška kriminaliteta | Neupravičen vstop v informacijski sistem | 24 | 88 | 10 | 69 |
| | Vdor v računalniški sistem | 6 | 4 | 2 | 4 |
| | Neupravičena uporaba avtorskega dela in | 6 | 7 | 5 | 6 |
| | Izdelovanje in pridobivanje orožja in pripomočkov, namenjenih za vdor ali napad na informacijski sistem | 2 | 13 | 2 | 17 |
| | SKUPAJ | 13 | 112 | 19 | 96 |

Vir: Policija, 2007

Pri posebnih oblikah kriminalitete izstopa porast obravnavanih kaznivih dejanj s področja računalniške kriminalitete, in sicer z 38 na 112, število ovadenih osumljencev pa se je povečalo z 19 na 96. Najbolj se je povečalo število kaznivih dejanj neupravičenega vstopa v informacijski sistem ter izdelovanja in pridobivanja pripomočkov za vdor ali neupravičen vstop v informacijski sistem.

**Tabela 3: Kazniva dejanja na področju računalniške kriminalitete za leto 2007 in 2008**

| | Vrsta kaznivega dejanja | Število kaznivih dejanj | | Št. ovadenih osumljencev | |
|---|---|---|---|---|---|
| | | 2007 | 2008 | 2007 | 2008 |
| Računalniška kriminaliteta | Zloraba osebnih podatkov na internetu | 1 | 1 | - | - |
| | Kršitev materialnih avtorskih pravic na internetu | 7 | 10 | 6 | 13 |
| | Napad na informacijski sistem | 88 | 283 | 69 | 275 |
| | Vdor v poslovni informacijski sistem | 4 | 7 | 4 | 5 |
| | Izdelovanje in pridobivanje orožja in pripomočkov, namenjenih za vdor ali napad na informacijski sistem | 13 | 10 | 17 | 11 |
| | SKUPAJ | 112 | 310 | 96 | 304 |

Vir: Policija, 2008

Pri posebnih oblikah kriminalitete je izstopal porast obravnavanih kaznivih dejanj s področja računalniške kriminalitete, in sicer s 112 na 310 ali za 176,8 %, število ovadenih 7 osumljencev pa se je povečalo s 96 na 304 ali za 216,7 %. Najbolj se je povečalo število obravnavanih kaznivih dejanj napada na informacijski sistem, kar je po oceni policije posledica razraščanja kriminalitete v kibernetskem prostoru, po drugi strani pa večje seznanjenosti ljudi o nevarnosti interneta in pripravljenosti za prijavljanje kaznivih dejanj.

**Tabela 4: Kazniva dejanja na področju računalniške kriminalitete za leto 2008 in 2009**

| | Vrsta kaznivega dejanja | Število kaznivih dejanj | | Št. ovadenih osumljencev | |
|---|---|---|---|---|---|
| | | 2008 | 2009 | 2008 | 2009 |
| Računalniška kriminaliteta | Zloraba osebnih podatkov in vdor v poslovni informacijski sistem in | 7 | 11 | 5 | 6 |
| | Kršitev materialnih avtorskih pravic na internetu | 10 | 5 | 13 | 6 |
| | Napad na informacijski sistem | 283 | 98 | 275 | 78 |
| | Izdelovanje in pridobivanje orožja ali pripomočkov za vdor ali napad na informacijski sistem | 10 | - | 11 | - |
| | SKUPAJ | 310 | 314 | 304 | 90 |

Vir: Policija, 2009

Pri posebnih oblikah kriminalitete izstopa upad kaznivih dejanj s področja računalniške kriminalitete, in sicer s 310 na 114 ali za 63,2 %, predvsem zaradi zmanjšanja števila kaznivih dejanj napada na informacijski sistem. V prejšnjem letu je namreč policija med 8 preiskovanjem drugih kaznivih dejanj, predvsem goljufij in velikih tatvin pri zlorabah elektronskega bančništva, odkrila tudi kazniva dejanja napada na informacijski sistem.

**Tabela 5: Kazniva dejanja na področju računalniške kriminalitete za leto 2009 in 2010**

| | Vrsta kaznivega dejanja | Število kaznivih dejanj | | Št. ovadenih osumljencev | |
|---|---|---|---|---|---|
| | | 2009 | 2010 | 2009 | 2010 |
| Računalniška kriminaliteta | Zloraba osebnih podatkov in vdor v poslovni informacijski sistem in | 11 | 18 | 6 | 4 |
| | Kršitev materialnih avtorskih pravic na internetu | 5 | 5 | 6 | 7 |
| | Napad na informacijski sistem | 98 | 76 | 78 | 25 |
| | Izdelovanje in pridobivanje orožja ali pripomočkov za vdor ali napad na informacijski sistem | - | 2 | - | 3 |
| | SKUPAJ | 114 | 101 | 90 | 39 |

Vir: Policija, 2010

Število kaznivih dejanj računalniške kriminalitete se je zmanjšalo s 114 na 101 ali za 11,4 %, število ovadenih oseb pa z 90 na 39 ali za 56,7 %. To je posledica zmanjšanja števila zlorab elektronskega bančništva, s pomočjo katerih so bila storjena druga kazniva dejanja računalniške kriminalitete. Policija se je tudi bolj usmerila v zavarovanje in preiskovanje elektronskih naprav oziroma t. i. računalniško forenziko. Uporabnike elektronskega bančništva, pa tudi interneta in novih tehnologij, je opozarjala na možne nevarnosti njihove uporabe.

# 7 Zaključek

Zlorabo informacijskega sistema pri nas ureja predvsem kazensko pravna zakonodaja, natančneje Kazenski zakonik RS KZ. Veljavni KZ izrecno inkriminira le vdor v informacijski sistem, medtem ko je stari KZ govoril o neupravičenem vstopu. Za upravljanje informacijske varnosti obstaja splošni kodeks najboljših praks. Na tem področju je najbolj znan standard ISO/IEC 27001. Gre za sistem upravljanja varovanja informacij, ki temelji na pristopu tveganja in zagotavlja vzpostavitev, vpeljavo, delovanje, spremljanje, pregledovanje, vzdrževanje in izboljševanje varovanja informacij. Standard predvideva organizacijske, tehnične in Logično tehnične postopke in ukrepe, s katerimi se varujejo podatki, preprečuje slučajno ali namerno nepooblaščeno uničevanje podatkov in njihova sprememba ali izguba ter nepooblaščena obdelava.

Zaradi povečanega števila groženj in napadov je potrebno za informacijsko varnost poskrbeti - tako z elementi tehnične in fizične zaščite, kot tudi z znanjem v smislu pristopa k delu v kibernetskem prostoru. V nasprotnem hitro pride do zmanjšane stopnje varnosti posameznika oz. do napada in posledično možne zlorabe podatkov oz. napadenega in sedaj okuženega sistema. Pri podjetjih je potrebno dodati še element notranje varnosti - kar pomeni, da je potrebno zagotoviti, da z občutljivimi podatki in občutljivimi sistemi operirajo in rokujejo osebe, ki so zanesljive in imajo ustrezno znanje s področja informacijske varnosti in odzivom na grožnje (Bernik, 2012).

Da uspešno zagotovimo varnost informacijskih sistemov je potrebna izdelana in izvajana varnostna politika, prav tako pa njeno preverjanje, revidiranje in stalno prilagajanje poslovnim zahtevam. Organizacijski ukrepi, pravila in procedure so opredeljeni v varnostni politiki, implementacijska plat pa je popolnoma odprta. Varnostni sistemi (varnostna programska in strojna oprema) so zgolj pripomočki za dosledno izvajanje varnostnih procedur in pravil. Njihova nedosledna uporaba popolnoma izniči vse njihove potencialne pozitivne učinke, zato človeški faktor pri varnosti igra bistveno vlogo.

# 8 Uporabljeni viri


Belič, I. (1999). Teoretični okvir informacijske varnosti. *Varstvoslovje, 1*(2), 45-51.

Berčič, B. (2003). Računalniški kriminal in računalniški dokazi. V A. Šinigoj, (ur.), *Ukrepi v primeru informacijskih nesreč* (str. 142-143).

Bernik, I. in Prislan, K. (2011). Informacijsko bojevanje v Sloveniji – od tradicionalno lokalnega v globalni kibernetski prostor. *Varstvoslovje, 13*(3), 261-279.

Bernik, I. in Prislan, K. (2012). *Kibernetska kriminaliteta, informacijsko bojevanje in kibernetski terorizem*. Ljubljana: Fakulteta za varnostne vede.

Bernik, I. (2012). *Intervju z Igorjem Bernikom*. Pridobljeno na http://web-center.si/informacijska-varnost/223-intervju-z-igorjem-bernikom

Brezavšček, A. in Moškon, S. (2008). Vzpostavitev sistema za upravljanje informacijske varnosti v organizaciji. V P. Umek (ur.), *IX. slovenski dnevi varstvoslovja: Javna in zasebna varnost* (str. 67-68). Ljubljana: Fakulteta za varnostne vede.

Council of Europe. (2001). *Convention on Cybercrime*. Pridobljeno na http://conventions.coe.int/Treaty/en/Reports/Html/185.htm

Dunn, M. (2005). *International CIIP Handbook 2005*. Zurich: Swiss federal institute of technology.

Fefer, D. (2008). Varnostno nadzorni centri. V P. Umek (ur.), *IX. slovenski dnevi varstvoslovja: Javna in zasebna varnost* (str. 70). Ljubljana: Fakulteta za varnostne vede.

Kazenski zakonik 1 (KZ-1). (2008). *Uradni list RS*, (55/2008).

Lukman, M. (2008). Računalniška kriminaliteta, mit o altruizmu. V P. Umek (ur.), *IX. slovenski dnevi varstvoslovja: Javna in zasebna varnost* (str. 68-69). Ljubljana: Fakulteta za varnostne vede.

Lušenc, J. (2009). *Pravni vidiki informacijske varnosti* (Diplomsko delo). Maribor: Pravna fakulteta.

Policija. (2007). *Letno poročilo Policije za leto 2006*. Pridobljeno na http://www.policija.si/images/stories/Statistika/LetnaPorocila/PDF/lp2006.pdf

Policija. (2008). *Letno poročilo Policije za leto (2007)*. Pridobljeno na http://www.policija.si/images/stories/Statistika/LetnaPorocila/PDF/LetnoPorocilo2007.pdf

Policija. (2009). *Letno poročilo Policije za leto (2008)*. Pridobljeno na http://www.policija.si/images/stories/Statistika/LetnaPorocila/PDF/LetnoPorocilo2008.pdf

Policija. (2010). *Letno poročilo Policije za leto (2009)*. Pridobljeno na http://www.policija.si/images/stories/Statistika/LetnaPorocila/PDF/LetnoPorocilo2009.pdf

Policija. (2011). *Letno poročilo Policije za leto (2010)*. Pridobljeno na http://www.policija.si/images/stories/Statistika/LetnaPorocila/PDF/LetnoPorocilo2010.pdf

Podjed, D. (2008). *Računalniški kriminal* (Diplomsko delo). Ljubljana: Fakulteta za upravo.

Resolucija o nacionalnem programu preprečevanja in zatiranja kriminalitete za obdobje 2012–2016 (ReNPPZK12-16). (2012). *Uradni list RS*, (83/2012).

Simčič, S. (2007). *Ogrožanje kritične informacijske infrastrukture v Republiki Sloveniji* (Diplomsko delo). Ljubljana: Fakulteta za družbene vede.

UNODC. (2010). *Cybercrime*. Pridobljeno na http://www.unodc.org/documents/data-and-analysis/tocta/10.Cybercrime.pdf

Ustava Republike Slovenije. (1991). *Uradni list RS*, (33/1991).

Završnik, A. (2005). Kibernetična kriminaliteta - (kiber) kriminološke in (kiber) viktimološke posebnosti »informacijske avtoceste«. *Revija za kriminalistiko in kriminologijo, 56*(3), 248-260.

Zakon o varstvu osebnih podatkov 1 (ZVOP-1, ZVOP-1A, ZVOP-1-UPB1). (2004, 2007). *Uradni list RS*, (86/2004, 67/2007, 94/2007).

Zakon o zasebnem varovanju (ZZasV, ZZasV-B, ZZasV-1). (2003, 2009, 2011). *Uradni list RS*, (126/2003, 41/2009, 17/2011).

Zakon o elektronskih komunikacijah (ZEKom, ZEKom-1). (2004, 2009, 2011, 2012). *Uradni list RS*, (43/2004, 110/2009, 33/2011, 109/2012).

Zakon o elektronskem poslovanju na trgu (ZEPT, ZEPT-A, ZEPT-UPB2). (2006, 2009). *Uradni list RS*, (61/2006, 79/2009, 96/2009).

Zakon o elektronskem poslovanju in elektronskem podpisu (ZEPEP, ZEPEP-A, ZEPEP-UPB1). (2000, 2004). *Uradni list RS*, (57/2000, 25/2004, 98/2004).