Primjena i provođenje informacijske sigurnosti u Republici Hrvatskoj - regulativni okviri i standardi

Dolić, Frano

Master's thesis / Diplomski rad

2022

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Split, University Department for Forensic Sciences / Sveučilište u Splitu, Sveučilišni odjel za forenzične znanosti**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:227:303340

SVEUČILIŠTE U SPLITU
SVEUČILIŠNI ODJEL ZA
FORENZIČNE ZNANOSTI

FORENZIKA I NACIONALNA SIGURNOST

DIPLOMSKI RAD

PRIMJENA I PROVOĐENJE INFORMACIJSKE SIGURNOSTI U REPUBLICI HRVATSKOJ- REGULATIVNI OKVIRI I STANDARDI

MENTOR: izv. prof. dr. sc. MARIJA BOBAN

FRANO DOLIĆ

557-2020

Split, 2022.

Rad je izrađen u Sinju,

pod nadzorom izv. prof. dr. sc. Marija Boban,

u vremenskom razdoblju od 1. svibnja do 27. kolovoza 2022. god..

Datum predaje diplomskog rada: **08. studeni 2022. god.**

Datum prihvaćanja rada: **09. studeni 2022. god.**

Datum usmenog polaganja **14. studeni 2022. god.**

Povjerenstvo: **1. Prof. dr. sc. Jozo Čizmć**

2. Doc. dr. sc. Marina Carić

3. Izv. prof. dr.sc. Marija Boban

SADRŽAJ

1. UVOD

U ovom diplomskom radu obradit ćemo temu primjena i provođenja informacijske sigurnosti u Republici Hrvatskoj- regulativni okviri i standardi. Rad će sadržavati definicije i pojmove koji se odnose na informacijsku sigurnost, informacijski sustav, sigurnosni rizik i procjenu rizika, pojam kibernetike i na što se sve odnosi, sigurnosnu politiku, zakonodavni okvir informacijske sigurnosti i na kraju, norme informacijske sigurnosti.

U današnjem vremenu veoma je važno shvatiti značenje informacijske sigurnosti i informacijskih sustava da bi ih mogli prikladno zaštititi. Informacijska tehnologija ima brojne prednosti; točnost, pouzdanost, brzina. Informacijski sustavi sastoje se od puno važnih podataka i informacija koji se moraju adekvatno osigurati raznim mjerama i metodama, analizama rizika mogućih prijetnji koje mogu ostaviti značajne posljedice. Svaka organizacija bi trebala razviti sustav upravljanja informacijskom sigurnošću koji bi se temeljio na pristupu upravljanja rizicima radi uspostavljanja, provođenja, praćenja, revizije, održavanja i unaprjeđivanja informacijske sigurnosti.

Kroz svakodnevni život nam se pojavljuje potreba za računalom, bilo da se radi o poslu, igranju igrica, školi (praćenje on-line nastave), kupovini, provjeri e-pošte, čitanju knjiga, pretraživanju raznoraznih interesa… Iznova se javljaju novi načini ugroze informacijske sigurnosti od strane skupina ili pojedinca koji se bave kibernetičkim kriminalom. Zato je vrlo bitno osvijestiti pojedinca, zaposlenike, kolektive o važnosti informacijske sigurnosti i stalno ih na to podsjećati – da sebe i svoju imovinu zaštite od najvjerojatnijeg oblika napada koliko god su to u mogućnosti.

Treba „uhvatiti korak“ sa razvojem informatičke tehnologije i prilagoditi se bržem načinu života gdje ipak moramo prvenstveno misliti na sigurnost podataka i informacija koje ostavljamo za sobom i koje koristimo za rad te naći način na koji spriječiti njihovu zlouporabu. Savršenog sustava nema, ali ima načina na koji se može vrlo dobro i kvalitetno osigurati.

2. CILJ RADA

Svrha ovog diplomskog rada je teoretski prikaz informacijske sigurnosti u Republici Hrvatskoj, određivanje pojmova koji se odnose na informacijsku sigurnost, informacijske sustave i zakonske regulative koje ih uređuju bilo da se radi o nacionalnom ili međunarodnom zakonodavstvu, sigurnosne rizike i procjenu rizika te pojam kibernetičkog kriminala.

Radi znanstvenog usmjerenja rada, postavit će se sljedeće hipoteze, koje će se kroz rad i u rezultatima rada opovrgnuti ili potvrditi.

1. Nijedan sustav nije siguran pa tako ni informacijski sustav te zbog povećanog broja ugroza treba misliti na informacijsku sigurnost i zaštitu.
2. U svijetu i u Republici Hrvatskoj informacijska sigurnost je regulirana mnogim zakonima, standardima i pravilima radi odgovarajuće zaštite podataka.

Rad se sastoji od 7 cjelina. U prvoj cjelini određuju se pojmovi bliski informacijskoj sigurnosti te se ukratko povijesno obrađuju informacijska sigurnost i informacijski sustavi. Druga cjelina odnosi se na informacijsku sigurnost, njene aspekte i područja. Treća daje definiciju informacijskih sustava. Sigurnosni rizik i procjena rizika tema su četvrte cjeline. Kibernetika se obrađuje u petoj cjelini kao i kibernetički rat, terorizam, kriminal, špijunaža te kibernetička sigurnost u Republici Hrvatskoj. U šestoj cjelini obrađuje se sigurnosna politika, zakonska regulativa o pitanjima informacijske sigurnosti u Republici Hrvatskoj te institucije koje brinu o zaštiti informacijske sigurnosti u RH. I na kraju, norme informacijske sigurnosti; ISO standardi.

3. IZVORI PODATAKA I METODE

Prilikom znanstvenog istraživanja u radu će se koristiti sva dostupna znanstvena literatura iz različitih stručnih područja kako bi potvrdila ili opovrgla navedene hipoteze. Korišteni su sekundarni podaci pri izradi rada (službene Internet stranice gdje se nalaze radovi i članci vezani za informacijsku sigurnost, katalozi biblioteka, rječnici, bibliografije) te metode;

- metoda deskripcije – postupak opisivanja pojava i predmeta kao i njihovih veza i odnosa bez znanstvenog objašnjenja i tumačenja.
- metoda analize – postupak raščlanjivanja složenih pojmova, ideja ili zaključaka na njihove sastavne elemente.
- metoda sinteze – postupak u kojem se jednostavne misaone tvorevine ili pojedini dijelovi spajanjem povezuju u cjelinu.
- induktivna metoda – na temelju poznatih činjenica donosi se zaključak.
- deduktivna metoda – sagledavanje cijele slike, ideje, pojave ili predmeta i na temelju toga donošenje suda.
- metoda komparacije – postupak uspoređivanja istih ili sličnih činjenica, pojava, predmeta i utvrđivanja njihovih sličnosti i razlika.

4. DEFINICIJE I POVIJESNI PRIKAZ

Radi lakšeg shvaćanja pojma informacijske sigurnosti prvo ćemo definirati pojmove informacije i sigurnosti, osobnih podataka, prava na privatnost te informacijsku privatnost.

Informacija (lat. *informatio*) – smislen skup podataka koji je bitan element za povećanje razmjene ljudskog znanja. Ljudi putem svojih osjetila primaju informacije u obliku skupa podataka. Informacije koje osoba dobiva putem određenih podataka ovise o znanju koje posjeduje tj. koliko dobro razumije primljenu informaciju.[1] Informacije se mogu koristiti više puta od strane više korisnika, zbog čega su specifični resursi i važno ih je čuvati jer se mogu koristiti u bilo kojem trenutku.

Sigurnost (lat. *securitas*) – atribut nekoga ili nečega tko ima određeno, jasno i sigurno znanje o nečemu. Poimanje sigurnosti kroz različite kontekste donosi mnoge definicije i različite karakteristike. Sigurnost se promatra kao višedimenzionalni koncept s različitim elementima ovisno o tome što se istražuje. [2] Sigurnost je oblik zaštite od štetnih utjecaja i događaja. Radi zaštite sigurnosti mogu se poduzeti određene mjere da ne bi došlo do neželjenih posljedica. Sigurnost se odnosi na niz mjera i postupaka koji se poduzimaju da bi se osiguralo normalno funkcioniranje informacijskog sustava bez narušavanja njegovog integriteta.[3]

Sigurnost informacija u današnjem vremenu postaje sve važnija. Modernizacijom i digitalizacijom sve više se razvija informatička i komunikacijska infrastruktura što dovodi do protoka velike količine informacija među raznoraznim subjektima i predstavlja brojne prijetnje za informacijsku sigurnost. Zato se sve više ulaže u zaštitu informacijske sigurnosti i provode se brojne edukacije na tu temu.[4]

---

[1] informacija. *Hrvatska enciklopedija, mrežno izdanje.* Leksikografski zavod Miroslav Krleža, 2021. [pristupljeno 05. 06. 2022] Dostupno na http://www.enciklopedija.hr/Natuknica.aspx?ID=27405

[2] sigurnost. *Hrvatska enciklopedija, mrežno izdanje.* Leksikografski zavod Miroslav Krleža, 2021. [pristupljeno 05. 06. 2022] Dostupno na http://www.enciklopedija.hr/Natuknica.aspx?ID=55892

[3] Boban, M. Nove tehnologije, intelektualno vlasništvo i informacijska sigurnost, Sveučilišni studijski centar za forenzične znanosti Split 2022. – prezentacije s predavanja

[4] ictbusiness.info Cyber sigurnost postaje sve važnija (Internet) 2015 [pristupljeno 05.06.2022.] Dostupno na https://www.ictbusiness.info/poslovanje/cyber-sigurnost-postaje-sve-vaznija

Pravo na privatnost „predstavlja elementarno čovjekovo pravo, kako međunarodno, tako i ustavno pravo javno-pravnog značaja te osobno pravo civilno-pravnog značaja kao jedan od nezamjenjivih elemenata čovjekovog postojanja koji štiti čovjeka od prekomjernog posezanja državne vlasti, javnosti i drugih pojedinaca u pojedinčevu odlučujuću duševnu, prostornu i informacijsku privatnost. Dakle, pravo na privatnost može se razmatrati s nekoliko aspekata: kao čovjekovo pravo međunarodnopravne prirode, kao temeljno ustavom zagarantirano pravo te kao osobno pravo zaštićeno instrumentima građanskoga prava.“[5]

Informacijska privatnost odnosi se na pravne vrijednosti zaštite prava pojedinca tj. na prikupljanje podataka o osobi, korištenje podataka te upravljanje istim. Odnosi se na osobne podatke koji trebaju odobrenje osobe za korištenje od strane treće osobe.[6]

4.1. Povijesni razvoj informacijske sigurnosti

Pretraživanjem literature pojavljuju se dva pristupa razvoju informacijske sigurnosti; prvi se osniva na procjeni prijetnji, a drugi je usmjeren ka krajnjem cilju i bavi se upravljanjem sustavima sigurnosti. Knjiga „Evolucija ciljeva informacijske sigurnosti od 1960ih do danas“[7] opisuje glavna obilježja razvoja što ćemo objasniti u nastavku.[8]

1950ih godina sigurnosne prijetnje bile su minimalne, računala nisu bila dostupna svima i bilo ih je veoma malo, a ponajviše su se koristila pri vladama i vojsci. Sigurnost se odnosila na fizički pristup računalima da ne bi došlo do oštećenja ili krađe.[9]

---

[5] Šimundić, S. Pravna informatika, Sveučilište u Splitu Pravni fakultet, Split 2007. str. 447. citirano u Marija Boban: Pravo na privatnosti i pravo na pristup informacijama u suvremenom informacijskom društvu, Zbornik radova Pravnog fakulteta u Splitu, god. 49, 3/2012., str. 575.- 598. [pristupljeno 06.06.2022.] Dostupno na https://www.academia.edu/68874878/Pravo_na_privatnost_i_pravo_na_pristup_informacijama_u_suvremenom_informacijskom_dru%C5%A1tvu

[6] Boban, M. Pravo na privatnosti i pravo na pristup informacijama u suvremenom informacijskom društvu, Zbornik radova Pravnog fakulteta u Splitu, god. 49, 3/2012. str. 584.- 585.

[7] Cherdantseva Y. , Hilton J. Evolucija informacijske sigurnosti ciljevi od 1960-ih do danas Sveučilište Cardiff, 2012 [pristupljeno 06.06.2022.] Dostupno na https://users.cs.cf.ac.uk/Y.V.Cherdantseva/LectureEvolutionInfoSecGOALS.pdf

[8] Vukelić B. Sigurnost informacijskih sustava – skripta (Udžbenik) Rijeka: Veleučilište u Rijeci 2016 [pristupljeno 06.06.2022.] Dostupno na https://www.academia.edu/40637227/Sigurnost_informacijskih str.12.

[9] Vukelić B. Sigurnost informacijskih sustava – skripta (Udžbenik) Rijeka Veleučilište u Rijeci 2016 [pristupljeno 07.06.2022.] Dostupno na https://www.academia.edu/40637227/Sigurnost_informacijskih str.13.

1960ih godina računala su bila dostupnija odnosno jedno računalo je koristilo više osoba i to je predstavljalo prijetnju da neovlaštene osobe imaju pristup podacima.[10]

1970ih godina pojavljuje se sve veći broj osobnih računala, ali su sigurnosne prijetnje još uvijek minimalne. Zato se pojavljuje identifikacija i autentifikacija da bi se mogao pratiti prijavljeni korisnik računala i njegovo djelovanje. Pojavljuje se problem lozinki i njihovo dijeljenje jer nije bilo sigurnosne politike u to vrijeme.[11]

1980ih godina upotreba računala je u porastu što dovodi do problema – nedovoljno obučenih zaposlenika pa se donose razni zakoni. Informacijska sigurnost dovedena je u pitanje zbog velike razmjene informacija i podataka koji su se počeli širiti na stolna računala koja su povezana računalnim mrežama. Tada se pojavljuje i operacijski sustav Microsoft Windows i lokalne mreže (LAN), a samim tim bilježi se i rast računalnih virusa putem disketa što je rezultat začetka i uvođenja antivirusnih programa.[12]

1990ih godina u prvi plan dolazi sigurnost sustava, počinje se pratiti učinkovitost sigurnosnih mjera, donose se međunarodni certifikati za informacijsku sigurnost (BS 7799). Provode se mnogi tečajevi i edukacije, obučavaju zaposlenici tako da se shvati bitnost informacijske sigurnosti.[13]

2005. godine fokus se stavlja na razvoj u području korporativnog upravljanja informacijskom sigurnošću. U tom vremenu napravio se korak u međunarodnoj praksi za korporativno upravljanje i upravljanje rizicima informacijske tehnologije.[14]

Od 2006. godine počinje „Val kibernetičke sigurnosti“ koji za cilj ima osiguranje informacijske sigurnosti u kibernetičkom prostoru. Pojavljuju se hakerski napadi zbog financijske dobiti, IT infrastruktura širi se kroz gotovo sve grane industrije – sve kreće biti elektronički (e-poslovanje, e-uprava, e-trgovina…). [15]

[10] Ibid.
[11] Ibid.
[12] Ibid.
[13] Ibid.
[14] Arbanas K. Radni okvir za procjenu i unapređenje kulture informacijske sigurnosti [disertacija] Varaždin: Sveučilište u Zagrebu, Fakultet organizacije i informatike; 2021 [pristupljeno 07.06.2022.] Dostupno na: https://urn.nsk.hr/urn:nbn:hr:211:439511 str. 14.-15.
[15] Ibid.

4.2. Povijesni razvoj informacijskih sustava

Prema načinu obrade podataka kroz povijest mogu se odrediti četiri faze[16]:

1. Faza ručne obrade podataka

– je najstariji oblik obrade podataka, čovjek je koristio samo svoj um i svoje ruke a za ostala sredstva snalazio se u prirodi (kamen, drvo). U kamenja su se urezivali simboli, na papirus se pisalo drvetom, utiskivanje u glinene pločice, voštane pločice da bi na kraju došli do papira. Način takve obrade podataka bio je spor, netočan i nepouzdan.

2. Faza mehaničke obrade podataka

– početak ove faze označava kraj srednjeg vijeka, kulturološki procvat, iskorak čovječanstva u materijalnom i tehničkom smislu, rast i povećanje znanja. Javlja se potreba za kvalitetnijim, bržim i boljim obrađivanjem veće količine podataka što upućuje na izradu mehaničkih strojeva i specijaliziranih obrađivača podataka (Pascalina, pisaći stroj, bušene kartice, analitički stroj).

3. Faza elektromehaničke obrade

– 1881.godine vlada SAD-a raspisala je natječaj za izradu stroja koji bi obrađivao podatke prikupljene u popisu stanovništva na kojem je pobijedio Hermann Hollerith[17] koji daje prijedlog da nositelj podataka bude bušena kartica i da se napravi poseban elektromehanički stroj koji se smatra prvim pravim strojem za obradu podataka.

4. Faza elektroničke obrade podataka

– kreće 1944.godine razvojem ENIAC-a[18] koji se uzima kao prvo pravo elektroničko računalo. U ovoj fazi obrađuju se velike količine podataka uz minimalan broj grešaka, omogućava se pohranjivanje podataka (trajno i privremeno), povezivanje operacija na podacima (obrada i prijenos podataka), grafika, slika i zvuk. Internet također spada u ovu fazu razvoja.

---

[16] Lerga J. Primjena računala st – povijesni pregled razvoja računala [prezentacija], Tehnički fakultet Sveučilišta u Rijeci [pristupljeno 08.06.2022.] Dostupno na https://www.academia.edu/21637101/PRIMJENA_RA%C4%8CUNALA_ST_P02_Povijesni_pregled_razvoja_ra%C4%8Dunala

[17] Herman Holerith (1860.-1929.) njemačko-američki statističar, izumitelj i poslovni čovjek, jedan od suvlasnika i suosnivatelja IBM tvrtke 1924.g. koja je jedna od najvećih i najuspješnijih tvrtki 20.stoljeća.

[18] ENIAC – Eletronic Numerical Integrator and Computer, prvo potpuno elektroničko, opće namjensko računalo na svijetu. Izgradili su ga J. Presper Eckert i John V. Mauchly, u Pennsylvaniji 1945.godine. Zadaća mu je bila izračunavanje balističkih tablica za američku vojsku, a upotrebljavo se za znanstvene proračune ranih 1950ih. Imao je masu 30 tona, zauzimao 140 m², sastavljen od 18000 elektronskih cijevi i 1500 releja. Kapacitet je bio 1 kB. On je razdjelnik između pokusnih i uporabnih elektroničkih računala i njime starta razdoblje digitalnih računala.
ENIAC. Hrvatska enciklopedija, mrežno izdanje. Leksikografski zavod Miroslav Krleža, 2021. [pristupljeno 09.06.2022.] Dostupno na http://www.enciklopedija.hr/Natuknica.aspx?ID=17976 .

5. INFORMACIJSKA SIGURNOST

Republika Hrvatska u Zakonu o informacijskoj sigurnosti[19], u uvodnom dijelu daje jasnu definiciju informacijske sigurnosti i objašnjava da je to „stanje povjerljivosti, cjelovitosti i raspoloživosti podatka, koje se postiže primjenom propisanih mjera i standarda informacijske sigurnost te organizacijskom podrškom za poslove planiranja, provedbe, provjere i dorade mjera i standarda“.

Gdje god se karakterizira primjena neke određene vrste podataka moraju se propisivati sigurnosni standardi. Ako se radi o vrstama podataka, informacijska sigurnost odnosi se na podatke koji imaju određeni stupanj tajnosti odnosno klasifikaciju podataka da bi se zaštitio njihov sadržaj.[20]

„Mjere informacijske sigurnosti su opća pravila zaštite podataka koja se realiziraju na fizičkoj, tehničkoj ili organizacijskoj razini.“[21]

„Standardi informacijske sigurnosti su organizacijske i tehničke procedure i rješenja namijenjena sustavnoj i ujednačenoj provedbi propisanih mjera informacijske sigurnosti.“[22]

Mjere i standardi informacijske sigurnosti utvrđuju se za klasificirane i neklasificirane podatke, sukladno stupnju tajnosti, broju, vrste te ugrozama tih podataka na određenoj lokaciji. Propisuju se uredbom koju donese Vlada Republike Hrvatske, a standardi za provođenje mjera propisuju se pravilnicima. One obuhvaćaju[23]:

- nadzor pristupa i postupanja
- postupanje prilikom neovlaštenog otkrivanja i gubitka podataka
- planiranje mjera kod izvanrednih situacija
- ustrojavanje posebnih fondova podataka za podatke klasificirane u Republici Hrvatskoj ili za klasificirane podatke predane od strane drugih država, međunarodnih organizacija ili institucija.

[19] Zakon o informacijskoj sigurnosti (NN 79/07) (u daljnjem tekstu ZoIS) Dostupno na https://narodne-novine.nn.hr/clanci/sluzbeni/2007_07_79_2484.html
[20] Čizmić J., Boban M., Zlatović D. Nove tehnologije, intelektualno vlasništvo i informacijska sigurnost, Sveučilište u Splitu Pravni fakultet, Split 2016. str.682.
[21] Čl.2.st.2. ZoIS-a
[22] Ured Vijeća za nacionalnu sigurnost – uvns.hr (Internet) [pristupljeno 10.06.2022.] Dostupno na https://www.uvns.hr/hr/sto-su-to-mjere-i-standardi-informacijske-sigurnosti
[23] Čl.5. ZoIS-a

Informacijskoj sigurnosti pridaje se mnogo važnosti u cijelom svijetu zbog sve većeg porasta razmjene podataka i informacija te digitalizacije što dovodi do velikih problema i bilježi sve veću porast na području računalnog kriminala, raznih prijevara, manipulacija, iskorištavanja, krađa identiteta.. Zato je iznimno važno da se informacijska sigurnost regulira zakonom ili drugim propisima koji se donose na najvišoj razini bez obzira radi li se o državi ili poslovnom subjektu. Informacije koje razni subjekti izmjenjuju trebaju se zaštiti od velikog broja prijetnji, potrebno je uvesti odgovarajuće kontrole sustava i raditi na njihovom unaprjeđenju da bi se spriječio gubitak podataka koji su pohranjeni ili u obradi, a prije svega treba educirati ljude koji rade s tim informacijama svakodnevno.

5.1. Aspekti informacijske sigurnosti

Tri su osnovna aspekta informacijske sigurnosti[24];

1. povjerljivost (eng. *confidentiality*)

   – podrazumijeva se tajnost i pristup informacijama samo osobama koje su ovlaštene i imaju dozvolu za korištenje. Takvim podacima najčešće prijetnje su; napadači tzv. hakeri, neovlašteni korisnici, trojanski konji, kopiranje podataka na sustave koji nemaju dovoljnu razinu zaštite, razni zlonamjerni programi, nezaštićeno preuzimanje, lokalne mreže..

2. integritet (eng. *integrity*)

   – znači da osoba koja koristi podatke ne može iste izmijeniti bez ovlaštenja. Vrlo često se može namjerno ili nenamjerno dogoditi da dođe do neovlaštene izmjene podataka. Integritet podataka osigurava da se to ne dogodi i kako bi se očuvao važno je da se može utvrditi identitet osobe nekakvom vrstom autentifikacije (lozinke, pametne kartice, biometrijski čitači i slično).

[24] Nacionalni centar za sigurnost računalnih mreža i sustava CARNet CERT (Internet) [pristupljeno 11.06.2022.] Dostupno na https://www.cert.hr/wp-content/uploads/2009/05/CCERT-PUBDOC-2009-05-265.pdf

3. dostupnost (eng. *availability*)

– informacije i podaci moraju biti dostupni kako bi informacijski sustav ispunio svrhu. Cilj dostupnosti je osigurati podatke i informacije kada one zatrebaju, a to se osigurava fizičkim, tehničkim i administrativnim mjerama. Dostupnost može biti narušena ako se dogodi DoS napad (napad uskraćivanjem usluge – onemogućavanje rada poslužitelja ovlaštenim korisnicima) ili gubitak mogućnosti obrade podataka.

Slika 1. Osnovni aspekti informacijske sigurnosti (Confidentiality, Integrity, Availability–CIA)[25]

Kombinacijom ova tri aspekta, stvaraju se i dodatna načela koja ih nadopunjuju i dodatno opisuju[26];

- neporecivost (osigurava nemogućnost poricanja izvršene aktivnosti ili primitka podatka)
- autentičnost (osigurava da identitet subjekta bude stvarno onaj za koji se tvrdi da jest)
- dokazivost (osigurava da aktivnosti subjekta mogu biti praćene do samog subjekta)
- pouzdanost (svojstvo dosljednog ponašanja i rezultata).

[25] Izvor: researchgate.net Requirements for cybersecurity in agricultural communication networks - Scientific Figure on ResearchGate. [pristupljeno 12.06.2022] Dostupno na https://www.researchgate.net/figure/The-Confidentiality-Integrity-Availability-CIA-triad_fig1_346192126

[26] čl. 2. st. 9., 13., 14., 15., 16. Odluka o primjerenom upravljanju informacijskim sustavom Dostupno na https://narodne-novine.nn.hr/clanci/sluzbeni/2010_03_37_958.html

5.2. Područja informacijske sigurnosti

Područja informacijske sigurnosti za koja se propisuju mjere i standardi informacijske sigurnosti jesu[27]:

- sigurnosna provjera
- fizička sigurnost
- sigurnost podataka
- sigurnost informacijskom sustava
- sigurnost poslovne suradnje.

5.2.1. Sigurnosna provjera

U članku 9. ZoIS-a, sigurnosna provjera se opisuje kao područje informacijske sigurnosti u čijem okviru se utvrđuju mjere i standardi informacijske sigurnosti koji se odnose i primjenjuju na osobe koje imaju pristup klasificiranim podacima („Povjerljivo“, „Tajno“ i „Vrlo tajno“) te dužnost da se vodi popis osoba koje imaju pristup takvoj vrsti podataka i registar zaprimljenih certifikata s rokovima važenja (osobe moraju proći sigurnosnu provjeru i dobiti certifikat o istom).

5.2.2. Fizička sigurnost

Fizička sigurnost odnosi se na područje informacijske sigurnosti gdje se utvrđuju mjere i standardi informacijske sigurnosti radi zaštite objekata, prostora i uređaja gdje se nalaze klasificirani podaci.[28]

5.2.3. Sigurnost podataka

Sigurnost podataka odnosi se na mjere i standarde informacijske sigurnosti koje se primjenjuju kao općenite zaštitne mjere radi prevencije, otkrivanja i otklanjanja štete od gubitaka ili neovlaštenog odavanja klasificiranih i neklasificiranih podataka.[29]

[27] Čizmić J.,. Boban M., Zlatović D. Nove tehnologije, intelektualno vlasništvo i informacijska sigurnost, Sveučilište u Splitu Pravni fakultet, Split 2016, str. 714
[28] Čl.10. ZoIS-a
[29] Čl.11. ZoIS-a

5.2.4. Sigurnost informacijskog sustava

Sigurnost informacijskog sustava određuje mjere i standarde informacijske sigurnosti podataka koji se obrađuju, spremaju ili prenose putem informacijskog sustava i zaštitu cijelog sustava u procesu planiranja, projektiranja, izgradnje, uporabe, održavanja i prestanka rada informacijskog sustava, kako bi se omogućio nesmetan rad samog informacijskog sustava.[30]

5.2.5. Sigurnost poslovne suradnje

Sigurnost poslovne suradnje je područje gdje se primjenjuju propisane mjere i standardi informacijske sigurnosti za provedbu natječaja ili ugovora s klasificiranim dokumentima. Osobe koje to koriste dužne su ishoditi uvjerenje o sigurnosnoj provjeri – certifikat poslovne sigurnosti koje izdaje središnje državno tijelo za informacijsku sigurnost.[31]

Informacijsku sigurnost obvezna su provoditi[32]:

- državna tijela
- tijela jedinica lokalne i područne samouprave
- pravne osobe s javnim ovlastima koje u svom radu koriste klasificirane i neklasificirane podatke
- fizičke i pravne osobe koje imaju pristup ili rade s klasificiranim i neklasificiranim podacima.

Savjetnik za informacijsku sigurnost su fizičke ili pravne osobe koje moraju ispuniti određene uvjete; visoka stručna sprema, aktivno poznavanje engleskog jezika, zaposlenik tijela ili pravne osobe u kojoj se imenuje, posjedovanje certifikata, radno iskustvo (minimalno dvije godine na poslovima informacijske sigurnosti). On obavlja poslove nadzora, provodi edukaciju i koordinira provedbe mjera informacijske sigurnosti sukladno pravilnicima koji se odnose na informacijsku sigurnost.[33]

---

[30] Čl.12. ZoIS-a
[31] Čl.13. ZoIS-a
[32] uvns.hr Ured Vijeća za nacionalnu sigurnost (Internet) [pristupljeno 14.06.2022.] Dostupno na https://www.uvns.hr/hr/tko-je-sve-obavezan-provoditi-informacijsku-sigurnost
[33] uvns.hr Ured Vijeća za nacionalnu sigurnost (Internet) [pristupljeno 14.06.2022.] Dostupno na https://www.uvns.hr/hr/tko-moze-biti-savjetnik-za-informacijsku-sigurnost

6. INFORMACIJSKI SUSTAV

Neke od mnogobrojnih definicija informacijskog sustava;

„Informacijski sustav je komunikacijski, računalni ili drugi elektronički sustav u kojem se podaci obrađuju, pohranjuju ili prenose tako da budu dostupni i upotrebljivi za ovlaštene korisnike.“[34]

„Informacijski sustav sastoji se od ljudi, opreme, tehnologije i postupaka koji omogućuju prikupljanje, pohranu, analizu, obradu i distribuciju podataka i informacija korisnicima, odnosno donositeljima poslovnih odluka.“[35]

„Informacijski sustav može se odrediti kao strukturirani, međusobno povezani kompleks ljudi, strojeva i procedura, predviđen za generiranje kontinuiranog toka odgovarajućih informacija prikupljenih iz unutarnjih i vanjskih izvora poduzeća za uporabu istih, kao baze pri donošenju poslovnih odluka.“[36]

Iz informacijskog sustava proizlaze informacije tako da se obrađuju podaci, organiziraju i prezentiraju na razumljiv način krajnjem korisniku. Informacijski sustav izrađuje se po mjeri i potrebi korisnika, tako da za različita područja postoje različiti informacijski sustavi.[37]

Svrha informacijskog sustava je da dostavi odgovarajuću informaciju u odgovarajuće vrijeme, na odgovarajuće mjesto uz što manje troškova.

Informacijski sustav ima šest sastavnih dijelova i svaki je podjednako važan za funkcioniranje informacijskog sustava (slika na sljedećoj stranici).

[34] Čl.2. ZoIS-a
[35] Srića, V., Spremić, M. Informacijskom tehnologijom do uspjeha, Sinergija, Zagreb, 2000. str. 8.
[36] Tihi, B., Istraživanje tržišta organizacije udruženog rada, V. Masleša, Sarajevo, 1987. str. 291.
[37] Tuđman, M., Boras, D., Doveden, Z., Uvod u informacijske znanosti, Školska knjiga, Zagreb 1993. [pristupljeno 15.06.2022.] Dostupno na http://dzs.ffzg.unizg.hr/text/Uvod%20u%20informacijske%20znanosti/pog9.htm

Komponente informacijskog sustava	Definicije
Podaci	Unos koji sustav uzima za stvaranje informacija
Hardver	Računalo i njegova periferna oprema: uređaji za unos, izlaz i pohranu; hardver uključuje i opremu za podatkovnu komunikaciju
Softver	Skupovi uputa koje računalu govore kako unositi podatke, kako ih obraditi, kako prikazati informacije i kako pohraniti podatke i informacije
Telekomunikacije	Hardver i softver koji olakšavaju brzi prijenos i prijem teksta, slika, zvuka i animacije u obliku elektroničkih podataka
Ljudi	Stručnjaci informacijskih sustava i korisnici koji analiziraju organizacijske informacijske potrebe, dizajniraju i konstruiraju informacijske sustave, pišu računalne programe, upravljaju hardverom i održavaju softver
Postupci	Pravila za postizanje optimalnih i sigurnih operacija u obradi podataka; postupci uključuju prioritete u izdavanju softverskih aplikacija i

Tablica 1. Komponente informacijskog sustava[38]

Postoji mnogo raznih vrsta informacijskih sustava, ali neka općenita podjela radi se prema osnovnoj namjeni, načinu prikupljanja, sredstava za obradu informacija te prema tipu upravljanja.

- Informacijski sustavi prema osnovnoj namjeni podijeljeni su na:[39]
- sustave za prikupljanje i obrađivanje podataka
- informirajuće sustave (informiranje javnosti, građana, poslovnih suradnika, informiranje zaposlenika, informatora)
- sustave informacija koji su podloga svim drugim informacijskim, poslovnim i drugim sustavima upravljanja
- integralne informacijske sustave (obuhvaćaju cjelinu informacijskih funkcija i poslova).
- Informacijski sustavi prema načinu prikupljanja informacija dijele se na:[40]

[38] Izvor: Stair, R.M, Reynolds, G & Reynolds, G.W. Osnove informacijskih sustava, peto izdanje, 2008. Cengage Learning str.102 [pristupljeno 16.06.2022.] Dostupno na https://research-methodology.net/information-system-and-its-components/

[39] Panian, Ž., Ćurko, K., Bosilj Vukšić, V., Čerić, V., Pejić Bach, M., Požgaj, Ž., Spremić, M., Strugar, I., Varga, M. Poslovni informacijski sustavi (knjiga) Zagreb, Element, 2010. str. 82.

- formalne informacijske sustave - sadrže informacije prikupljene na definiran i pravilan način, nužne da bi neka organizacija funkcionirala.
- neformalne informacijske sustave – sačinjeni od razgovora radnika, ideja, osobnih podataka, uvjeravanja kupaca i sl.

➢ Informacijski sustavi prema sredstvima za obradu informacija dijele se na:[41]

- mehanografski informacijski sustav – utemeljen na strojevima koji ne sadrže mikroprocesor
- računalni informacijski sustav – koristi se i oslanja na informacijsku tehnologiju
- ručni informacijski sustav – iako zastarjelo, još postoji. Koristi ljudski rad za obradu i čuvanje podataka.

6.1. Vrste prijetnji informacijskom sustavu

Informacijski sustav može biti ugrožen na mnogo načina, a može se podijeliti na[42]:

➢ djelovanje ljudi (namjerno ili nenamjerno)
➢ opremu (mehanička oštećenja, prestanak napajanja, greške u sustavu, tvorničke greške, prekid komunikacije)
➢ prirodne nepogode (požar, poplava, potres, erupcija vulkana).

Pregledom dostupne literature, ustanovljeno je da je najčešća prijetnja informacijskog sustava ljudski faktor i to nenamjernim djelovanjem, a tek onda dolazi oprema i prirodne nepogode. Ljudska greška može se umanjiti stalnim educiranjem i provođenjem nadzora nad informacijskom sigurnošću. Sukladno navedenom, izrađuju se metode zaštite da bi se zaštitio informacijski sustav.

---

[40] Pavlić, M. Informacijski sustavi (udžbenik) Zagreb: Školska knjiga d.d. 2011. str. 40
[41] Ibid.
[42] Boban M, Perišić M. Biometrija u sustavu sigurnosti, zaštite i nadzora informacijskih sustava. Zbornik radova Veleučilišta u Šibeniku (Internet) 2015 [pristupljeno 17.06.2022] (1-2/2015):115-148. Dostupno na https://hrcak.srce.hr/142285

6.2. Kategorije napada

Napadi se označavaju kao akcije koje su usmjerene na ugrožavanje sigurnosti podataka, mreža i računalnih sustava što čini sigurnost informacijskog sustava. Razlikuje se nekoliko vrsta[43]:

- **presijecanje ili prekidanje komunikacijskog kanala** (eng. *interruption*) – korisniku se onemogućava normalno korištenje usluga, prekida se protok podataka. Napadač može; blokirati pristup mreži, prikriti informacije kako se ne bi vidjela njegova prisutnost i mogućnost budućih napada, slati nevažeće podatke aplikacijama i mrežnim servisima što dovodi do prestanka rada i nestabilnosti, poplava mreže ili računala s mrežnim prometom što vodi do preopterećenja.[44]
- **presretanje informacija u komunikacijskim kanalima** (eng. *interception*) – to su napadi koji se događaju posredstvom treće osobe u komunikaciji tako da treća strana može pratiti, bilježiti i kontrolirati komunikaciju. Napadač može preusmjeriti razmjenu podataka, ubacuje se u komunikaciju između korisnika, prosljeđuje poruke na svoje računalo i predstavlja se kao osoba koja je već u razgovoru i izvlači podatke i informacije. Ova vrsta napada predstavlja mogućnost preusmjeravanja podataka.[45]
- **izmjena informacija** (eng. *modification*) – nakon što napadač dobije potrebne informacije i podatke, promijeni ih bez znanja drugih sudionika, u svoju korist. Ovakva vrsta napada je iznimno štetna, posebno kada se radi o novčanim transakcijama, podjelom podataka o osobama ili određenim subjektima.[46]
- **proizvodnja** (eng. *fabrication*) – metoda umetanja lažnih podataka služi za krađu i zlonamjerno korištenje podataka i informacija. Napadač umeće lažne podatke u korisnikovu mrežu da bi naštetio korisniku ili ukrao podatke i informacije.[47]

---

[43] Boban M, Perišić M. Biometrija u sustavu sigurnosti, zaštite i nadzora informacijskih sustava. Zbornik radova Veleučilišta u Šibeniku (Internet) 2015 [pristupljeno 18.06.2022] (1-2/2015):115-148. Dostupno na https://hrcak.srce.hr/142285

[44] docs.microsoft.com - službena stranica Microsofta [pristupljeno 18.06.2022] Dostupno na https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-2000-server/cc959354(v=technet.10)

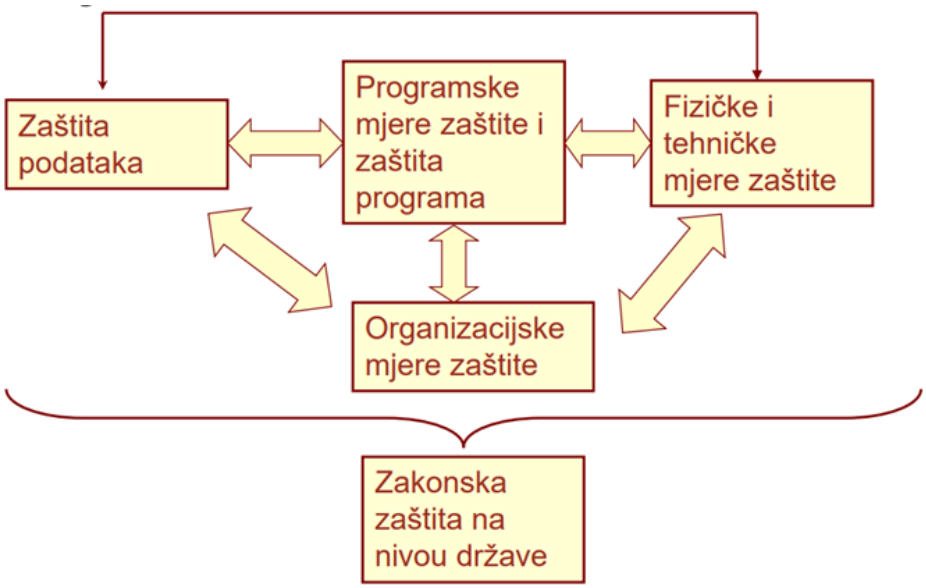
[45] Ibid.

[46] Ibid.

[47] docs.microsoft.com - službena stranica Microsofta [pristupljeno 19.06.2022] Dostupno na https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-2000-server/cc959354(v=technet.10)

6.3. Mjere zaštite informacijskih sustava

Potreba za mjerama zaštite informacijskih sustava javlja se kada su se računala počela primjenjivati u poslovnoj praksi. Na početku primjene računala zaštita je bila samo fizička i tehnička zaštita jer su se računala nalazila u prostorijama i objektima zbog svog obujma. Kasnije se javlja potreba i za drugim oblicima zaštite. Prema Uredbi o mjerama informacijske sigurnosti[48] (RH) mjere zaštite informacijskog sustava su; zaštita hardvera, softvera i medija za pohranu podataka, upravljanje konfiguracijom i sustavom korisničkog pristupa, kontrola povezivanja i uporabe informacijskih sustava, zaštita od rizika elektromagnetskog zračenja, primjena kriptografske zaštite.[49]



Slika 2. Mjere zaštite informacijskog sustava[50]

Postoji par razina organizacijske sigurnosti: infrastruktura informacijske sigurnosti, sigurnost pristupa treće osobe i outsourcing.

[48] Uredba o mjerama informacijske sigurnosti (NN 46/2008) Dostupna na https://narodne-novine.nn.hr/clanci/sluzbeni/full/2008_04_46_1547.html
[49] Čl.46. Uredbe o mjerama informacijske sigurnosti
[50] Izvor: Boban, M. Nove tehnologije, intelektualno vlasništvo i informacijska sigurnost, Sveučilišni studijski centar za forenzične znanosti Split 2022. – prezentacije s predavanja

6.3.1. Infrastruktura informacijske sigurnosti

Cilj je upravljanje informacijskom sigurnosti unutar organizacije, a dijeli se na[51]:

- tim za upravljanje informacijskom sigurnosti
- koordinaciju rada informacijske sigurnosti
- dodjele odgovornosti za informacijsku sigurnost
- proces autorizacije
- savjeti stručnjaka o informacijskoj sigurnosti
- suradnja među organizacijama
- neovisni pregledi efikasnosti informacijske sigurnosti.

Svi zaposleni moraju se brinuti o sigurnosti informacijskog sustava. Ponegdje se osnivaju timovi ili se uzima jedan pojedinac koji će kontrolirati i voditi brigu o svim problemima, pratiti promjene, donositi nove sigurnosne politike za boljitak sigurnosti informacijskog sustava na razini organizacije.

6.3.2. Sigurnost pristupa treće osobe

Ponekad se javlja potreba da se zaposle treće osobe u organizaciji (čistači, dobavljači, zaštitari, studenti, konzultanti, partneri..), a mora se očuvati sigurnost organizacije. Tada se javlja kontrola pristupa i trećim osobama dozvoljava se pristup samo onim prostorijama/stvarima koje su neophodne za njihov nesmetan rad. Razlikuje se fizički i logički pristup. Fizičkim pristupom, trećim stranama se omogućava pristup prostorijama sa računalima, uredima i ormarima za pohranu, a logičkim pristupom daje se pristup bazama podataka i informacijskim sustavima.[52]

Trećim osobama dozvoljava se pristup informacijama za rad tek iza potpisivanja ugovora.

6.3.3. Outsourcing

Označava davanje određenog posla vanjskim dobavljačima jer tvrtke koje to primjenjuju smanjuju troškove koji nastaju podmirivanjem potrebe za djelatnostima koje im nisu temeljne.[53]

[51] Garača, Ž., Informatičke tehnologije, Sveučilište u Splitu, Split, 2007. str. 98-110
[52] Panian, Ž. Kontrola i revizija informacijskih sustava. Zagreb, Sinergija nakladništvo, 2001. str. 178
[53] bolje.hr (Internet) [pristupljeno 21.06.2022] Dostupno na https://bolje.hr/rijec/outsourcing-gt-izdvajanje-posla/1/

Kada se ugovaraju takvi poslovi bitno je sklopiti nekakav ugovor uz primjenu procjene rizika i sigurnosnih postupaka kako ne bi došlo do neovlaštenog korištenja informacija. Prednost ovakvog zapošljavanja za rad na pojedinom zadatku ne obvezuje zadržavanje osobe nakon završenog posla ako za nju nema potrebe i samim time je lakše prekinuti radni odnos. Outsourcing čini neke zadatke bržim i učinkovitijim, omogućava pristup kvalificiranim radnicima te maksimizira fleksibilnost radne snage.[54]

Korištenje zaštitnih mjera pri upravljanju informacijskim sustavom osigurava se višeslojna zaštita resursa informacijskog sustava, a one imaju ulogu[55]:

- prevencije
- odvraćanja
- otkrivanja
- ograničavanja
- korigiranja
- oporavka
- nadzora
- osvješćivanja.

[54] moj-posao.net Outsourcing što je i zašto se koristi? (Internet) [pristupljeno 22.06.2022] Dostupno na https://www.moj-posao.net/Vijest/60807/Outsourcing-sto-je-i-zasto-se-koristi/

[55] HNB, Smjernice za upravljanje informacijskim sustavom u cilju smanjenja operativnog rizika, [pristupljeno 23.06.2022] Dostupno na https://www.hnb.hr/documents/20182/639854/h-smjernice-za-upravljanje-informacijskim-sustavom.pdf/e5579931-e846-47ab-af23-6809debef700 str.12.

7. SIGURNOSNI RIZIK I PROCJENA RIZIKA

Sigurnosni rizik definiran je kao mogućnost realizacije nekog neželjenog događaja koji može negativno utjecati na povjerljivost, integritet i raspoloživost informacijskih resursa.[56]

Upravljanje rizikom – proces identifikacije rizika, procjene rizika i poduzimanja koraka da se rizik smanji na prihvatljiv nivo.[57]

Upravljanje sigurnosnim rizikom nova je disciplina koja je začeta iz potrebe za standardizacijom postupaka koji su povezani s upravljanjem sigurnošću. Odnosi se na proces identifikacije čimbenika koji mogu negativno utjecati na povjerljivost, integritet i raspoloživost informacijskih resursa kao i njihovo analiziranje i izradu troškova zaštite. Krajnji korak obuhvaća provođenje zaštitnih mjera kojima se identificira sigurnosni rizik i svodi na minimum.[58]

Proces upravljanja sigurnosnim rizikom ima tri faze[59];

- procjena rizika (mora biti temeljita - konkretno određivanje sigurnosnog rizika, detaljna analiza prijetnji i ranjivosti, vjerojatnost realizacije rizika i posljedica, uklanjanje rizika i postupci uklanjanja)
- umanjivanje rizika (analizira se i evaluira, implementira u odgovarajuće sigurnosne kontrole s ciljem umanjivanja sigurnosnog rizika)
- ispitivanje i analiza (periodične analize i evaluacije za održavanje postignute razine sigurnosti – nadogradnja, instalacija..).

Prijetnjom se smatra bilo koja okolnost ili događaj, vanjski ili unutarnji, koji ima namjeru uzrokovati štetu informacijskom sustavu ili njegovim aplikacijama i podacima ili nanošenje štete resursima.[60]

Pri procjeni rizika obraća se pozornost na strategiju organizacije za koju se donosi i koji su njeni ciljevi. Uzima se obzir stupanj ranjivosti, predlažu se zaštitne mjere kako bi se što više

[56] cis.hr Upravljanje sigurnosnim rizicima (Internet) [pristupljeno 24.06.2022] Dostupno na https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2003-10-44.pdf
[57] Ibid.
[58] Ibid.
[59] Ibid.
[60] cis.hr Osnove upravljanja rizikom (Internet) [pristupljeno 24.06.2022] Dostupno na https://www.cis.hr/files/Celuska-Osnove_upravljanja_rizikom.pdf

smanjio rizik, analiziraju se postojeće prijetnje informacijskom sustavu, provode se periodične procjene kako bi se došlo do novih saznanja o opasnostima koje mogu utjecati na rizik.

„Ranjivost je slabost koju je moguće slučajno aktivirati ili namjerno iskoristiti, a posljedica toga može biti nanošenje štete informacijskom sustavu i poslovnim ciljevima.“ [61]

Ranjivost sustava odnosi se na sve slabosti sustava sigurnosti gdje postoji opasnost od provođenja nedopuštenih aktivnosti. Ranjivosti se odnose na propuste vezane za programski kod, dizajn sustava, održavanje i ažuriranje sustava, neadekvatan izbor tehnologije… Ako nije provedena detaljna analiza ranjivosti sustava tada nije moguće odrediti sigurnosni rizik.[62]

Sigurnosne prijetnje odnose se na svaki događaj koji poništava ili smanjiva produktivnost sustava tj. ograničava ili onemogućava ispunjenje cilja određenog procesa ili sustava.[63]

TIP IMOVINE	RANJIVOST	PRIJETNJA
Hardver	Neredovito održavanje	Tehnički kvar na sustavu
	Nezaključani ormarići	Krađa medija i dokumenata
	Nekontrolirano odbacivanje medija	Krađa medija i dokumenata
Softver	Nedovoljno testiranje softvera	Greška u aplikaciji
	Poznate ranjivosti u softveru	Iskorištavanje poznatih ranjivosti
	Nedostatak operativnih i sistemskih zapisa	Neovlaštene promjene u sustavu
Mreža	Slabo upravljanje zaporkama	Napadi probijanjem zaporki
	Nekriptirani promet	Prisluškivanje prometa
	Neredundantna oprema	Kvar na mrežnom uređaju
Ljudi	Nedovoljna obučenost djelatnika	Greške pri korištenju
	Manjak obučenog kadra	Otkaz djelatnika
Lokacija	Blizina rijeke	Poplava
	Nedostatak agregata i/ili UPS-ova	Nestanak struje

Tablica 2. Primjeri prijetnji i ranjivosti[64]

[61] hnb.hr HNB – Hrvatska narodna banka [pristupljeno 26.06.2022] Dostupno na https://www.hnb.hr/documents/20182/639854/h-smjernice-za-upravljanje-informacijskim-sustavom.pdf/e5579931-e846-47ab-af23-6809debef700 str.10.

[62] Boban, M. Nove tehnologije, intelektualno vlasništvo i informacijska sigurnost, Sveučilišni studijski centar za forenzične znanosti Split 2022. – prezentacije s predavanja

[63] Boban, M. Nove tehnologije, intelektualno vlasništvo i informacijska sigurnost, Sveučilišni studijski centar za forenzične znanosti Split 2022. – prezentacije s predavanja

[64] Izvor: Uremović, D. Kako upravljati IT rizicima? (članak) [pristupljeno 28.06.2022] Dostupno na https://alterinfo.hr/lib/q55e1o/Upravljanje_rizicima-ku2buxeu.pdf

Sigurnosni zahtjevi ovise o vrsti informacija i podataka koji se žele zaštititi. On dobiva na važnosti zbog sve veće opasnosti od prijetnji i ranjivosti sustava i mora zaštititi podatke i informacije. Pri definiranju sigurnosnih zahtjeva u obzir se uzimaju tri najbitnije kategorije[65]:

- procjena rizika
- propisani zakoni
- skup ciljeva, načela i poslovnih zahtjeva organizacije.

Postoji mnogo podjela i klasifikacija rizika kao na primjer; čisti (može biti krađa, elementarna nepogoda), temeljni, zajednički, pojedini, subjektivni, objektivni, poslovni, informatički, financijski.. Nebitno o kojoj se djelatnosti i entitetu radi, rizike je moguće podijeliti s obzirom na[66]:

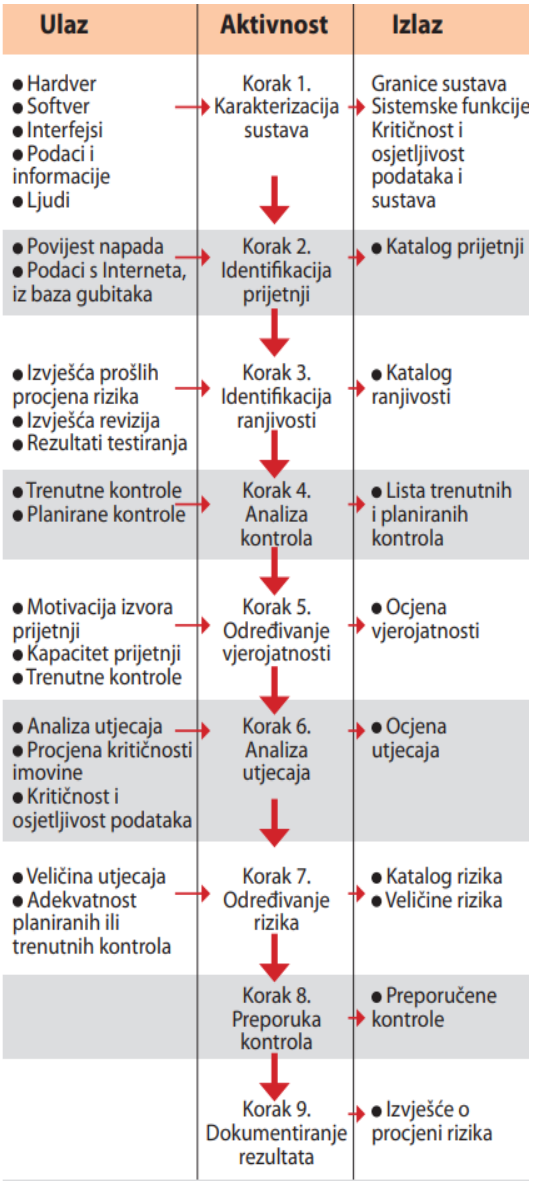
- pristup (opći i specifični rizici)
- vezivanje (poslovni i neposlovni rizici)
- porijeklo (unutarnji i vanjski rizik)
- očekivanje (realni i oportunitetni rizik)
- stvaranje dobiti (špekulativni i hazardni rizici)
- prijenos (prenosivi i neprenosivi rizici)
- mjerenje (mjerljivi i nemjerljivi rizici)
- utjecaj (objektivni i subjektivni rizici)
- nastup (direktni i indirektni rizici)
- pojavnost (tipični i netipični rizici)
- brzina (katastrofični i puzajući rizici).

[65] Boban, M. Nove tehnologije, intelektualno vlasništvo i informacijska sigurnost, Sveučilišni studijski centar za forenzične znanosti Split 2022. – prezentacije s predavanja
[66] Andrijanić, I., Gregurek, M., Merkaš, Z. Upravljanje poslovnim rizicima. Zagreb: Libertas – Plejada 2016 str. 43.-45.

7.1. Metodologija upravljanja rizikom

Procjena rizika prvi je korak u metodologiji upravljanja rizikom koji prate informacijski sustav, a sastoji se od devet koraka[67];

1. karakterizacija sustava (definira se cilj – detektiraju se granice informacijskog sustava zajedno sa hardverom i softverom koji čine sustav)
2. identificiranje prijetnji (procjenjuju se svi potencijalni izvori prijetnji koji mogu načiniti štetu sustavu; prirodne nepogode, tehnički kvarovi opreme, ljudski izvori prijetnji)
3. identificiranje ranjivosti (cilj je razvoj liste ranjivosti sustava – pogreške ili slabosti)
4. analiza kontrola (analizira se kontrola koja je primijenjena/planirana za organizaciju da bi se smanjila ili uklonila vjerojatnost da prijetnja iskoristi ranjivost sustava)
5. određivanje vjerojatnosti (motivacija i mogućnost prijetnje, priroda ranjivosti, postojanost i učinkovitost kontrola)
6. analiza utjecaja (određivanje štetnog utjecaja)
7. određivanje rizika (procjena nivoa rizika za informacijski sustav)
8. preporuka kontrola (preporučuju se kontrole koje mogu smanjiti/eliminirati rizik na način koji odgovara organizacijama)
9. dokumentiranje rezultata (rezultati se sastavljaju kao izvještaj koji sadrži prijetnje i ranjivosti, mjeri rizik i preporučuje kontrole primjene).



Slika 3. Koraci procjene prema NIST-u[68]

[67] cis.hr Osnove upravljanja rizikom (Internet) [pristupljeno 01.07.2022] Dostupno na https://www.cis.hr/files/Celuska-Osnove_upravljanja_rizikom.pdf

[68] Izvor: Uremović, D. Kako upravljati IT rizicima? (članak) [pristupljeno 01.07.2022] Dostupno na https://alterinfo.hr/lib/q55e1o/Upravljanje_rizicima-ku2buxeu.pdf

8. KIBERNETIKA

„Kibernetika je znanost koja istražuje opće zakonitosti procesa upravljanja i veza u bilo kojim sustavima (tehničkim, biološkim, ekonomskim, socijalnim, administrativnim i dr.).“[69]

Također postoji i definicija da je ona skup teorijskih disciplina i praktičnih postupaka koji se koriste pri vođenju složenih sustava. Naziv je uveo Norbert Wiener, američki matematičar, u svom djelu „Kibernetika ili kontrola i komunikacije u živim bićima i stroju“ iz 1948. godine. Osnovana je na ideji kibernetičkog sustava unutarnjih akcija i reakcija – nebitno da li se radi o elektroničkim strojevima ili o ljudskom mozgu – što je čovjeku osjet to je kibernetici informacija. Daljnji razvoj označava se kibernetičkom teorijom koju je razvijao Claude Shennon. Poslije toga, kibernetika se razvija kao suradnja mnogih disciplina (biologija, ekonomija, matematika, elektronika, fiziologija..).[70]

Kibernetički prostor je „virtualni prostor stvoren pomoću globalno umreženih računala tj. svijet interneta s njegovim okruženjem; također kiberprostor.“ U kibernetičkom prostoru ljudi mogu komunicirati, razmjenjivati ideje, trgovati, upoznavati se.. Kibernetički prostor je virtualan, realna stvarnost, koja sve više počinje biti pitanjem u međunarodnim odnosima. Kibernetički napadi stvaraju velike probleme i opasnosti za informacijske sustave raznih institucija i organizacija. [71]

Kibernetičke aktivnosti mogu se podijeliti na četiri područja[72]; kibernetički kriminal, kibernetička špijunaža, kibernetički terorizam i kibernetički rat.

[69] enciklopedija.lzmk.hr Leksikografski zavod Miroslav Krleža Kibernetika [pristupljeno 03.07.2022] Dostupno na http://enciklopedija.lzmk.hr/clanak.aspx?id=18859

[70] Obradović D. Kibernetika – što je to? Common Foundations 2018 - uniSTem: 6th Congress of Young Researchers in the Field of Civil Engineering and Related Sciences. Split: Sveučilište u Splitu, Fakultet građevinarstva, arhitekture i geodezije; 2018. str. 158-163. [pristupljeno 04.07.2022.] Dostupno na https://urn.nsk.hr/urn:nbn:hr:123:706233

[71] Brzica, N. Informacijska nadmoć: na sjecištu informacijskog i kibernetičkog ratovanja. Polemos, XXIII (47), 13-31. 2020. . [pristupljeno 04.07.2022.] Dostupno na https://hrcak.srce.hr/262944

[72] Vuković H. Kibernetska sigurnost i sustav borbe protiv kibernetskih prijetnji u Republici Hrvatskoj. National security and the future (Internet) 2012 [pristupljeno 05.07.2022.];13(3):12-31. Dostupno na: https://hrcak.srce.hr/100728 str.17.

8.1. Kibernetički kriminal

Odnosi se na kriminalne radnje koje uključuju mrežu, računalo i Internet, a to može biti krađa identiteta, prijevara, špijuniranje, krađa podataka ili informacija.[73]

Osobe koje se koriste kibernetičkim kriminalom rade to na način da odaberu neko računalo kao svoj cilj (napad poput krađe podataka, krađe identiteta, širenje virusa, zlonamjerne aktivnosti), koriste svoje računalo kao „oružje“ (sa svog računala šalju neželjene poruke, izvode prijevare) i kao svoj dodatni pribor za rad (spremanje nelegalno pribavljenih podataka). [74]

Konvencija o kibernetičkom kriminalu je oblik međunarodnog ugovora i kao takav važan je izvor međunarodnog prava kojim se uređuju odnosi između subjekata međunarodnog prava. Donijelo je Vijeće Europe 23.11.2001.godine, a stupila je na snagu 01.07.2004.godine, a 38 zemalja su potpisnice. Odredbe Konvencije nisu izravno primjenjive nego ih svaka država mora implementirati u svoje zakonodavstvo. Republika Hrvatska ratificirala je Konvenciju i odredbe unijela u Kazneni zakon Republike Hrvatske.[75]

8.2. Kibernetička špijunaža

Pojavljuje se kao oblik kibernetskog kriminala odnosno dobivanja informacija i podataka koje mogu biti profitabilne za hakera, bilo da se radi o grupi ili pojedincu. Događa se kroz neko određeno vrijeme kako bi se došlo do povjerljivih informacija. To je akt ili praksa pribavljanja podataka i informacija bez odobrenja vlasnika istih, koristeći se raznim metodama putem interneta, mreže ili pojedinačnih računala (ubacivanje programa u sustav – spyware, crvi, trojanac). Najčešće se pojavljuje na razini države, obavještajnih agencija, vojska, industrija da bi se stekla prednost – bolji proizvod od konkurencije, resursi države, podaci obavještajnih agencija.. Ima mnogo metoda prikupljanja podataka; skeniranje dokumenata, pronalaženje

[73] hr.eyewated.com Što je cyber-kriminal? (Internet) [pristupljeno 06.07.2022] Dostupno na https://hr.eyewated.com/cyber-%E2%80%8B%E2%80%8Bkriminal-sto-je-to/

[74] hr.theastrologypage.com Što je cyber-kriminal? – definicija iz tehopedije [pristupljeno 07.07.2022] Dostupno na https://hr.theastrologypage.com/cybercriminal

[75] Vojković, G., Štambuk-Sunjić, M. Konvencija o kibernetičkom kriminalu i kazneni zakon Republike Hrvatske 2005 Izvorni znanstveni članak [pristupljeno 07.07.2022] Dostupno na https://www.academia.edu/28199406/Konvencija_o_kiberneti%C4%8Dkom_kriminalu_i_kazneni_zakon_Republike_Hrvatske

lokacije, bube (mikrofoni), skrivene privatne mreže, kamere, keylogger, screen grabber, eksfiltracija, manipulacija materijala, prisluškivanje mobitela…[76]

8.3. Kibernetički rat

Rat koji se vodi računalima i mrežama koje ih povezuju. Većinom se provodi od strane jedne države protiv druge države, njihove vlade i vojske, da bi se uništila ili omela njihova upotreba. Vrlo česta je usporedba sa informacijskim i informatičkim ratom koji predstavljaju poduzete postupke da bi se postigla informacijska prednost nad protivnikom, istovremeno braneći svoje informacije, sustave i mreže.[77]

8.4. Kibernetički terorizam

To su planirani napadi od strane nacionalnih skupina ili pojedinaca koji su usmjereni protiv informacijskih sustava, računalnih programa i podataka koji za posljedicu imaju nasilje nad neborbenim metama. Spada pod podvrstu terorizma čije je „oružje“ informatika. Odvija se u kibernetskom prostoru a glavna karakteristika mu je da poluči nerazmjeran učinak u uništavanju, iskorištavanju, remećenju i obmanjivanju.[78]

8.5. Hibridni rat

Može se definirati kao veza između informatičkog i uobičajenog rata, to je vojno-politički fenomen. Informacije su glavno sredstvo odnosno „oružje“ kojim se želi nanijeti šteta državnoj vlasti – krive i lažne informacije, lažiranje događaja, izmišljene činjenice, špijunaža, propagandne akcije, obavještajne radnje, organizacija nereda unutar zemlje..[79]

---

[76] wikiwand.com (Internet) Kibernetička špijunaža [pristupljeno 07.07.2022] Dostupno na https://www.wikiwand.com/hr/Kiberneti%C4%8Dka_%C5%A1pijuna%C5%BEa

[77] Vuković H. Kibernetska sigurnost i sustav borbe protiv kibernetskih prijetnji u Republici Hrvatskoj. National security and the future [Internet]. 2012 [pristupljeno 09.07.2022.];13(3):12-31. Dostupno na https://hrcak.srce.hr/100728 str.19.

[78] Ibid. str.18.

[79] Cvrtila, Ž. Hibridni rat – suvremeni naziv za već poznate oblike ratovanja (stručni članak) 2017 [pristupljeno 09.07.2022.] Dostupno na https://www.bib.irb.hr/1086183

Hibridni rat koristi[80]:

- informacijske operacije (ometanje razmjene podataka)
- operacije psihološke prirode (stvaranje nepovjerenja prema državi u javnom životu)
- kibernetički napadi (neovlašten pristup tajnim podacima)
- ekonomski pritisak (sankcije, prestanak ulaganja)
- subverzivne operacije (podrška opozicijskim pokretima, aktivno korištenje protesta potencijalnih civilnih masa – sponzoriranje terorista i ekstremista, kriminalnih i destruktivno-opozicijskih snaga).

8.6. Kibernetička sigurnost u Republici Hrvatskoj

Prema SOA-i, Hrvatska je kao članica NATO-a i EU-a, na meti kibernetičkih napada. SOA je 2019.godine osnovala Centar za kibernetičku sigurnost kojoj je cilj zaštita nacionalnog kibernetičkog prostora. Zajedničkim snagama SOA i Zavod za sigurnost informacijskih sustava izgradili su sustav SK @UT koji predstavlja središnji sustav za otkrivanje, rano upozorenje i zaštitu od kibernetičkih napada i ugroza koji alarmira ključna državna tijela i pravne osobe. Vlada je 01.04.2021.godine donijela Odluku o mjerama i aktivnostima za podizanje nacionalnih sposobnosti pravovremenog otkrivanja i zaštite od državno sponzoriranih kibernetičkih napada, Advanced Persistent Threat (APT) kampanja te drugih kibernetičkih ugroza.[81]

Tijela koja se bave kibernetičkim prijetnjama u Republici Hrvatskoj su:

- Ured vijeća za nacionalnu sigurnost (UVNS)
- Zavod za sigurnost informacijskih sustava (ZSIS)
- Nacionalni CERT
- Odjel za visokotehnički kriminalitet
- Centar za sigurnosnu suradnju RACVIAC
- Agencija za zaštitu osobnih podataka (AZOP).

[80] Cvrtila, Ž. Hibridni rat – suvremeni naziv za već poznate oblike ratovanja (stručni članak) 2017 [pristupljeno 09.07.2022.] Dostupno na https://www.bib.irb.hr/1086183

[81] SOA – sigurnosno-obavještajna agencija (službena Internet stranica) [pristupljeno 10.07.2022.] Dostupno na https://www.soa.hr/hr/podrucja-rada/kiberneticka-sigurnost/

8.7. Kibernetički rizik

Informatički rizici označavaju kolika je vjerojatnost da će doći do nekog nepoželjnog događaja koji može uzrokovati štetu ili zastoj rada informacijskog sustava ili ugroziti informacije koje se u njemu nalaze. Kibernetički rizik spada pod vrstu informatičkog rizika.[82]

Svjedoci smo pojave modernog kriminala – kibernetičkog kriminala koji se događaju u obliku kibernetičke špijunaže, kibernetičkog ratovanja, kibernetičkog terorizma, kibernetičkih prijevara ili cyberbullyinga[83] koji mogu imati velike razorne posljedice.[84]

Da bi se donekle smanjili kibernetički rizici, postoje definirane četiri temeljne aktivnosti:[85]

1. Priprema – zahtjeva da se razumije kritična imovina, razvijanje sposobnosti da bi se riješili rizici raznih razina, utvrđivanje sklonosti rizicima i upravljanje rizicima treba provesti kroz cjelokupnu organizaciju.
2. Zaštita – osigurati dobro pripremljenu, utemeljenu i ponovljivu kibernetičku pripravnost, ocijeniti prijetnje i kontrole, osigurati provjeru procesa za treće osobe, omogućavanje i osnaživanje upravljanja incidentima, izrada i provedba plana za odgovor na incidente, neprestano usavršavanje.
3. Detekcija – razvijati i neprestano pratiti sposobnost za rješavanje prijetnji.
4. Poboljšanje – izgraditi bazu podataka incidenata i raditi na što kraćem roku za rješavanje i oporavak od incidenata.

---

[82] Spremić, M. Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije 2017 Zagreb Ekonomski fakultet Zagreb str. 74.

[83] Cyberbullying – jedna od najopasnijih internetskih prijetnji koja iskorištava žrtve u svrhu poniženja, o njima se objavljuje javno nekakav sadržaj koji im može naštetiti. To je čin zastrašivanja, prisiljavanja i ucjenjivanja žrtve putem prijetećih poruka, objavljivanja kompromitirajućih fotografija, videozapisa, otvaranja web stranice.. Ima mnogo vrsta; neprestano dosađivanje (slanje poruka), spolno napastovanje (slike, videozapisi, poruke sa seksualnim sadržajem), trolling (lažne poruke da bi se dobila emocionalna reakcija), doxing (izlazak – dijeljenje nečijih osobnih podataka u svrhu ponižavanja i osramoćivanja), fraping (stvaranje lažnog profila žrtve), omalovažavanje, somovi (stvaranje izmišljene osobnosti – internetska veza – novac), swatting (novi oblik – lažni pozivi hitnim službama), isključenje (odbacivanje žrtve iz društvenog kruga).

[84] Bara, D. Uloga cyber-osiguranja u upravljanju i prijenosu rizika cyber-sigurnosti, stručni članak Zbornika radova: Dani hrvatskog osiguranja 2015 [pristupljeno 12.07.2022.] Dostupno na https://www.bib.irb.hr/791437

[85] thecroforum.org Kiberotpornost – izazov kiberrizika i uloga osiguranja (Internet) [pristupljeno 12.07.2022.] Dostupno na https://www.thecroforum.org/2014/12/19/cyber-resilience-cyber-risk-challenge-role-insurance/

Digitalizacija, globalizacija i sve veća povezanost putem interneta dovode do povećanja kibernetičkog kriminala i kibernetičkih incidenata time ugrožavajući privatnost i zaštitu osobnih podataka koji su ključni kibernetički rizici.[86]

	Kategorija	Opis
1.	Krađa intelektualnog vlasništva	- gubitak imovine intelektualnog vlasništva, gubitak prihoda kao posljedica smanjenog udjela na tržištu
2.	Prekid poslovanja	- nastali troškovi, izgubljena dobit – razlog je kibernetički napad ili IT propust
3.	Gubitak podataka i aplikacija	-„vraćanje“ aplikacije ili softvera u rad zbog brisanja ili korumpiranosti
4.	Kibernetička iznuda	-incident koji zahtjeva plaćanje otkupnine za podatke i informacije
5.	Kibernetički kriminal/prijevara	-financijski gubitak koji proizlazi iz korištenja računala za djelo prijevare ili krađe novca, papira, informacija..
6.	Događaj povrede privatnosti	-istraživanje događaja povrede privatnosti, rad IT forenzičara, obavještavanje zahvaćenih nositelja podataka, odgovornost potraživanja trećih strana, kazne od regulatora i udruga
7.	Mrežne pogreške	-sigurnosni događaji preko kojih dolazi do napada treće osobe
8.	Utjecaj ne reputaciju	-gubitci prihoda koji dolaze iz odljeva kupaca ili smanjenja transakcija
9.	Fizičko oštećenje imovine	-gubitak prve strane zbog uništenja fizičke imovine proizašle iz kibernetičkih napada
10.	Smrt i tjelesna ozljeda	-odgovornost trećih osoba za smrt i ozljede koje su proizašle iz kibernetičkih napada
11.	Istraživanje incidenta i troškovi odgovora	-troškovi nastali istraživanjem i zatvaranjem incidenta

Tablica 3. Autor[87] – Kategorije gubitaka kao posljedica kibernetičkih napada

[86] Bara, D. Uloga cyber-osiguranja u upravljanju i prijenosu rizika cyber-sigurnosti, stručni članak Zbornika radova: Dani hrvatskog osiguranja 2015. [pristupljeno 14.07.2022.] Dostupno na https://www.bib.irb.hr/791437

[87] Tablica: autor prema - Bara, D. Uloga cyber-osiguranja u upravljanju i prijenosu rizika cyber-sigurnosti, stručni članak Zbornika radova: Dani hrvatskog osiguranja 2015. [pristupljeno 14.07.2022.] Dostupno na https://www.bib.irb.hr/791437

9. SIGURNOSNA POLITIKA

Sigurnosna politika je skup pravila i postupaka koji određuju razinu sigurnosti nekog informacijskog sustava s fokusom na tehnologiju i informacije koje informacijski sustav sadržava. Sigurnosna politika nameće korisnicima obvezna pravila ponašanja i obveze da bi se zaštitilo informacijski sustav, točnije podatke koji se u njemu nalaze, od vanjskih utjecaja (maliciozni programi, napadi s daljine i slično) ali i od korisnika (neovlašteno korištenje podataka, krađa informacija, izmjena i slično). [88]

Sigurnosna politika je službena izjava ili plan organizacije koji uključuje ciljeve, smjernice te prihvatljive postupke, a zahtjeva poštivanje pravila koja su njome definirana, ukazuje da nepoštivanje tih pravila može dovesti do sankcija ili kazni nadležnih tijela ili institucija te da se sigurnosna politika temelji na već definiranim standardima. Provođenjem sigurnosne politike korisnicima su nametnuta pravila ophođenja koja im ograničavaju slobodu pregleda i dostupnosti povjerljivih informacija, ali i pravila za ispravno korištenje računalne opreme koja im je dostupna i dana na korištenje.[89]

Sigurnosna politika određuje što zaštiti ali ne i na koji način zaštiti informacijski sustav. Nemoguće je općenito definirati sigurnosnu politiku za informacijske sustave jer se napretkom tehnologije pojavljuju nove metode koje znače ugrozu za sustav. Sigurnosna politika namijenjena korisnicama mora biti jasna i kratka tako da je mogu razumjeti, mora biti naglašeno što je prihvatljivo ponašanje, a što ne sve radi zaštite vrijednosti informacijskog sustava.[90]

Standard se odnosi na pravila koja su donesena da bi se politiku učinilo suvislom i učinkovitom, a mora sadržavati jedan ili više tehničkih opisa za komponente računala i programe kao i njihovo rukovanje. Smjernice su upute ili preporuke koje daju naputke za provedbu sigurnosne politike, napravljene tako da se ostvare ciljevi sigurnosne politike. One nisu obvezujuće nego imaju savjetodavni karakter za uspostavu sigurnosne politike.[91]

---

[88] CARNet – Hrvatska akademska i istraživačka mreža (Internet) [pristupljeno 16.07.2022.] Dostupno na https://www.cert.hr/wp-content/uploads/2009/05/CCERT-PUBDOC-2009-05-265.pdf
[89] Ibid.
[90] Ibid.
[91] Ibid.

9.1. Zakonska regulativa o pitanjima informacijske sigurnosti u Republici Hrvatskoj

U Republici Hrvatskoj postoji mnogo zakona i podzakonskih akata koji se odnose na informacijsku sigurnost, a ovo su neki od njih (nabrojani i objašnjeni ukratko);

- Zakon o informacijskoj sigurnosti
- Zakon o pravu na pristup informacijama
- Zakon o sigurnosno-obavještajnom sustavu Republike Hrvatske
- Zakon o tajnosti podataka
- Zakon o sigurnosnim provjerama
- Zakon o elektroničkoj ispravi
- Zakon o provedbi Uredbe (EU) br.910/2014 Europskog parlamenta i Vijeća od 23.07.2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ
- Uredba o sigurnosnoj provjeri za pristup klasificiranim podacima
- Uredba o mjerama informacijske sigurnosti
- Uredba o načinu označavanja klasificiranih podataka, sadržaju i izgledu uvjerenja o obavljenoj sigurnosnoj provjeri i izjave o postupanju s klasificiranim podacima
- Nacionalna strategija kibernetičke sigurnosti i akcijski plan za provedbu strategije
- Zakon o provedbi opće uredbe o zaštiti podataka
- Opća uredba o zaštiti podataka (Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ)

9.1.1. Zakon o informacijskoj sigurnosti

Najvažniji zakon koji se odnosi i uređuje sigurnost informacijskih sustava. Njime se definira informacijska sigurnost, koja su njena područja i nadležna tijela koja donose, provode i nadziru mjere i standarde informacijske sigurnosti. U člancima su utvrđeni minimalni kriteriji koji se odnose na zaštitu podataka. Donesen je za sva državna tijela, tijela jedinica lokalne i

regionalne samouprave i na pravne osobe s javnim ovlastima koje u svom radu koriste klasificirane i neklasificirane podatke, ali i za pravne i fizičke osobe koje imaju pristup takvim podacima. Nadzor provode savjetnici za informacijsku sigurnost (nadzor organizacije, provedba i učinkovitost propisanih mjera).[92]

9.1.2. Zakon o pravu na pristup informacijama

Uređuje se pravo na pristup informacijama i ponovnu uporabu informacija koje imaju tijela javne vlasti, propisuju se načela prava na pristup informacijama i ponovnu upotrebu informacija, ograničenja prava na pristup informacijama, postupak za ostvarivanje i zaštitu prava na pristup informacijama, postupak za ostvarivanje i zaštitu prava na pristup informacijama, djelokrug, način i uvjete rada za imenovanje Povjerenika za informiranje, inspekcijski nadzor, prekršajne odredbe i ostale obveze tijela javne vlasti. [93]

9.1.3. Zakon o sigurnosno-obavještajnom sustavu Republike Hrvatske

Ovaj zakon donosi se radi očuvanja nacionalne sigurnosti i prijetnji koje su usmjerene protiv neovisnosti, jedinstvenosti i suvereniteta Republike Hrvatske, nasilnom rušenju državne vlasti, ugrožavanju temeljnih ljudskih prava i sloboda utvrđenih Ustavom i zakonima i to tako da se osnivaju sigurnosno-obavještajne agencije: SOA (sigurnosno-obavještajna agencija) i VSOA (vojna sigurnosno-obavještajna agencija).[94] SOA prikuplja podatke od važnosti za nacionalnu sigurnost, obrađuje ih i analizira, pruža obavještajnu potporu nadležnim državnim tijelima i donositeljima političkih odluka.[95] VSOA za zadaću ima prikupljanje, analizu, obradu i procjenu podataka o vojskama i obrambenim sustavima drugih zemalja, o vanjskim pritiscima koji mogu imati utjecaj na obrambenu sigurnost, poduzima mjere otkrivanja i praćenja ugroze obrane države.[96]

---

[92] ZoIS

[93] Zakon o pravu na pristup informacijama (NN 25/13, 85/15, 69/22) Dostupno na https://zakon.hr/z/126/Zakon-o-pravu-na-pristup-informacijama

[94] Zakon o sigurnosno-obavještajnom sustavu Republike Hrvatske (NN 79/06, 105/06) Dostupno na https://zakon.hr/z/744/Zakon-o-sigurnosno-obavje%C5%A1tajnom-sustavu-Republike-Hrvatske

[95] SOA – sigurnosno-obavještajna agencija (službena Internet stranica) [pristupljeno 21.07.2022] Dostupno na https://www.soa.hr/hr/o-nama/sto-je-soa/

[96] morh.hr Ministarstvo obrane RH (službena Internet stranica) [pristupljeno 21.07.2022] Dostupno na https://www.morh.hr/o-vojnoj-sigurnosno-obavjestajnoj-agenciji/

9.1.4. Zakon o tajnosti podataka

Definira i utvrđuje što su klasificirani i neklasificirani podaci, stupnjeve tajnosti (vrlo tajno, tajno, povjerljivo, ograničeno), postupak klasifikacije i deklasifikacije, pristup takvim podacima, njihovu zaštitu i nadzor nad provedbom Zakona. Odnosi se na državna tijela, jedinice lokalne i područne samouprave, pravne osobe s javnim ovlastima, ali i fizičke i pravne osobe koje prema ovom Zakonu imaju pravo pristupa ovoj vrsti podataka.[97] Tajna je podatak koji je poznat i smije biti poznat samo određenom krugu ljudi i pritom mora postojati društvena norma koja zabranjuje iznošenje tih podataka izvan kruga. U širem poimanju, tajna predstavlja sve ono što je nepoznato, a u užem se javlja u međuljudskim odnosima i sačinjavaju je činjenice koje određene grupe osoba ili institucija čuvaju za sebe i skrivaju od drugih – javnosti.[98]

9.1.5. Zakon o sigurnosnim provjerama

Ovim Zakonom određuje se pojam, vrsta i stupanj sigurnosne provjere (postupak kojim nadležno tijelo utvrđuje sigurnosne zapreke za pravne i fizičke osobe), sigurnosne zapreke (provjera jesu li činjenice koje ukazuju na neki rizik ili zlouporabu radnog mjesta ili dužnosti, nekih prava ili ovlasti na štetu nacionalne sigurnosti ili interesa Republike Hrvatske) i postupak provođenja istih.[99]

9.1.6. Zakon o elektroničkoj ispravi

Uređuje pravo pravnih i fizičkih osoba na upotrebu elektroničke isprave u svim poslovnim radnjama i djelatnostima te u postupcima koji se vode pred tijelima javne vlasti u kojima se elektronička oprema i programi mogu primjenjivati u izradi, prijenosu, pohrani i čuvanju informacija u elektroničkom obliku, pravna valjanost elektroničke isprave te uporaba i promet elektroničkih isprava. Elektronička isprava ima istu pravnu snagu kao i ona na papiru.[100]

---

[97] Zakon o tajnosti podataka (NN 79/07, 86/12) Dostupno na https://zakon.hr/z/217/Zakon-o-tajnosti-podataka

[98] Čizmić J.,. Boban M., Zlatović D., , Nove tehnologije, intelektualno vlasništvo i informacijska sigurnost, Sveučilište u Splitu Pravni fakultet, Split 2016 str. 691.

[99] Zakon o sigurnosnim provjerama (NN 85/08, 86/12) Dostupno na https://zakon.hr/z/536/Zakon-o-sigurnosnim-provjerama

[100] Zakon o elektroničkoj ispravi (NN 150/05) Dostupno na https://zakon.hr/z/272/Zakon-o-elektroni%C4%8Dkoj-ispravi

9.1.7. Zakon o provedbi uredbe (EU) br.910/2014 Europskog parlamenta i Vijeća od 23.07.2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ

Ovim Zakonom utvrđuju se nadležna tijela i njihove zadaće za provedbu Uredbe, tijela za inspekcijski nadzor nad provođenjem Uredbe, tijelo za ocjenu sukladnosti, prekršajne odredbe, utvrđuju se prava i obveze potpisnika i pružatelja usluga.[101]

9.1.8. Uredba o sigurnosnoj provjeri za pristup klasificiranim podacima

Propisuje za koje se osobe provodi sigurnosna provjera, vrste i postupak provođenja sigurnosnih mjera da bi ostvarile pristup klasificiranim podacima (zaposlenici u državnim tijelima, fizičke i pravne osobe koje obavljaju poslove za državna tijela, temeljem međunarodnih ugovora Republike Hrvatske s drugim državama). Provjeru provodi SOA i VSOA.[102]

9.1.9. Zakon o provedbi opće uredbe o zaštiti podataka

To je pravni akt kojim se osigurava provedba Uredbe (EU) 2016/679 Europskog parlamenta i Vijeća i odnosi se na zaštitu pojedinaca u vezi s obradom osobnih podataka, zaštitu od prijetnji javnoj sigurnosti, nacionalnoj sigurnosti i obrani. Određuje novčane kazne za kršenje odredbi. Nadzorno tijelo je Agencija za zaštitu osobnih podataka.[103]

9.1.10. Uredba o mjerama informacijske sigurnosti

Ova Uredba utvrđuje mjere informacijske sigurnosti za rukovanje s klasificiranim i neklasificiranim podacima. Odnosi se ponajviše na državna tijela, tijela jedinica lokalne

[101] Zakon o provedbi Uredbe br. 910/2014 Europskog parlamenta i Vijeća od 23.07.2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ (NN 62/17) Dostupno na https://www.zakon.hr/z/923/Zakon-o-provedbi-Uredbe-%28EU%29-br.-910-2014-Europskog-parlamenta-i-Vije%C4%87a-od-23.-srpnja-2014.-o-elektroni%C4%8Dkoj-identifikaciji-i-uslugama-povjerenja-za-elektroni%C4%8Dke-transakcije-na-unutarnjem-tr%C5%BEi%C5%A1tu-i-stavljanju-izvan-snage-Direktive-1999-93-EZ

[102] Uredba o sigurnosnoj provjeri za pristup klasificiranim podacima (NN 72/2007) Dostupno na https://narodne-novine.nn.hr/clanci/sluzbeni/2007_07_72_2237.html

[103] Zakon o provedbi Opće uredbe o zaštiti podataka (NN 42/18) https://www.zakon.hr/z/1023/Zakon-o-provedbi-Op%C4%87e-uredbe-o-za%C5%A1titi-podataka

samouprave i pravne osobe s javnim ovlastima, ali i na fizičke i pravne osobe koje imaju pravo pristupa takvim podacima.[104]

9.1.11. Uredba o načinu označavanja klasificiranih podataka, sadržaju i izgledu uvjerenja o obavljenoj sigurnosnoj provjeri i izjave o postupanju s klasificiranim podacima

Ova Uredba propisuje način kako označiti klasificirani i neklasificirani podatak, izgled i sadržaj Uvjerenja o obavljenoj sigurnosnoj provjeri i izgled Izjave o postupanju s klasificiranim podacima. Odnosi se na tijela ovlaštena za klasifikaciju i deklasifikaciju podataka i pravne i fizičke osobe koje postupaju s njima.[105]

9.1.12. Nacionalna strategija kibernetičke sigurnosti i akcijski plan za provedbu strategije

Nacionalna strategija kibernetičke sigurnosti je dokument kojim Hrvatska sustavno i sveobuhvatno planira najvažnije aktivnosti radi zaštite svih korisnika elektroničkih usluga u privatnom i javnom sektoru. Strategija otkriva vrijednosti koje trebaju biti zaštićene, poduzima mjere iz svoje nadležnosti, razmjenjuje podatke, prilagođava se i to sve kako bi kibernetički prostor bio dostupan, otvoren, siguran i uređen za upotrebu.[106]

Cilj izrade Strategije razrađen je u Akcijskom planu, usuglašen sa Strategijom kibernetičke sigurnosti Europske unije[107], usmjeren na osposobljavanje i koordinaciju svih sektora društva što se postiže zajedničkim koordiniranjem raznih institucija. Strategija se donosi

---

[104] Uredba o mjerama informacijske sigurnosti (NN 46/2008) Dostupno na https://narodne-novine.nn.hr/clanci/sluzbeni/2008_04_46_1547.html

[105] Uredba o načinu označavanja klasificiranih podataka, sadržaju i izgledu Uvjerenja o obavljenoj sigurnosnoj provjeri i Izjave o postupanju s klasificiranim podacima (NN 102/2007) Dostupno na https://narodne-novine.nn.hr/clanci/sluzbeni/2007_10_102_2985.html

[106] Nacionalna strategija kibernetičke sigurnosti i Akcijski plan za provedbu Strategije [pristupljeno 27.07.2022] Dostupno na https://mup.gov.hr/UserDocsImages/dokumenti/kiberneticka_sigurnost/Sa%C5%BEetak%20Nacionalne%20strategije%20kiberneti%C4%8Dke%20sigurnosti.pdf

[107] europa.eu – službena Internet stranica EU Strategija kibersigurnosti [pristupljeno 28.07.2022] Dostupno na https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy

na postojećim zakonima ali dolazi do potrebe da se neka zakonska rješenja preispitaju i usklade kroz provedbu mjera Akcijskog plana.[108]

Opći ciljevi Strategije[109]:

- sustavni pristup u primjeni i razvoju nacionalnog zakonodavnog okvira
- provođenje aktivnosti i mjera u svrhu povećanja sigurnosti, otpornosti i pouzdanosti kibernetičkog prostora
- uspostavljanje učinkovitijeg mehanizma razmjene, ustupanja i pristupa podacima
- jačanje svijesti o sigurnosti
- poticanje razvoja usklađenih obrazovnih programa
- poticanje razvoja e-usluga
- poticanje istraživanja i razvoja
- sustavni pristup međunarodnoj suradnji.

9.1.13. Opća uredba o zaštiti podataka (uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27.04.2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage direktive 95/46/EZ)

Eng. *General Dana Protection Regulation – GDPR* – svim građanima Europske unije omogućava bolju kontrolu nad njihovim osobnim podacima, direktno se primjenjuje u zemljama članicama bez implementacije u nacionalno zakonodavstvo. Cilj i svrha joj je uskladiti regulativu na polju upravljanja osobnima podacima i svim drugim podacima koji su vezani za pojedince u cijeloj Europskoj uniji i njenim državama članicama. Ovime se traži bolji uvid gdje i kako se koriste osobni podaci, kako se spremaju i transportiraju, kakav je pristup tim podacima.[110]

Podaci se smatraju osobnima ako se iz njih s velikom vjerojatnošću može otkriti identitet osobe (ime i prezime, broj osobne iskaznice, lokacijski podaci, zdravstveni karton, biometrijski

[108] Nacionalna strategija kibernetičke sigurnosti i Akcijski plan za provedbu Strategije [pristupljeno 29.07.2022] Dostupno na https://mup.gov.hr/UserDocsImages//dokumenti/kiberneticka_sigurnost//Sa%C5%BEetak%20Nacionalne%20strategije%20kiberneti%C4%8Dke%20sigurnosti.pdf

[109] Ibid.

[110] iusinfo.hr Zbirka propisa, sudske prakse i pravne literature u RH (Internet) [pristupljeno 29.07.2022] Dostupno na https://www.iusinfo.hr/document?sopi=DDHR20181007N112

podaci, genetski podaci (DNA), vjerska i filozofska uvjerenja, etnička pripadnost, ekonomsko stanje, članstvo u sindikatu, seksualna orijentacija i spolni život, IP adresa, osobne poruke e-pošte, kolačići u pregledniku, pseudonimizirani podaci). GDPR iznimno je kompleksan.[111]

Pojavljuju se i dosad neviđene kazne za nepoštivanje Uredbe – do 4% ukupnog godišnjeg prometa na svjetskoj razini ili do 20 milijuna eura – ovisi koja vrijednost je viša.[112]

9.2. Institucije informacijske sigurnosti u Republici Hrvatskoj

Republika Hrvatska donosi mnoge zakone i podzakonske akte vezane za informacijsku sigurnost i samim time osniva institucije koje brinu da se ti zakoni provode;

- Ured vijeća za nacionalnu sigurnost
- Zavod za sigurnost informacijskih sustava
- Nacionalni CERT
- Agencija za zaštitu osobnih podataka
- Agencija za podršku informacijskim sustavima i informacijskim tehnologijama (APIS IT)
- Odjel za visokotehnološki kriminal
- Regionalno središte za kibernetsku sigurnost unutar Centra za sigurnosnu suradnju – RACVIAC
- Središnji državni ured za e-Hrvatsku.

[111] gdprinformer.com Vodič kroz GDPR za početnike? (Internet) [pristupljeno 30.07.2022] Dostupno na https://gdprinformer.com/hr/vodic-kroz-gdpr

[112] Čizmić, J., Boban, M. Učinak nove EU Uredbe 2016/679 (GDPR) na zaštitu osobnih podataka u Republici Hrvatskoj, Zbornik Pravnog fakulteta Sveučilišta u Rijeci, vol. 39, br. 1, 377-410, 2018 [pristupljeno 30.07.2022] Dostupno na https://www.researchgate.net/publication/326182255_Ucinak_nove_EU_Uredbe_2016679_gdpr_na_zastitu_osobnih_podataka_u_Republici_Hrvatskoj str.21.

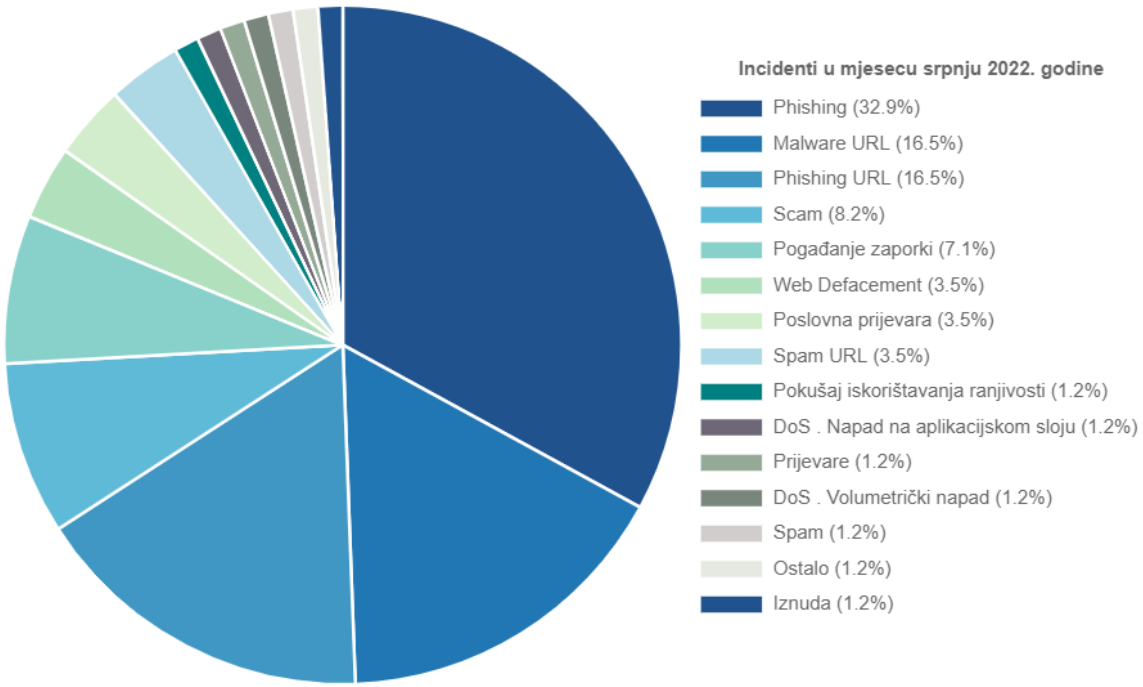
9.2.1. Nacionalni CERT

To je odjel Hrvatske akademske i istraživačke mreže CARNET koji je osnovan na temelju Zakona o informacijskoj sigurnosti radi prevencije i zaštite od računalnih ugroza sigurnosti javnih informacijskih sustava u Republici Hrvatskoj. Osnovni cilj i zadatak je obrada računalno-sigurnosnih incidenata da bi se očuvala kibernetička sigurnost, ali samo ako se jedna od strana nalazi u Republici Hrvatskoj. CERT.hr u svojoj domeni provodi proaktivne i reaktivne mjere. Proaktivne mjere koriste se da bi se spriječila ili umanjila moguća šteta i podrazumijevaju aktivno praćenje stanja na području računalne sigurnosti, praćenje računalno-sigurnosnih tehnologija, provođenje detaljne edukacije za određene grupe korisnika, provjeru ranjivosti za ustanove članice CARNET-a, izdavanje elektroničkih certifikata… Reaktivne mjere služe da bi se suzbili incidenti koji ugrožavaju informacijsku sigurnost u Republici Hrvatskoj, u njima se prikupljaju i obrađuju i pripremaju sigurnosne preporuke o slabostima u informacijskim sustavima te koordinacija rješavanja značajnijih incidenata. U djelokrug rada nije uključeno podnošenje kaznenih prijava, rješavanje problema, kažnjavanje korisnika, arbitraža u sporovima.[113]

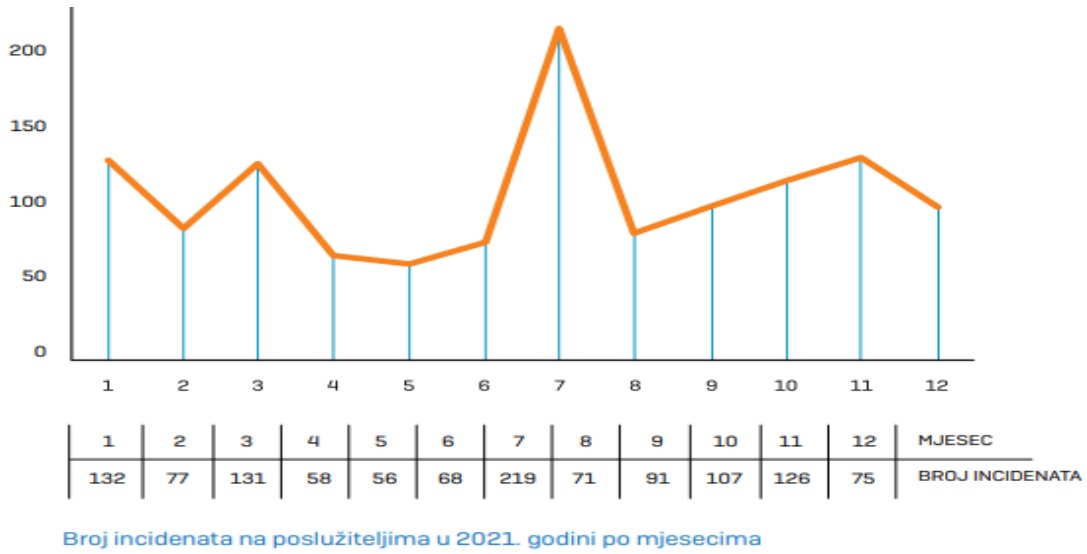
Sigurnosni incident koji se dogodi treba se odmah prijaviti nadležnim ustanovama. Odnosi se na neplanirani događaj koji za posljedicu ima povredu propisa, sigurnosnu politiku i načela informacijskog sustava te pravilnika u raznim ustanovama koji su vezani za informacijsku sigurnost.[114] Zaposlenike je potrebno uputiti i educirati što je sigurnosni incident te kako ga prepoznati i što napraviti ukoliko se on dogodi. Ovo su neki od koraka[115]:

- prijava sigurnosnog incidenta (što prije ga prijaviti u što kraće vrijeme)
- prijava ranjivosti sustava (prijaviti u što kraće vrijeme nadležnima)
- upravljanje sigurnosnim prijavama (definirati procedure)
- odgovornosti i procedure (definirati procedure i postupke da bi se zaštitilo od ponavljanja).

[113] cert.hr O nama (službena Internet stranica) [pristupljeno 31.07.2022.] Dostupno na https://www.cert.hr/onama/
[114] hnb.hr Hrvatska narodna banka Smjernice za upravljanje informacijskim sustavom u cilju smanjenja operativnog rizika (službena Internet stranica) [pristupljeno 31.07.2022.] Dostupno na https://www.hnb.hr/-/smjernice-za-upravljanje-informacijskim-sustavom-u-cilju-smanjenja-operativnog-rizika str.67.
[115] cert.hr Službena politika (službena Internet stranica) [pristupljeno 31.07.2022.] Dostupno na https://www.cert.hr/wp-content/uploads/2009/05/CCERT-PUBDOC-2009-05-265.pdf str.23.



Slika 4. Postotak računalno-sigurnosnih incidenata u mjesecu srpnju 2022.godine.[116]



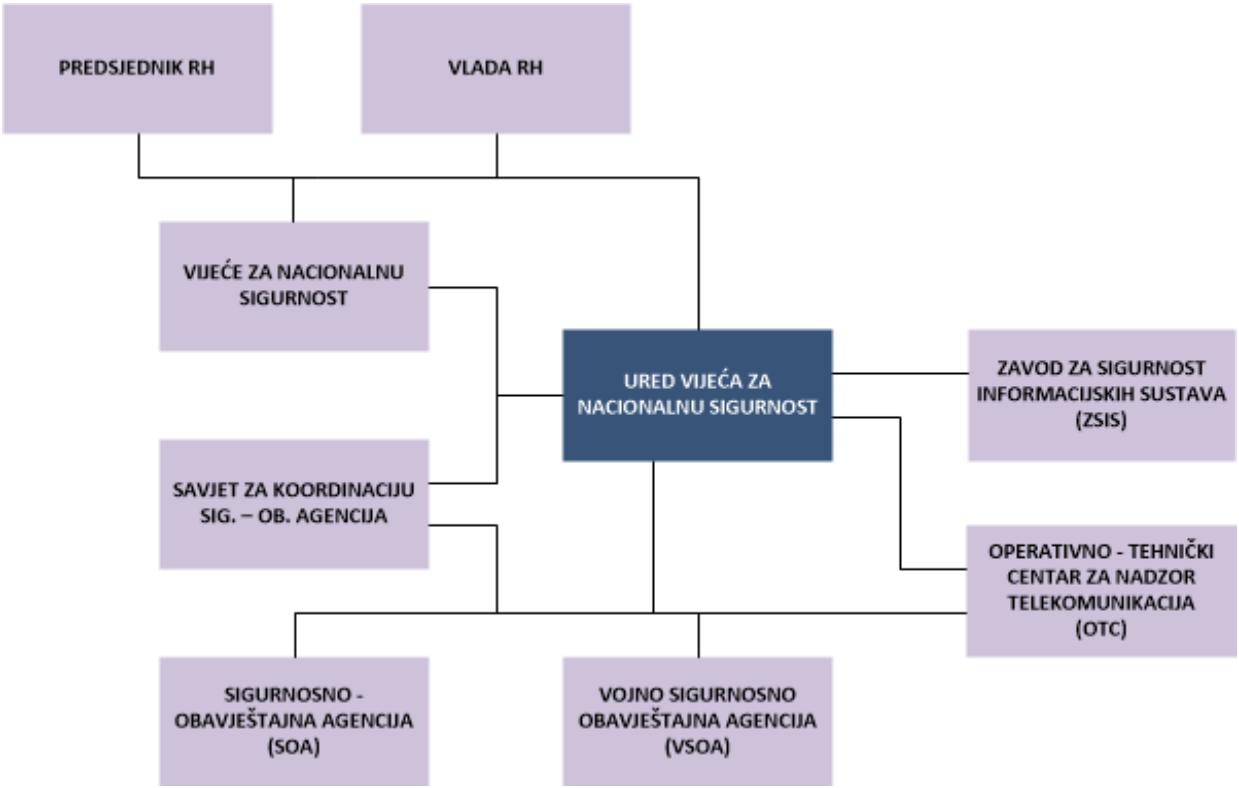
Slika 5. Broj incidenata na poslužiteljima u 2021. godini po mjesecima prema CERT-u[117]

[116] Izvor: cert.hr [pristupljeno 31.07.2022.] Dostupno na https://www.cert.hr/statistika/

[117] Izvor: cert.hr [pristupljeno 31.07.2022.] Dostupno na https://www.cert.hr/wp-content/uploads/2022/03/CERT-godisnje-izvjesce-2021.pdf

9.2.2. Ured vijeća za nacionalnu sigurnost (UVNS)

Središnje je državno tijelo za informacijsku sigurnost koje obavlja stručne i administrativne poslove za Vijeće za nacionalnu sigurnost i Savjet za koordinaciju sigurnosno-obavještajnih agencija te administrativne poslove za Koordinaciju za sustav domovinske sigurnosti ali i poslove za Predsjednika Republike Hrvatske i Vladu koji im daju uvid u rad sigurnosno-obavještajnih agencija i tijela sigurnosno obavještajnog sustava. UVNS koordinira, usklađuje donošenje i nadzire primjenu mjera i standarda informacijske sigurnosti.[118] Funkcija UVNS utemeljena je na trajnom usklađivanju propisanih mjera i standarda informacijske sigurnosti u RH s međunarodnim standardima i preporukama te sudjeluje u nacionalnoj normizaciji područja informacijske sigurnosti.[119]



Slika 6. UVNS u sigurnosno-obavještajnom sustavu RH[120]

[118] uvns.hr Ured Vijeća za nacionalnu sigurnost (službena Internet stranica) [pristupljeno 01.08.2022.] Dostupno na https://www.uvns.hr/hr/hr/o-nama/uvodna-rijec

[119] Boban M, Perišić M. Biometrija u sustavu sigurnosti, zaštite i nadzora informacijskih sustava. Zbornik radova Veleučilišta u Šibeniku (Internet) 2015 [pristupljeno 01.08.2022] (1-2/2015):115-148. Dostupno na https://hrcak.srce.hr/142285 str.122.

[120] Izvor: uvns.hr O nama [pristupljeno 01.08.2022.] Dostupno na https://www.uvns.hr/hr/o-nama/shema-uvns-u-sigurnosno-obavjestajnom-sustavu-rh

9.2.3. Zavod za sigurnost informacijskih sustava

Središnje državno tijelo koje obavlja poslove u tehničkim područjima informacijske sigurnosti državnih tijela Republike Hrvatske. Poslovi obuhvaćaju standarde sigurnosti, sigurnosnu akreditaciju, upravljanje kripto materijalima koji se koriste za razmjenu klasificiranih podataka, koordinaciju prevencije i otklanjanja problema vezanih uz sigurnost računalnih mreža u držanim tijelima, a sve to u suradnji s Uredom Vijeća za nacionalnu sigurnost.[121] Djelokrug i zadaće propisane su Zakonom o sigurnosno-obavještajnom sustavu Republike Hrvatske, Zakonom o informacijskoj sigurnosti te Uredbom Republike Hrvatske o mjerama informacijske sigurnosti. Osim gore nabrojanih zadaća, Zavod istraživa, razvija i ispituje tehnologiju namijenjenu zaštiti klasificiranih podataka i za reguliranje standarda tehničkih područja sigurnosti informacijskih sustava.[122]

9.2.4. Agencija za zaštitu osobnih podataka

To je neovisno i samostalno tijelo sa svojstvima pravne osobe i odgovara Hrvatskom saboru, ima nadzorne ovlasti, savjetodavnu ulogu i ovlasti intervencije.[123] Osnovana je na temelju Zakona o zaštiti osobnih podataka. Glavni zadaci Agencije su učinkovito djelovanje na ispunjavanje svih prava i obveza iz domene zaštite osobnih podataka, povećanje odgovornosti svih sudionika u procesu obrade osobnih podataka uz primjenu mjera informacijske sigurnosti. Ima trajnu zadaću podizati razinu svijesti svih sudionika o važnosti zaštite osobnih podataka, njihovim pravima i obvezama te predlaganje mjera za unaprjeđivanje zaštite osobnih podataka. Nadležna je za izvršavanje zadaća i ovlasti koje su joj povjerene u skladu s Općom uredbom o zaštiti podataka na području Republike Hrvatske.[124]

---

[121] Boban M, Perišić M. Biometrija u sustavu sigurnosti, zaštite i nadzora informacijskih sustava. Zbornik radova Veleučilišta u Šibeniku (Internet) 2015 [pristupljeno 02.08.2022] (1-2/2015):115-148. Dostupno na https://hrcak.srce.hr/142285 str.122

[122] zsis.hr Zavod za sigurnost informacijskih sustava (službena Internet stranica) [pristupljeno 02.08.2022] Dostupno na https://www.zsis.hr/default.aspx?id=13

[123] Boban M, Perišić M. Biometrija u sustavu sigurnosti, zaštite i nadzora informacijskih sustava. Zbornik radova Veleučilišta u Šibeniku [Internet]. 2015 [pristupljeno 02.08.2022] (1-2/2015):115-148. Dostupno na https://hrcak.srce.hr/142285 str.122

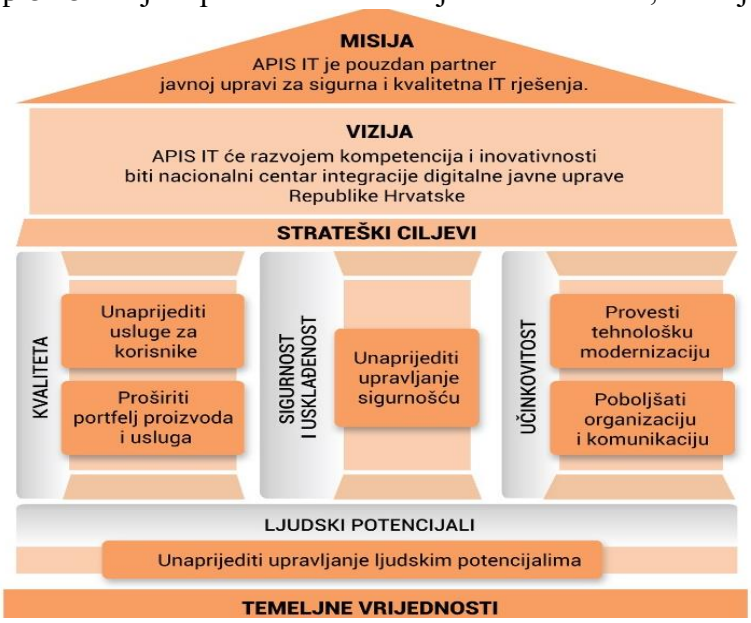
[124] azop.hr Agencija za zaštitu osobnih podataka (službena Internet stranica) [pristupljeno 02.08.2022] Dostupno na https://azop.hr/djelokrug/

9.2.5. Središnji državni ured za e-Hrvatsku

Glavni cilj i zadatak središnjeg državnog ureda za e-Hrvatsku bio je promicanje i sustavno unapređivanje izgradnje informacijsko-komunikacijske infrastrukture u Republici Hrvatskoj, razvitak primjene informacijske i komunikacijske tehnologije i sustava elektroničke uprave te javnog pristupa internetskim uslugama i sadržajima. Prestao je s radom 2011.godine kada je pripojen Ministarstvu uprave kada su mu uz nabrojene ciljeve dodani i poslovi modernizacije i informatizacije.[125]

9.2.6. Agencija za podršku informacijskim sustavima i informacijskim tehnologijama (APIS IT)

Osnovana 2005.godine ugovorom između Vlade Republike Hrvatske i Grada Zagreba s ciljem obavljanja poslova razvoja i podrške informacijskim sustavima Republike Hrvatske i Grada Zagreba te razvijanja aplikativnih servisa i čuvanja potrebnih informacijskih baza. APIS IT nudi usluge razvoja, projektiranja, implementaciju i podršku informacijskim sustavima, razvoja integriranih IT rješenja, usluge savjetovanja u IT projektima, pružanje IT podrške. Cilj je održavanje i izgradnja sustava koji omogućava komunikaciju unutar tijela javne uprave ali i s europskim organizacijama i institucijama radi što brže, učinkovitije i prilagođenije uprave za građane i stvaranje uprave budućnosti.[126]



Slika 7. Misija, vizija i strategija APIS IT-a[127]

[125] Wikipedia.org Središnji državni ured za e-Hrvatsku (Internet) [pristupljeno 03.08.2022] Dostupno na https://hr.wikipedia.org/wiki/Sredi%C5%A1nji_dr%C5%BEavni_ured_za_e-Hrvatsku

[126] apis-it.hr Agencija za podršku informacijskim sustavima i informacijskim tehnologijama (službena Internet stranica) [pristupljeno 04.08.2022] Dostupno na https://www.apis-it.hr/apisit/index.html#/page?docId=862092FC53B6F468C1257F400043EACF

9.2.7. Odjel za visokotehnološki kriminal

Ustrojen je u sklopu Ravnateljstva policije, Službe za gospodarski kriminalitet i korupciju, Uredbom o unutarnjem ustrojstvu MUP-a Republike Hrvatske 2012.godine i u njemu rade specijalizirani policijski službenici u suradnji s Nacionalnim CERT-om, CARNet-om te Zavodom za sigurnost informacijskih sustava s ciljem jedinstvenog učinkovitog nacionalnog odgovora na kibernetički kriminal. Njihov rad obuhvaća kaznena djela iz kibernetičkog kriminala i kaznena djela na štetu intelektualnog vlasništva. [128]

9.2.8. Regionalno središte za kibernetsku sigurnost unutar centra za sigurnosnu suradnju – RACVIAC

RACVIAC je međunarodna, neovisna organizacija koja za cilj ima poticanje suradnje što se tiče sigurnosnih pitanja u jugoistočnoj Europi kroz partnerstvo između zemalja u regiji i njihovih međunarodnih partnera. Godišnji program obuhvaća četiri područja; borba protiv oružja za masovno uništenje, borba protiv transnacionalnih sigurnosnih prijetnje, zadružno sigurnosno okruženje i upravljanje sigurnosnim sektorom.[129]

[127]Izvor: apis-it.hr [pristupljeno 04.08.2022] Dostupno na https://www.apis-it.hr/apisit/index.html#/page?docId=6F1FA2DF4923825CC1257F99002E2D4D

[128] mup.gov.hr Ministarstvo unutarnjih poslova (službena Internet stranica) [pristupljeno 04.08.2022] Dostupno na https://mup.gov.hr/UserDocsImages//dokumenti//MUP_godisnjak_2013.pdf str. 39.-41.

[129] Racviac.org (službena Internet stranica) [pristupljeno 04.08.2022] Dostupno na https://www.racviac.org/what-is-racviac/

10. NORME INFORMACIJSKE SIGURNOSTI

Međunarodna udruga za normizaciju (eng. *International Standards Organization – ISO*) je neovisna, nevladina međunarodna organizacija koju čini 167 nacionalnih tijela za standarde koja radi na podizanju svijesti o standardima i standardizaciji. Standardi se odnose na upravljanje kvalitetom, upravljanje okolišem, zdravstveni i sigurnosni standardi, standardi upravljanja energijom, sigurnosti hrane, IT sigurnosti, informacijske sigurnosti…[130]

Međunarodno tehničko povjerenstvo (eng. *International Electrotehnical Commission – IEC*) je svjetska organizacija za pripremu i objavljivanje međunarodnih standarda za sve elektroničke, električne i slične tehnologije. Okuplja više od 170 zemalja svijeta. Usvajanje je dobrovoljno iako se često implementiraju u nacionalne zakone.[131]

U području koje se odnosi na informacijske tehnologije ISO i IEC osnovali su zajednički tehnički odbor (eng. *Joint Tehnical Committeee – JTC*) – ISO/IEC JTC, a zadaća im je priprema međunarodnih standarda.[132]

Kada se uspostavi sigurnosna politika potrebno je odabrati standarde prema kojima će se ista uspostaviti. Putem tih standarda osigurava se jedinstveno funkcioniranje sigurnosnih sustava neke organizacije ili ustanove, standardi odnosno norme mogu pomoći u definiranju opsega djelovanja, ali na kraju se svodi da rukovoditelji informacijske sigurnosti pronađu najbolji način vođenja i nadzora i prilagode ga potrebama organizacije ili institucije. U području informacijskih sustava važni su standardi pod nazivom ISO/IEC 27001 – Sustav upravljanja informatičkom sigurnošću te ISO/IEC 27002 – Kodeks postupaka za upravljanje informacijskom sigurnošću i oba su bitna za kvalitetan sustav upravljanja informacijskim sustavom.[133]

[130] iso.org – svjetska organizacija za standardizaciju (službena Internet stranica) [pristupljeno 05.08.2022] Dostupno na https://www.iso.org/what-we-do.html
[131] iec.ch – međunarodna elektrotehnička komisija [pristupljeno 05.08.2022] Dostupno na https://www.iec.ch/about-us
[132] Ibid.
[133] cert.hr Hrvatska akademska i istraživačka mreža Croatian academic and research nerwork Sigurnosna politika [pristupljeno 06.08.2022] Dostupno na https://www.cert.hr/wp-content/uploads/2009/05/CCERT-PUBDOC-2009-05-265.pdf str.16.

U Republici Hrvatskoj osnovan je Hrvatski zavod za norme[134] i radi kao neovisna i neprofitna javna ustanova osnovana zbog ostvarivanja ciljeva standardizacije (povećanje razine sigurnosti proizvoda i procesa, čuvanje zdravlja i života, zaštita okoliša, promicanje kvalitete proizvoda, procesa i usluga, poboljšanje proizvodne učinkovitosti, ograničenja raznolikosti…). Član je ISO, IEC, Europskog odbora na normizaciju (CEN), Europskog odbora za elektrotehničku normizaciju (CENELEC) te Europskog instituta za telekomunikacijske norme (ETSI).[135]

ISO/IEC 27000:2018 – Informacijska tehnologija – Sigurnosne tehnike – Sustavi upravljanja informacijskom sigurnošću – Pregled i vokabular → serija normi daje pregled sustava upravljanja informacijskom sigurnošću (ISMS) i definira mnoge pojmove.[136] U ovoj seriji postoji nekoliko desetaka normi, ali izdvojiti ćemo samo najvažnije.

ISMS (eng. *Information Security Managment Systems*) je sustav upravljanja informacijskom sigurnošću koji se temelji na pristupu upravljanja rizicima da bi se uspostavila, provodila, pratila, revidirala, održavala i unaprjeđivala informacijska sigurnost. ISO 27001 opisuje kako razviti ISMS.[137] Putem ISMS-a rukovodstvo neke organizacije ili institucije provodi nadzor nad sigurnosti informacijskog sustava. Za njegovu izgradnju potreban je PDCA model.

10.1. ISO/IEC 27001:2013

Sustav upravljanja informatičkom sigurnošću (ISMS) kojeg je donijela ISO, punog naziva „Informacijske tehnologije – Tehnike zaštite – Specifikacije za sustav upravljanja informacijskim sustavima“. ISO 27001 sastavili su ponajbolji svjetski eksperti iz djelokruga informacijske sigurnosti kako bi propisali metodologiju upravljanja informacijskom sigurnošću u

[134] hzn.hr Hrvatski zavod za norme (Internet) [pristupljeno 06.08.2022] Dostupno na https://www.hzn.hr/default.aspx?id=6
[135] Ibid.
[136] iso.org ISO/IEC 27000:2018 [pristupljeno 06.08.2022] Dostupno na https://www.iso.org/standard/73906.html
[137] advisera.com Što je sustav upravljanja informacijskom sigurnošću (ISMIS) prema ISO 27001? [pristupljeno 06.08.2022] Dostupno na https://advisera.com/27001academy/blog/2016/05/23/information-security-management-system-isms-according-iso-27001/

organizacijama, na temelju standarda BS 7799 (British Standards). Najpoznatiji je standard informacijske sigurnosti u svijetu i ako ga se implementira u sustav dobije se certifikat.[138]

Bazira se na zaštitu povjerljivosti, raspoloživosti i cjelovitosti podataka u organizacijama, institucijama ili tvrtkama što se postiže prepoznavanjem mogućih problema na vrijeme i definiraju mjere koje trebaju biti poduzete da se takvi problemi ne dogode. Znači, cijela ova norma odnosi se na upravljanje rizicima – prepoznavanje i zaštitu. U njemu se navode zahtjevi za implementaciju kontrole informacijske sigurnosti prilagođene potrebama pojedine organizacije.[139]

ISO 27001 zahtijeva da se procjena rizika sastoji od 5 koraka[140];

1. identifikacija rizika
2. dodjela vlasnika rizika (odgovorna osoba)
3. analiza rizika (posljedice i vjerojatnosti)
4. izračun rizika
5. procjena rizika.

Razne organizacije i institucije imaju kontrole informacijske sigurnosti ali bez ISMS-a one su pomalo kaotične, neorganizirane. „ISO/IEC 27001 formalno ne propisuje posebne kontrole informacijske sigurnosti jer se potrebne kontrole znatno razlikuju u širokom rasponu organizacija koje usvajaju normu.“[141]

ISO/IEC 27001:2013 sastoji se od 10 odjeljaka:[142]

0. uvod – opis procesa sustavnog upravljanja informacijskih rizicima i svrha ISO 27001
1. opseg – objašnjenje kako je ovaj standard primjenjiv za bilo koju organizaciju
2. normativne reference – vodi na ISO/IEC 27000 kao standard gdje su objašnjeni pojmovi
3. pojmovi i definicije – isto vodi na ISO/IEC 27000

[138] iso.org ISO/IEC 27001:2013 [pristupljeno 05.08.2022] Dostupno na https://www.iso.org/standard/54534.html
[139] advisera.com Kako funkcionira ISO 27001? [pristupljeno 07.08.2022] Dostupno na https://advisera.com/27001academy/hr/sto-je-iso-27001/#section2
[140] advisera.com Upravljanje rizicima (Internet) [pristupljeno 07.08.2022] Dostupno na https://advisera.com/27001academy/iso-27001-risk-assessment-treatment-management/#assessment
[141] iso27001security.com ISO/IEC 27001:2013 (Internet) [pristupljeno 07.08.2022] Dostupno na https://www.iso27001security.com/html/27001.html
[142] Ibid.

4. kontekst organizacije – razumijevanje konteksta organizacije, definiranje primjene ISMS-a, objašnjava PDCA krug (uspostava, upravljanje, pregledavanje, poboljšavanje)
5. vodstvo – određuju se uloge i odgovornosti za provođenje ISMS-a
6. planiranje – opisuje postupak utvrđivanja, analize i planiranja obrade rizika, pojašnjava cilj informacijske sigurnosti, planiranje u PDCA krugu
7. podrška – moraju se dodijeliti odgovarajući izvori, pripremiti dokumentacija, kontrolirati, podići razinu svijesti
8. operacija – detaljnije obrađen dio o procjeni i obradi informacijskih rizika, upravljanju i dokumentiranju
9. evaluacija uspješnosti – definira uvjete za praćenje, analizu, mjerenje, procjenu, unutarnju reviziju kako bi se poboljšale stvari prema potrebi
10. poboljšanje – definiraju se uvjeti za ispravke, neusklađenost, mjere korekcije i poboljšanje.

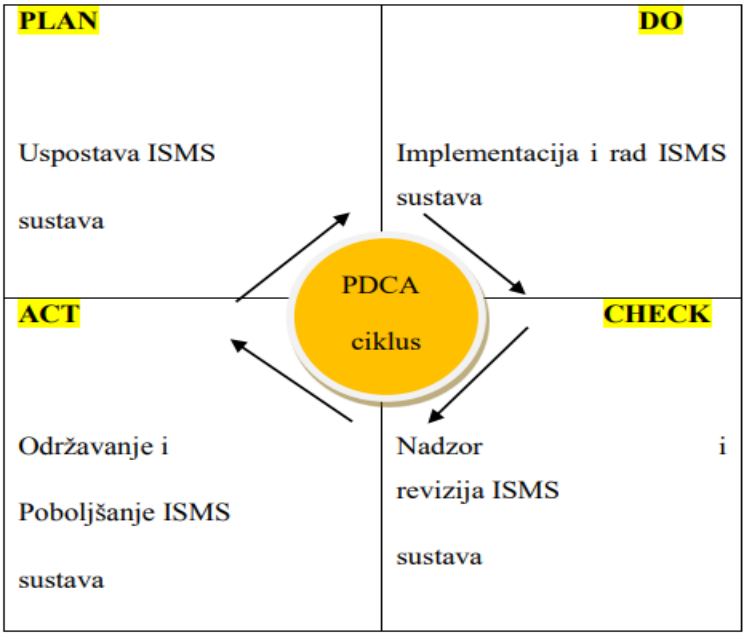
    Aneks A nudi katalog sigurnosnih mjera.

10.1.1. PDCA model

Osnovni koncept koji je razvio William Edwards Deming za upravljanje sastoji se od 4 koraka:[143]

1. plan – planiranje - odnosi se na planiranje ISMS politike, odabiru se mjere zaštite koje su najbolje, procedura za upravljanje rizikom, poboljšanje sigurnosti, što se želi postići (ciljevi)
2. do – implementacija – rad i implementacija ISMS kontrola i procesa, kontinuitet poslovanja, sve na što je ISO standard usmjeren
3. check – provjera – provjera plana, mjera i ciljeva.
4. act – djelovanje – poduzimanje preventivnih i korektivnih mjera na temelju revizije, nadgledanje funkcioniranja ISMS-a.

[143] lucidchart.com Kako primijeniti model Zakona o planu i provjeri (PDCA) za poboljšanje vašeg poslovanja [pristupljeno 08.08.2022] Dostupno na https://www.lucidchart.com/blog/plan-do-check-act-cycle



Slika 8. PDCA model[144]

10.2. ISO/IEC 27002:2022

Puni naziv za ovu normu je „Informacijska sigurnosti, kibersigurnost i zaštita privatnosti – Kontrole informacijske sigurnosti“. Ova norma služi za implementaciju sigurnosnih mjera i pokazala se kao najbolja u praksi u uvođenju normi. Ona je kao i 27001 norma utemeljena na BS 7799 standardu, ali je mnogo preciznija. Ovo je norma koja se može upotrijebiti kao skup smjernica za implementaciju norme ISO 27001. Nije ju moguće certificirati jer nije upravljačka norma.[145]

Razlika između normi 27001 i 27002 je u detaljima koji su posvećeni nekoj sigurnosnoj mjeri.

ISO/IEC 27002 savjetodavnog je karaktera, preporuka. Organizacijama se savjetuje kako da utvrde i ocjene svoje informacijske rizike, odaberu najbolje kontrole kako bi to spriječile. Isto tako, primjenjiva je na sve vrste organizacija nebitno o veličini. Norma se odnosi na

[144] Juran A. Sigurnost informacijskih sustava, Pomorski fakultet u Rijeci, Sveučilište u Rijeci, diplomski rad 2014. [pristupljeno 08.08.2022] Dostupno na http://www.pfri.uniri.hr/knjiznica/NG-dipl.LMPP/290-2014.pdf
[145] advisera.com Sličnosti i razlike između ISO 27001 i ISO 27002 [pristupljeno 08.08.2022] Dostupno na https://advisera.com/27001academy/hr/blog/2010/09/13/iso-27001-vs-iso-27002-3/

informacijsku sigurnost što znači na sve oblike informacija, ne samo sustava, mreža i kibersigurnosti.[146]

10.3. ISO/IEC 27005

Puni naziv „Informacijska tehnologija – Sigurnosne tehnike – Upravljanje rizicima informacijske sigurnosti“. Ova norma daje smjernice za upravljanje rizicima informacijske sigurnosti oslanjajući se na normu ISO/IEC 27001 i donijeta je da bi se pomoglo u provedbi informacijske sigurnosti putem pristupa upravljanju rizicima. Ova norma ne navodi ni ne preporučuje nikakve konkretne metode upravljanja rizicima informacijske sigurnosti nego raspravlja i opisuje upravljanje rizikom (utvrđivanje i procjena rizika, odlučivanje o rizicima, praćenje rizika, informiranje sudionika).[147]

10.4. ISO/IEC 27014

Punog naziva „Informacijska sigurnost, kibersigurnost i zaštita privatnosti – Upravljanje informacijskom sigurnošću“, pruža smjernice o ciljevima i procesima upravljanja informacijskom sigurnošću da ih uz njihovu pomoć mogu ocijeniti, usmjeriti, nadzirati unutar organizacije. Primjenjuje se na sve vrste i veličine organizacija, a posebno se odnosi na upravljačko tijelo i najviše rukovodstvo, osobe odgovorne za evaluaciju i praćenje ISMS-a, osobe odgovorne za upravljanje informacijskom sigurnošću koja se odvija van područja primjene ISMS-a.[148]

---

[146] iso37001security.com ISO/IEC 27002:2022 [pristupljeno 08.08.2022] Dostupno na https://www.iso27001security.com/html/27002.html

[147] iso37001security.com ISO/IEC 27005:2018 [pristupljeno 08.08.2022] Dostupno na https://www.iso27001security.com/html/27005.html

[148] iso37001security.com ISO/IEC 27014:2020 [pristupljeno 08.08.2022] Dostupno na https://www.iso27001security.com/html/27014.html

10.5. Nacionalni institut za standarde i tehnologiju

Skraćeno NIST (eng. *National Institute of Standards and Tehnology*) jedan od najstarijih laboratorija za fizičke znanosti u SAD-u, dio Ministarstva trgovine SAD-a. Misija instituta je promicanje američkih inovacija i industrijske konkurentnosti unaprjeđivanjem znanosti, normi i tehnologija mjerenja da bi poboljšali ekonomsku sigurnost i općenito kvalitetu života. Temeljne vrijednosti NIST-a su: ustrajnost, integritet, inkluzivnost, izvrsnost. Objavljuje posebne publikacije koje se odnose na aspekte informacijskih sustava.[149]

Neki od posebnih publikacija su (NIST Special Publication (SP))[150]:

- NIST SP 800-12 – Uvod u informacijsku sigurnost
- NIST SP 800-30 – Vodič za provođenje procjena rizika
- NIST SP 800-39 – Upravljanje rizikom informacijske sigurnosti: prikaz organizacije, misije i informacijskog sustava
- NIST SP 800-50 – Izgradnja programa svjesnosti i osposobljavanje o sigurnosti informacijske tehnologije
- NIST SP 800-53 – Kontrolne polazne vrijednosti za informacijske sustave i organizacije
- NIST SP 800-61 – Vodič za rukovanje računalnim sigurnosnim incidentima

NIST je razvio Okvir za kibernetičku sigurnost (eng. *NIST Cybersecurity Framework*) kao praksu za računalnu sigurnost. Osmišljen je za pojedinačna poduzeća i organizacije radi procjene rizika koji im prijeti. Nudi smjernice za osiguranje sustava koji pomažu revizorima da usklade sigurnosne zahtjeve i pokretače.[151]

[149] nist.gov Nacionalni institut za standarde i tehnologiju O NIST-u (službena Internet stranica) [pristupljeno 09.08.2022] Dostupno na https://www.nist.gov/about-nist

[150] csrc.nist.gov Laboratorij za informacijske tehnologije [pristupljeno 09.08.2022] Dostupno na https://csrc.nist.gov/publications/search?keywords-lg=800-&sortBy-lg=Number+ASC&viewMode-lg=brief&ipp-lg=all&status-lg=Final%2CDraft&topicsMatch-lg=ANY&controlsMatch-lg=ANY

[151] en.wikipedia.org Nist okvir za kibernetičku sigurnost [pristupljeno 09.08.2022] Dostupno na https://en.wikipedia.org/wiki/NIST_Cybersecurity_Framework

Prema NIST-u informacijskim sustavima dijele se na[152]:

- greške i kvarove (najčešće ljudske radnje)
- prijevare i krađe
- sabotaža od strane zaposlenika
- gubitak fizičke i infrastrukturne potpore
- hakere
- zlonamjerne programe
- prijetnje privatnosti korisnika.

[152] cert.hr(službena Internet stranica) [pristupljeno 09.08.2022.] Dostupno na https://www.cert.hr/wp-content/uploads/2 009/05/CCERT-PUBDOC-2009-05-265.pdf

11. REZULTATI

1. Nijedan sustav nije siguran pa tako ni informacijski sustav te zbog povećanog broja ugroza treba misliti na informacijsku sigurnost i zaštitu.

Informacijski sustav sastoji se od procesa, tehnologije i kao najvažnije – ljudi. Cilj informacijske sigurnosti je zaštita od zlouporabe i ugroza da bi se smanjio sigurnosni rizik. U informacijskoj sigurnosti kao najveća ugroza spominju se pojedinci ili zaposlenici u organizacijama koji nenamjerno (neki čak i namjerno) rade propuste koji dovode do širenja informacija i podataka, samim time zlouporabe i računalnih prijevara. Zbog toga je veoma važno provoditi periodične kontrole sustava da ne bi došlo do nepotrebnih gubitaka. Također je vrlo važno educirati se i osposobljavati u području informacijske sigurnosti, raditi na zaštiti informacijskog sustava, upoznati se sa zakonskim regulativama i iste poštivati. Nijedan sustav nije siguran, pogotovo informacijski, jer tehnologija svakodnevno napreduje, a samim tim i moguće vrste napada na sustave i pojedinca i prema tome, treba misliti na informacijsku sigurnost pri svakom koraku koliko god je to moguće da bi se zaštitili ili barem sveli na minimum sigurnosne rizike.

2. U svijetu i u Republici Hrvatskoj informacijska sigurnost je regulirana mnogim zakonima, standardima i pravilima radi odgovarajuće zaštite podataka.

U svijetu i Republici Hrvatskoj postoji veliki broj zakona i podzakonskih akata vezanih za informacijsku sigurnost da bi se postigla što veća razina zaštite podataka. Hrvatska je iz svih zakona i podzakonskih akata iznjedrila dosta institucija koje se bave informacijskom sigurnošću kao na primjer Nacionalni CERT, Ured vijeća za nacionalnu sigurnost, Zavod za sigurnost informacijskih sustava, Agenciju za zaštitu osobnih podataka, Agenciju za podršku informacijskim sustavima i informacijskim tehnologijama (APIS IT), Odjel za visokotehnološki kriminal, Regionalno središte za kibernetsku sigurnost unutar Centra za sigurnosnu suradnju (RACVIAC) te Središnji državni ured za e-Hrvatsku. Također, informacijska sigurnost štiti se

normama i standardima skupine ISO/IEC 27000 koja sadrži nekoliko desetaka normi i daje pregled sustava upravljanja informacijskom sigurnošću i definira mnoge pojmove.

12. ZAKLJUČAK

Ovim radom htjela se prikazati važnost informacijske sigurnosti i informacijskih sustava. Kada se govori o informacijskoj sigurnosti ona se sastoji od tehnologija, ljudi i procesa. Kako je vidljivo, uvijek postoji jedna određena razina opasnosti za sigurnost i sustav i toga treba biti svjestan te pronaći načina, ulagati, educirati se i napredovati da bi se uspješno reagiralo na moguće napade i prijetnje. Svakodnevno se pojavljuju sve inovativniji načini ugroze informacijske sigurnosti i sustava započeti od strane jedne osobe ili skupine osoba koje se bave kibernetičkim kriminalom.

Informacijska sigurnost odnosi se na zaštitu i sigurnost određenih informacija u bilo kojoj vrsti organizacije. Sve više se osvještava da je potrebno ulagati u informacijsku sigurnost da bi se sačuvale informacije, upoznali pojedinci i zaposlenici sa problemima i opasnostima korištenja i dijeljenja informacija. Informatizacija i modernizacija doprinose povećanoj opasnosti od zlouporabe i sigurnosnih incidenata. Samim time, zanemarivanje informacijske sigurnosti dovodi do napada sustava koji treba periodično kontrolirati i osiguravati prema preporukama stručnjaka jer sadrži mnoštvo osobnih podataka, podataka važnih za rad i poslovanje organizacija.

Republika Hrvatska zakonski regulira pitanje informacijske sigurnosti i osniva institucije koje se o tome brinu, ali i dalje se mora ulagati i poraditi na edukaciji i osposobljavanju zaposlenika i pojedinaca da bi svojim odgovornim ponašanjem spriječili napade i zlouporabu podataka.

Informacijsku sigurnost i zaštitu ne treba sagledavati kao jednu stavku koja je samo trošak i stavljati je po strani. Vrlo je bitno shvatiti na vrijeme važnost informacijske sigurnosti iako taj pojam još nije u potpunosti shvaćen. Ulaganjem u informacijsku sigurnosti i podizanje razine svijesti uvelike bi se smanjili sigurnosni rizici.

Najveći problem u informacijskoj sigurnosti zapravo leži u zaposlenicima/pojedincima koji su ključni za ovaj problem, a samim time oni su i rješenje tog problema – edukacijom i osposobljavanjem smanjuje se vjerojatnost sigurnosnih incidenata i zlouporabe.

LITERATURA

1. Andrijanić, I., Gregurek, M., Merkaš, Z. Upravljanje poslovnim rizicima. Zagreb, Libertas – Plejada 2016.
2. Arbanas K. Radni okvir za procjenu i unapređenje kulture informacijske sigurnosti, Disertacija, Varaždin, Sveučilište u Zagrebu, Fakultet organizacije i informatike, 2021.
3. Brzica, N. Informacijska nadmoć: na sjecištu informacijskog i kibernetičkog ratovanja. Polemos, XXIII (47), 13-31. 2020.
4. Cherdantseva Y. , Hilton J. Evolucija informacijske sigurnosti ciljevi od 1960-ih do danas Sveučilište Cardiff, 2012.
5. Cvrtila, Ž. Hibridni rat – suvremeni naziv za već poznate oblike ratovanja, Stručni članak, 2017.
6. Čizmić J., Boban M., Zlatović D. Nove tehnologije, intelektualno vlasništvo i informacijska sigurnost, Sveučilište u Splitu Pravni fakultet, Split 2016.
7. Garača, Ž., Informatičke tehnologije, Sveučilište u Splitu, Split, 2007.
8. Juran A. Sigurnost informacijskih sustava, Diplomski rad, Pomorski fakultet u Rijeci, Sveučilište u Rijeci, 2014.
9. Obradović, D. Kibernetika – što je to? Common Foundations 2018 - uniSTem: 6th Congress of Young Researchers in the Field of Civil Engineering and Related Sciences. Sveučilište u Splitu, Fakultet građevinarstva, arhitekture i geodezije, 2018.
10. Panian, Ž. Kontrola i revizija informacijskih sustava. Zagreb, Sinergija nakladništvo, 2001.
11. Panian, Ž., Ćurko, K., Bosilj Vukšić, V., Čerić, V., Pejić Bach, M., Požgaj, Ž., Spremić, M., Strugar, I., Varga, M. Poslovni informacijski sustavi, Zagreb, Element, 2010.
12. Pavlić, M. Informacijski sustavi, Zagreb: Školska knjiga d.d., 2011.
13. Spremić, M. Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije, Zagreb, Ekonomski fakultet Zagreb, 2017.
14. Srića, V., Spremić, M. Informacijskom tehnologijom do uspjeha, Sinergija, Zagreb, 2000.
15. Šimundić, S. Pravna informatika, Sveučilište u Splitu Pravni fakultet, Split 2007.
16. Tihi, B., Istraživanje tržišta organizacije udruženog rada, V. Masleša, Sarajevo, 1987.

17. Tuđman, M., Boras, D., Doveden, Z., Uvod u informacijske znanosti, Školska knjiga, Zagreb 1993.
18. Vojković, G., Štambuk-Sunjić, M. Konvencija o kibernetičkom kriminalu i kazneni zakon Republike Hrvatske, Znanstveni članak, 2005.
19. Vukelić, B. Sigurnost informacijskih sustava – skripta, Udžbenik, Rijeka, Veleučilište u Rijeci 2016.
20. Vuković H. Kibernetska sigurnost i sustav borbe protiv kibernetskih prijetnji u Republici Hrvatskoj, National security and the future, 2012.
21. Zbornik Pravnog fakulteta Sveučilišta u Rijeci, vol. 39, br. 1, 377-410, Čizmić, J., Boban, M. Učinak nove EU Uredbe 2016/679 (GDPR) na zaštitu osobnih podataka u Republici Hrvatskoj, 2018.
22. Zbornik radova Pravnog fakulteta u Splitu, god. 49, 3/2012, Boban, M. Pravo na privatnosti i pravo na pristup informacijama u suvremenom informacijskom društvu, 2012.
23. Zbornik radova Veleučilišta u Šibeniku, (1-2/2015):115-148, Boban M, Perišić M. Biometrija u sustavu sigurnosti, zaštite i nadzora informacijskih sustava, 2015.
24. Zbornika radova: Dani hrvatskog osiguranja, Bara, D. Uloga cyber-osiguranja u upravljanju i prijenosu rizika cyber-sigurnosti, Stručni članak, 2015.

Propisi

1. Nacionalna strategija kibernetičke sigurnosti i Akcijski plan za provedbu Strategije (NN 108/2015) dostupna na https://mup.gov.hr/UserDocsImages/dokumenti/kiberneticka_sigurnost/Sa%C5%BEetak%20Nacionalne%20strategije%20kiberneti%C4%8Dke%20sigurnosti.pdf
2. Odluka o primjerenom upravljanju informacijskim sustavom (NN 37/2010) dostupna na https://narodne-novine.nn.hr/clanci/sluzbeni/2010_03_37_958.html
3. Uredba o mjerama informacijske sigurnosti (NN 46/2008) dostupna na https://narodne-novine.nn.hr/clanci/sluzbeni/full/2008_04_46_1547.html
4. Uredba o mjerama informacijske sigurnosti (NN 46/2008) dostupna na https://narodne-novine.nn.hr/clanci/sluzbeni/2008_04_46_1547.html
5. Uredba o načinu označavanja klasificiranih podataka, sadržaju i izgledu Uvjerenja o obavljenoj sigurnosnoj provjeri i Izjave o postupanju s klasificiranim podacima (NN 102/2007) dostupna na https://narodne-novine.nn.hr/clanci/sluzbeni/2007_10_102_2985.html
6. Uredba o sigurnosnoj provjeri za pristup klasificiranim podacima (NN 72/2007) dostupna na https://narodne-novine.nn.hr/clanci/sluzbeni/2007_07_72_2237.html
7. Zakon o elektroničkoj ispravi (NN 150/05) dostupan na https://zakon.hr/z/272/Zakon-o-elektroni%C4%8Dkoj-ispravi
8. Zakon o informacijskoj sigurnosti (NN 79/07) dostupan na https://zakon.hr/z/218/Zakon-o-informacijskoj-sigurnosti
9. Zakon o pravu na pristup informacijama (NN 25/13, 85/15, 69/22) dostupan na https://zakon.hr/z/126/Zakon-o-pravu-na-pristup-informacijama
10. Zakon o provedbi Opće uredbe o zaštiti podataka (NN 42/18) dostupan na https://www.zakon.hr/z/1023/Zakon-o-provedbi-Op%C4%87e-uredbe-o-za%C5%A1titi-podataka
11. Zakon o provedbi Uredbe br. 910/2014 Europskog parlamenta i Vijeća od 23.07.2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ (NN 62/17) dostupan na https://www.zakon.hr/z/923/Zakon-o-provedbi-Uredbe-%28EU%29-br.-910-2014-

Europskog-parlamenta-i-Vije%C4%87a-od-23.-srpnja-2014.-o-elektroni%C4%8Dkoj-identifikaciji-i-uslugama-povjerenja-za-elektroni%C4%8Dke-transakcije-na-unutarnjem-tr%C5%BEi%C5%A1tu-i-stavljanju-izvan-snage-Direktive-1999-93-EZ

12. Zakon o sigurnosnim provjerama (NN 85/08, 86/12) dostupan na https://zakon.hr/z/536/Zakon-o-sigurnosnim-provjerama
13. Zakon o sigurnosno-obavještajnom sustavu Republike Hrvatske (NN 79/06, 105/06) dostupan na https://zakon.hr/z/744/Zakon-o-sigurnosno-obavje%C5%A1tajnom-sustavu-Republike-Hrvatske
14. Zakon o tajnosti podataka (NN 79/07, 86/12) dostupan na https://zakon.hr/z/217/Zakon-o-tajnosti-podataka

Internetske stranice

1. http://enciklopedija.lzmk.hr/clanak.aspx?id=18859 pristupljeno 03.07.2022.g.
2. http://www.enciklopedija.hr/Natuknica.aspx?ID=17976 pristupljeno 09.06.2022.g.
3. http://www.enciklopedija.hr/Natuknica.aspx?ID=27405 pristupljeno 05. 06. 2022.g.
4. http://www.enciklopedija.hr/Natuknica.aspx?ID=55892 pristupljeno 05. 06. 2022.g.
5. https://advisera.com/27001academy/blog/2016/05/23/information-security-management-system-isms-according-iso-27001/ pristupljeno 06.08.2022.g.
6. https://advisera.com/27001academy/hr/blog/2010/09/13/iso-27001-vs-iso-27002-3/ pristupljeno 08.08.2022.g.
7. https://advisera.com/27001academy/hr/sto-je-iso-27001/#section2 pristupljeno 07.08.2022.g.
8. https://advisera.com/27001academy/iso-27001-risk-assessment-treatment-management/#assessment pristupljeno 07.08.2022.g.
9. https://azop.hr/djelokrug/ pristupljeno 02.08.2022.g.
10. https://bolje.hr/rijec/outsourcing-gt-izdvajanje-posla/1/ pristupljeno 21.06.2022.g.
11. https://csrc.nist.gov/publications/search?keywords-lg=800-&sortBy-lg=Number+ASC&viewMode-lg=brief&ipp-lg=all&status-lg=Final%2CDraft&topicsMatch-lg=ANY&controlsMatch-lg=ANY pristupljeno 09.08.2022.g.
12. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy pristupljeno 28.07.2022.g.
13. https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-2000-server/cc959354(v=technet.10) pristupljeno 18. i 19.06.2022.g.
14. https://en.wikipedia.org/wiki/NIST_Cybersecurity_Framework pristupljeno 09.08.2022.g.
15. https://gdprinformer.com/hr/vodic-kroz-gdpr pristupljeno 30.07.2022.g.
16. https://hr.eyewated.com/cyber-%E2%80%8B%E2%80%8Bkriminal-sto-je-to/ pristupljeno 06.07.2022.g.
17. https://hr.theastrologypage.com/cybercriminal pristupljeno 07.07.2022.g.
18. https://hr.wikipedia.org/wiki/Sredi%C5%A1nji_dr%C5%BEavni_ured_za_e-Hrvatsku pristupljeno 03.08.2022.g.

19. https://mup.gov.hr/UserDocsImages//dokumenti//MUP_godisnjak_2013.pdf pristupljeno 04.08.2022.g.
20. https://www.academia.edu/21637101/PRIMJENA_RA%C4%8CUNALA_ST_P02_Povijesni_pregled_razvoja_ra%C4%8Dunala pristupljeno 08.06.2022.g.
21. https://www.apis-it.hr/apisit/index.html#/page?docId=862092FC53B6F468C1257F400043EACF pristupljeno 04.08.2022.g.
22. https://www.cert.hr/onama/ pristupljeno 31.07.2022.g.
23. https://www.cert.hr/wp-content/uploads/2009/05/CCERT-PUBDOC-2009-05-265.pdf pristupljeno 11.06.2022.g.
24. https://www.cis.hr/files/Celuska-Osnove_upravljanja_rizikom.pdf pristupljeno 24.06.2022.g.
25. https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2003-10-44.pdf pristupljeno 24.06.2022.g.
26. https://www.hnb.hr/-/smjernice-za-upravljanje-informacijskim-sustavom-u-cilju-smanjenja-operativnog-rizika pristupljeno 31.07.2022.g.
27. https://www.hnb.hr/documents/20182/639854/h-smjernice-za-upravljanje-informacijskim-sustavom.pdf/e5579931-e846-47ab-af23-6809debef700 pristupljeno 23.06.2022.g.
28. https://www.hzn.hr/default.aspx?id=6 pristupljeno 06.08.2022.g.
29. https://www.ictbusiness.info/poslovanje/cyber-sigurnost-postaje-sve-vaznija pristupljeno 05.06.2022.g.
30. https://www.iec.ch/about-us pristupljeno 05.08.2022.g.
31. https://www.iso.org/standard/54534.html pristupljeno 05.08.2022.g.
32. https://www.iso.org/standard/73906.html pristupljeno 06.08.2022.g.
33. https://www.iso.org/what-we-do.html pristupljeno 05.08.2022.g.
34. https://www.iso27001security.com/html/27001.html pristupljeno 07.08.2022.g.
35. https://www.iso27001security.com/html/27002.html pristupljeno 08.08.2022.g.
36. https://www.iso27001security.com/html/27005.html pristupljeno 08.08.2022.g.
37. https://www.iso27001security.com/html/27014.html pristupljeno 08.08.2022.g.
38. https://www.iusinfo.hr/document?sopi=DDHR20181007N112 pristupljeno 29.07.2022.g.

39. https://www.lucidchart.com/blog/plan-do-check-act-cycle pristupljeno 08.08.2022.g.
40. https://www.moj-posao.net/Vijest/60807/Outsourcing-sto-je-i-zasto-se-koristi/ pristupljeno 22.06.2022.g.
41. https://www.morh.hr/o-vojnoj-sigurnosno-obavjestajnoj-agenciji/ pristupljeno 21.07.2022.g.
42. https://www.nist.gov/about-nist pristupljeno 09.08.2022.g.
43. https://www.racviac.org/what-is-racviac/ pristupljeno 04.08.2022.g.
44. https://www.soa.hr/hr/o-nama/sto-je-soa/ pristupljeno 21.07.2022.g.
45. https://www.soa.hr/hr/podrucja-rada/kiberneticka-sigurnost/ pristupljeno 10.07.2022.g.
46. https://www.thecroforum.org/2014/12/19/cyber-resilience-cyber-risk-challenge-role-insurance/ pristupljeno 12.07.2022.g.
47. https://www.uvns.hr/hr/hr/o-nama/uvodna-rijec pristupljeno 01.08.2022.g.
48. https://www.uvns.hr/hr/sto-su-to-mjere-i-standardi-informacijske-sigurnosti pristupljeno 10.06.2022.g.
49. https://www.uvns.hr/hr/tko-je-sve-obavezan-provoditi-informacijsku-sigurnost pristupljeno 14.06.2022.g.
50. https://www.uvns.hr/hr/tko-moze-biti-savjetnik-za-informacijsku-sigurnost pristupljeno 14.06.2022.g.
51. https://www.wikiwand.com/hr/Kiberneti%C4%8Dka_%C5%A1pijuna%C5%BEa pristupljeno 07.07.2022.g.
52. https://www.zsis.hr/default.aspx?id=13 pristupljeno 02.08.2022.g.

SAŽETAK

U ovom diplomskom radu pokušali smo objasniti i približiti temu i definiciju informacijske sigurnosti koja uključuje ljude, procese, tehnologije, uređaje, mreže, informacije, postrojenja, proizvode, politike, postupke i sustave. Obrađena su poglavlja koja se odnose na informacijsku sigurnost, informacijski sustav, sigurnosne rizike i procjenu rizika, kibernetiku i kibernetički kriminal, sigurnosnu politiku, zakonodavni okvir informacijske sigurnosti te norme informacijske sigurnosti (ISO standardi). Svaki navedeni pojam je objašnjen i definiran, ukratko je opisan povijesni razvoj informacijske sigurnosti i informacijskih sustava. Posebnu pažnju treba skrenuti na zaštitu informacijske sigurnosti edukacijom i obrazovanjem pojedinaca i zaposlenika, uvođenjem sigurnosnih pravila i zaštitnih mjera da bi se sigurnosni rizici sveli na minimum te voditi brigu o ažuriranju sustava informacijske tehnologije.

ključne riječi: informacijska sigurnost, informacijski sustav, sigurnosni rizik, kibernetika

ABSTRACT

In this thesis, we tried to explain and approximate the topic and definition of application and implementation of information security in the Republic of Croatia- regulatory framework and standards, which includes people, processes, technologies, devices, networks, information, plants, products, policies, procedures and systems. Chapters related to information security, information system, security risks and risk assessment, cybernetics and cybercrime, security policy, legislative framework of information security and information security norms (ISO standards) are covered. Each mentioned term is explained and defined, the historical development of information security and information systems is briefly described. Particular attention should be paid to the protection of information security through the education and training of individuals and employees, the introduction of security rules and protective measures to minimize security risks, and to take care of updating the information technology system.

keywords: information security, information system, security risk, cybernetics

ŽIVOTOPIS

Osobne informacije Dolić Frano
Adresa: Miletin 15 D, 21230 Sinj (Hrvatska)
br. mobitela: 097 797 1928
e-mail: franodolic2001@gmail.com
Datum rođenja: 20.01.1990.

Radno iskustvo Radni staž :

- 2011. – 2012. :GIP, obrt za ugostiteljstvo, Hvar (Hrvatska)

- 2014.–2017. Ministarstvo obrane, Oružane snage RH,
- USTROJBENA JEDINICA: HRVATSKA RATNA MORNARICA, OBALNA STRAŽA RH,
  1. DIVIZIJUN OBALNE STRAŽE RH,

- 2017.–2018. Ministarstvo obrane, Oružane snage RH,
- USTROJBENA JEDINICA: HRVATSKA RATNA MORNARICA, FLOTILA HRVATSKE RATNE MORNARICE,
- DIVIZIJUN ZA POVRŠINSKO DJELOVANJE, RTOP-12,
- ustrojbeni čin: skupnik

- 2018.-2020. Ministarstvo obrane, Oružane snage RH,
- USTROJBENA JEDINICA: HRVATSKA RATNA MORNARICA, FLOTILA HRVATSKE RATNE MORNARICE,
- SATNIJA MORNARIČKOG DESANTNOG PJEŠAŠTVA
- ustrojbeni čin: poručnik

- 2020.-2022. Ministarstvo obrane, Oružane snage RH,
- USTROJBENA JEDINICA:OBAVJEŠTAJNA PUKOVNIJA, BOJNA ZA OBAVJEŠTAJNU POTPORU OPERACIJAMA
- SATNIJA ZA BESPOSADNE ZRAČNE SUSTAVE
- Ustrojbeni čin: natporučnik

Obrazovanje i osposobljavanje

2020. – 2022.
Magistar forenzike (smjer: Forenzika i nacionalne sigurnosti)
Sveučilišni odjel za forenzične znanosti, Split (Hrvatska)

2013. – 2016.
Stručni prvostupnik, bacc. javne uprave
Sveučilište u Splitu, Pravni fakultet

2002. – 2007.
Tehnička i industrijska škola Ruđera Boškovića u Sinju (Hrvatska)
Smjer: strojarski tehničar

Osobne vještine	Brza prilagodba na promjene, disciplina, inicijativa, pouzdanost, odgovornost, točnost, želja za usavršavanjem,
Materinski jezik	hrvatski jezik

Strani jezici	RAZUMIJEVANJE			GOVOR	PISANJE
	Slušanje	Čitanje	Govorna interakcija	Govorna produkcija	
engleski	C1	B2	C1	B2	B2
njemački	B1	A1	B1	B1	A2

*stupnjevi: A1 i A2 Početnik, B1 i B2 Samostalni korisnik, C1 i C2 Iskusni korisnik

Komunikacijske vještine	Verbalna i neverbalna komunikacija, prezentacija, javni govor, pisanje
Organizacijske/ voditeljske vještine	Rukovođenje, sposobnost odlučivanja, upravljanje kriznim situacija, rješavanje problema, strateško planiranje, pregovaranje
Digitalne vještine	Poznavanje rada na računalu – Word, Power Point, Excel, korištenje Interneta, pretraživanje raznih baza podataka, uporaba digitalnih/društvenih medija
Vozačka dozvola	B kategorija

IZJAVA O AKADEMSKOJ ČESTITOSTI

SVEUČILIŠTE U SPLITU
Sveučilišni odjel za forenzične znanosti

Informacijska sigurnost

Izjava o akademskoj čestitosti

Ja, ____Frano Dolić_____, izjavljujem da je moj diplomski rad pod naslovom: „Primjena i provođenje informacijske sigurnosti u Republici Hrvatskoj – regulativni okvir i standardi“

_____

rezultat mojega vlastitog rada, da se temelji na mojim istraživanjima te da se oslanja na izvore i radove navedene u bilješkama i popisu literature. Nijedan dio ovoga rada nije napisan na nedopušten način, odnosno nije prepisan bez citiranja i ne krši ičija autorska prava.
Izjavljujem da nijedan dio ovoga rada nije iskorišten u ijednom drugom radu pri bilo kojoj drugoj visokoškolskoj, znanstvenoj, obrazovnoj ili inoj ustanovi.
Sadržaj mojega rada u potpunosti odgovara sadržaju obranjenoga i nakon obrane uređenoga rada.

Split, _____

Potpis studenta/studentice: _____

POPIS SLIKA

SLIKE

TABLICE