Kibernetska sigurnost

Hercigonja, Maja

Undergraduate thesis / Završni rad

2019

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **The University of Applied Sciences Baltazar Zaprešić / Veleučilište s pravom javnosti Baltazar Zaprešić**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:129:855649

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-03-28**

Repository / Repozitorij:

Digital Repository of the University of Applied Sciences Baltazar Zaprešić - The aim of Digital Repository is to collect and publish diploma works, dissertations, scientific and professional publications





VELEUČILIŠTE
s pravom javnosti
BALTAZAR ZAPREŠIĆ
Zaprešić

Preddiplomski stručni studij
Informacijske tehnologije

MAJA HERCIGONJA

KIBERNETSKA SIGURNOST

STRUČNI ZAVRŠNI RAD

Zaprešić, 2020. godine

VELEUČILIŠTE
s pravom javnosti
BALTAZAR ZAPREŠIĆ
Zaprešić

Preddiplomski stručni studij
Informacijske tehnologije

STRUČNI ZAVRŠNI RAD

KIBERNETSKA SIGURNOST

Mentor:
prof. dr. sc. Vladimir Mateljan

Studentica:
Maja Hercigonja

Naziv kolegija:
UVOD U KRIPTOGRAFIJU

JMBAG studenta:
0234056378

SADRŽAJ

SAŽETAK 1
CYBER SECURITY 2
ABSTRACT 2
1. UVOD 3
1.1. Predmet i cilj rada 3
1.2. Struktura i sadržaj rada 3
2. INFORMACIJSKI SUSTAV 4
2.1. Pojam informacijskog sustava 4
2.2. Svrha, cilj i zadaci informacijskog sustava 5
2.3. Elementi, dijelovi i vrste informacijskog sustava 6
2.4. Rizici od zloporabe i informacijska sigurnost 8
3. KIBERNETIKA 11
3.1. Pojam kibernetike 11
3.2. Kibernetski prostor 12
3.3. Derivati kibernetike 12
3.4. Kibernetička kartografija 14
3.5. Kibernetski model sustava 14
4. PRIJETNJE KIBERNETSKOJ SIGURNOSTI 16
4.1. Kibernetski kriminal 17
4.2. Kibernetska špijunaža 17
4.3. Kibernetski terorizam 18
4.4. Kibernetski rat 19
4.5. Hibridni rat 20
5. MEĐUNARODNA SURADNJA I AKTIVNOSTI 21
5.1. Ujedinjeni narodi 21
5.2. INTERPOL 22
5.3. EUROPOL 23
5.4. NATO 23
5.5. Vijeće Europe 24

5.6. CEPOL 25
5.7. EC3 25
5.8. ENISA 25
6. KIBERNETSKA SIGURNOST U REPUBLICI HRVATSKOJ 27
6.1. Kibernetska sigurnost u Republici Hrvatskoj 27
6.2. Kibernetski napadi u Republici Hrvatskoj 29
6.3. Nacionalna strategija kibernetičke sigurnosti 30
7. ZAKLJUČAK 32
8. IZJAVA 34
9. POPIS LITERATURE 35
9.1. Knjige i članci 35
9.2. Internetski izvori 35
9.3. Završni radovi, diplomski radovi 37
10. POPIS SLIKA 39
ŽIVOTOPIS 40

SAŽETAK

Brzi razvoj tehnoloških sustava, napredak u tehnologiji i povećanje broja korisnika interneta predstavlja sve veću opasnost od cyber napada. Kibernetika kao znanstvena disciplina proučava opće zakonitosti procesa upravljanja i komunikacije, te je potrebna kako bi informacijski sustavi opstali. Informacijski sustav je dio svakog poslovnog sustava čija je funkcija kontinuirana opskrba potrebnim informacijama.

U ovom završnom radu opisan je opći dio informacijskog sustava i kibernetike. Cilj rada je prikazati i objasniti pojam kibernetike, njezine prijetnje i prevencije na području Republike Hrvatske.

Ključne riječi: IS, kibernetika, kibernetska sigurnost, kibernetske prijetnje

CYBERSECURITY

ABSTRACT

The rapid development of technological systems, advances in technology and the increasing number of Internet users poses an increasing threat of cyber attacks. Cybernetics, as a scientific discipline, studies the general principles of management and communication, and is required for information systems to survive. An information system is a part of any business system whose function is a continuous supply of necessary information.

This final paper describes the general part of an information system and cybernetics. The aim of this paper is to present and explain the concept of cybernetics, its threats and prevention in the territory of the Republic of Croatia.

Key words: IS, cybernetics, cyber security, cyber threats

1. UVOD

Internet i napredak u tehnologiji doveo je društvo do novog doba, informacijskog doba. Pristup internetu omogućen je gotovo svakom računalu ili mobilnom telefonu, dok je broj korisnika interneta sve veći. Porastom broja korisnika na internetu dolazi do suvremenih zahtjeva tržišta za sigurnošću interneta. Ranjivost interneta može biti u operacijskom sustavu, ali i u aplikacijama koje se svakodnevno koriste. Najveći problem u rješavanju napada predstavljaju hakeri koji koriste napredne sustave. Pravovremeno uočavanje i reagiranje na prijetnje je ključno za rješavanje problema cyber napada. Svrha završnog rada je naglasiti ulogu kibernetike, njezine sigurnosti i prevencije protiv računalnog kriminala.

1.1. Predmet i cilj rada

Predmet rada je kibernetska sigurnost. Cilj rada je objasniti IS. Približiti i teoretski objasniti čitatelju rad kibernetike te proučiti sigurnost kibernetike na području Republike Hrvatske. Korištena literatura obuhvaća knjige, znanstvene i stručne članke te relevantne internetske izvore.

1.2. Struktura i sadržaj rada

Struktura rada podijeljena je na sedam cjelina. Nakon uvodnog dijela, u drugoj cjelini se teoretski objašnjava i proučava IS. U trećoj cjelini riječ je o kibernetici, njezinom prostoru, kartografiji, derivatima te njezinom modelu sustava. Četvrta cjelina obrađuje prijetnje kibernetske sigurnosti, a peta cjelina se odnosi na međunarodnu suradnju i aktivnosti. Navode se i objašnjavaju međunarodne organizacije za borbu protiv kibernetskih prijetnji. Šesta cjelina odnosi se na područje Republike Hrvatske gdje se proučava sigurnost, važniji napadi koji su se odvijali u prošlosti te navodi se nacionalna strategija kibernetičke sigurnosti. U posljednjem dijelu u kojem se ističe značaj kibernetske sigurnosti, iznosi se zaključak završnog rada. Na samom kraju nalazi se popis literature popis slika.

2. INFORMACIJSKI SUSTAV

Svaki sustav sastoji se od uređenog skupa od najmanje dva elementa. Elementi su organizirani te tvore sistemsku funkciju. Broj elemenata mora biti konačan. U ovom poglavlju objašnjava se pojam IS, njegova svrha, cilj i zadaci, elementi i dijelovi IS-a. Uz navedeno spomenut će se i rizici od zloporabe i informacijska sigurnost.

2.1. Pojam informacijskog sustava

IS sastoji se od dvije riječi, informacije i sustava. Kombinacijom tih riječi dolazi do pojma informacijski sustav. Sustav je skupina komponenti povezanih u funkcionalnu cjelinu koji funkcioniraju zajedno da se postigne određeni rezultat, a informacija je resurs za rukovođenje. Razlikuje se od podataka, te je temelj za donošenja poslovnih i osobnih odluka. Neke od karakteristika informacije su pravovremenost, različitost karaktera i vrsta te se s toga može podijeliti na verbalnu, neverbalnu, slikovnu, primarnu, zvučnu i slično. Kao resurs ima posebna obilježja jer za razliku od ostalih resursa (energije) korištenjem se ne troši niti se smanjuje. Za donošenje odluka nisu dovoljne samo informacije, već je potrebno poznavati i metode koje omogućuju pronalaženje racionalnih rješenja, npr. metode za traženje optimalnog rješenja, simulacija poslovnih procesa ili ekspertni sustavi. Za kvalitetno i brzo prikupljanje i pohranjivanje informacija te njihovo učinkovito pretraživanje i upotrebu u metodama i modelima koji omogućuju donošenje kvalitetnih odluka, nužna je informacijska tehnologija (Čerić i Varga, 2004, 2). Pravovremenost informacije važna je za IS.

IS se ubraja u složene društvene sustave te se bavi podacima i informacijama. Navedeno se može pokrijepiti definicijama IS-a. Prema definiciji autora Paniana i Strugara "IS je uređeni skup elemenata odnosno komponenata koje u interakciji obavljaju funkcije prikupljanja, obrade, pohranjivanja i diseminacije (izdavanja na korištenje) informacija".[1] Prema definiciji autora Ćerića i Varge IS možemo definirati kao "sustav koji prikuplja, pohranjuje, čuva, obrađuje i isporučuje informacije važne za organizaciju, tako da budu dostupne i upotrebljive svakome kome su potrebne".[2] Ključni element u sustavu je informacija koja prestaje biti podatak kada u određenom kontekstu dobije značaj. Informacijski sustav se može koristiti informacijskom tehnologijom, ali i ne mora te je postao strateško oružje u konkurentskoj borbi na tržištu.

[1] Panian Ž., Strugar I. (2013). Informatizacija poslovanja. Zagreb. str. 23
[2] Čerić V., Varga M. (2004) Informacijska tehnologija u poslovanju str. 19

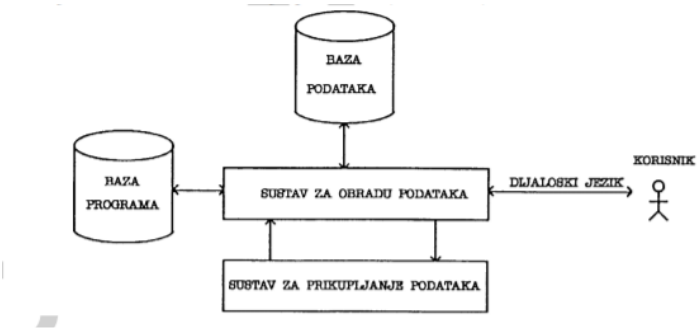
2.2. Svrha, cilj i zadaci informacijskog sustava

Svrha IS-a je dostaviti pravu informaciju u pravo vrijeme, na pravom mjestu i uz minimalne troškove. IS uključuje organizaciju, infrastrukturu, tehnologiju i ljude potrebne za rad s informacijama. U nekim organizacijama poslove obavlja moderna informacijska tehnologija, dok negdje te postupke obavljaju ljudi.

Kao što su uočili autori Čerić i Varga cilj IS-a je opskrbiti poslovni sustav informacijama potrebnima izvršnom podsustavu za:[3]

- izvođenje poslovnog procesa
- upravljačkom podsustavu za upravljanje poslovnim sustavom
- suradnji i komunikaciji unutar poslovnog sustava i prema okolini.

IS poduzeća upravlja tokovima informacija i podataka od izvora do odredišta, menadžera koji na temelju dobivenih rezultata donosi odluke. Glavni zadatak IS-a je osigurati informacije za upravljanje poslovnim sustavom. Svaka organizacija nastoji izgraditi kvalitetni IS koji će davati točne informacije brzo i za kvalitetno donošenje odluka. Najvažnije zadaće su prikupljanje te obrada tih podataka, njihovo pohranjivanje i čuvanje te oblikovanje i raspoređivanje podataka i informacija na sve radne razine poslovnog sustava. Kod prikupljanja podataka moramo odabrati izvorni sustav podataka, podrijetlo ulaznih podataka te moramo napraviti pripremu za unošenje podataka. Podaci mogu nastati u poslovnom procesu, izvan poslovnog procesa, podaci koji su nastali u postupku odlučivanja te oni koji su nastali na različitim razinama odlučivanja. Prikupljeni podaci se obrađuju te se pohranjuju radi potrebe kasnijeg korištenja ili se dostavljaju korisnicima radi potrebe odlučivanja. Jedan od zadataka je i osigurati informacije i znanje za potrebe odlučivanja i upravljanja poslovanjem te najvažniji zadatak informacijskog menadžera je planiranje, odabir i izrada strategije.



Slika 1. Informacijski sustav

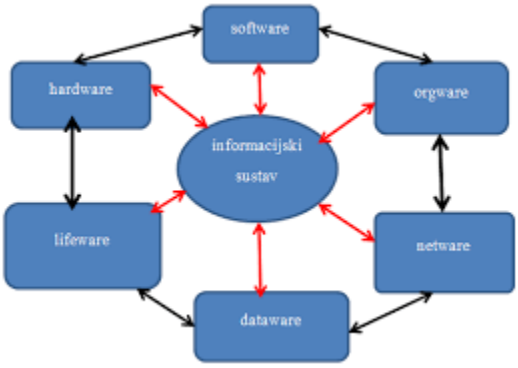
Izvor: https://www.fpz.unizg.hr/ztos/iszp/a2.pdf

[3] Čerić V., Varga M. (2004) Informacijska tehnologija u poslovanju str. 20

2.3. Elementi, dijelovi i vrste informacijskog sustava

IS se sastoji od različitih elemenata koji su potrebni za obavljanje gore navedenih funkcija. Osnovni elementi IS-a su:[4]

- hardware ili materijalno – tehnička komponenta – fizički dio informacijskog sustava. Strojevi, uređaji i sredstva namijenjena isključivo ili pretežito obradi podataka i informacija
- software ili nematerijalna komponenta – nematerijalni dio informacijskog sustava u obliku programskih rješenja. Ukupno ljudsko znanje ugrađeno u strojeve, opremu i uređaje koji je predmet obrade ili određuje način obrade u sustavu
- lifeware ili ljudska komponenta – ljudi koji rade s informacijskim tehnologijama te na bilo koji način sudjeluju u radu sustava i koriste rezultate obrade podataka i informacija
- netware ili prijenosna komponenta – tvori sredstva i veze za prijenos podataka na daljinu, odnosno komunikacijska i mrežna rješenja koja povezuju sve elemente u jednu cjelinu
- orgware ili organizacijska komponenta – organizacijski postupci i metode povezivanja svih elemenata u jednu cjelinu.



Slika 2. Elementi informacijskog sustava
Izvor: https://repozitorij.fpz.unizg.hr/islandora/object/fpz%3A1319/datastream/PDF/view

IS dolazi u različitim oblicima i veličinama te se može podijeliti na više dijelova, od kojih je svaki zadužen za izvršenje jednog od ciljeva:[5]

- sustav za obradu transakcija
- sustav za potporu odlučivana
- sustav za komunikaciju, suradnju i individualni rad.

[4] Panian Ž., Strugar I. (2013). Informatizacija poslovanja. Zagreb. str. 28
[5] Čerić V., Varga M. (2004) Informacijska tehnologija u poslovanju str. 22

Sustav za obradu transakcija služi za izvođenje poslovnog procesa. Pripada operativnoj razini poslovnih aktivnosti te je potpora izvršnom podsustavu za izvođenje poslovnih procesa. Povezuje informacije u cjelovit sustav za praćenje, isto tako vodi evidenciju o obavljenim transakcijama, generira potrebne dokumente u poslovanju i izvještava o stanju poslovnog procesa.

Sustav za potporu odlučivanja služi za upravljanje poslovnim sustavom, te je isto tako informativni i analitički sustav. Cilj sustava je da uz pomoć informacija iz transakcijskog dijela pomogne u procesu donošenja odluka. Obrađuje informacije dobivene iz različitih unutarnjih i vanjskih izvora te je nova generacija BI sustava (sustavi poslovne inteligencije).

Sustav za komunikaciju, suradnju i individualni rad je dio IS-a koji uključuje različite primjene informacijske tehnologije za obavljanje administrativnih poslova, naziva se i uredski sustav. Potpora je radu u skupinama kako bi bilo učinkovitije skupno odlučivanje (telekonferencije), ali potpora je i individualnom radu.



Slika 3. Slojevi informacijskog sustava

Izvor:https://www.pfri.uniri.hr/knjiznica/NG-dipl.LMPP/269-2014.pdf

Kako poslovni sustavi nemaju isti značaj primjene informacijskih sustava razlikujemo četiri osnovna tipa informacijskih sustava. To su:[6]

- operativni informacijski sustav
- potporni informacijski sustav
- strateški informacijski sustav
- izgledni informacijski sustav.

Operativni informacijski sustav je sustav o kojemu ovisi uspjeh tekućeg poslovanja. Ovisan je o informacijskoj tehnologiji, te informacijski sustav služi kao potpora svakodnevnom poslovanju.

Potporni informacijski sustav je sustav koji je koristan ali nije nužan za poslovni uspjeh poduzeća. Postoji mala ovisnost o tehnologiji te mala ovisnost o funkcioniranju poduzeća.

[6]Peraković D., Periša M.: Informacijski sustavi mrežnih operatera, Sveučilište u Zagrebu, URL: https://www.weboteka.net/fpz/Informacijski%20sustavi%20mre%C5%BEnih%20operatera/04_-_Podjele_vrste_i_elementi_informacijskih_sustava.pdf (n.d.)

Strateški informacijski sustav je sustav koji je kritičan za buduću poslovnu strategiju i za buduće poslovanje poduzeća. Jako ovisi o informacijskoj tehnologiji, te mora omogućiti brzu obradu i sigurnu pohranu podataka. Uspjeh poduzeća ovisi o strateškom informacijskom sustavu.

Izgledni informacijski sustav je sustav koji može, ali i ne mora utjecati na buduće poslovanje i budući uspjeh poduzeća te možemo reći da ovdje postoji mala ovisnost o tehnologiji, dok je utjecaj na poslovni rezultat značajan.

Operativnoj razini pripadaju transakcijski sustavi koji su namijenjeni za izvođenje procesa osnovne djelatnosti. Taktičkoj razini namijenjeni su izvršni informacijski sustavi čiji rezultat su izvješća nužna za upravljanje. Strateškoj razini namijenjeni su sustavi potpore odlučivanju kao što je prikazano na slici 4.



Slika 4. Strukturna razina informacijskog sustava

Izvor:https://repozitorij.fpz.unizg.hr/islandora/object/fpz%3A1319/datastream/PDF/view

Svakom sustavu pripada i neki informacijski podsustav te se tako može odrediti tip informacijskog podsustava. Također može se i ocijeniti redoslijed izgradnje IS-a. Neovisno o sustava, u njega s spremaju podaci potrebni za daljne korištenje i odlučivanje, te zbog toga IS mora zadovoljiti određena načela. Cilj postojanja IS-a je unaprijediti poslovanje te ostvariti ukupan pozitivan poslovni rezultat.

2.4. Rizici od zloporabe i informacijska sigurnost

Kako bi mogli definirati rizike zloporabe potrebno je prvo definirati pojam rizika te pojam rizika u informacijskoj tehnologiji. Rizik u općem smislu bila bi neka opasnost od učinjene aktivnosti koja može dovesti do neželjenih i negativnih posljedica.

Primjenjujući ovu definiciju rizika, možemo definirati rizik u informacijskoj tehnologiji. Prema autorima Paniana i Strugara možemo reći da "Rizici informacijske sigurnosti predstavljaju opasnost da njena primjena dovede do neželjenih posljedica (šteta) u organizacijskom sustavu i/ili njegovome okruženju".[7]

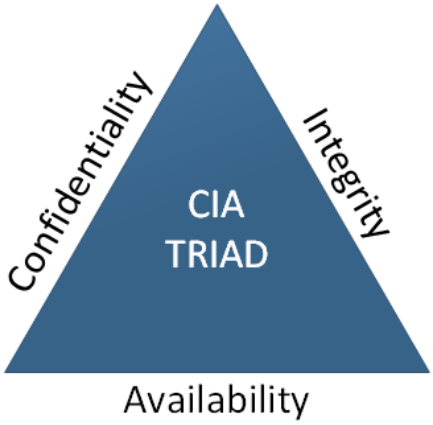
Rizici mogu imati dva obilježja (težina i učestalost) te se mogu podijeliti na objektivne i subjektivne. Objektivni su oni koji nastaju funkcioniranjem sustava u kojem se informacijska tehnologija koristi, a subjektivni su oni koji nastaju namjerom skupine ili pojedinca, isto tako se mogu javiti u sustavu kada se ne zaštiti od objektivnih rizika (Panian i Strugar, 2013). Objektivne rizike nije moguće u potpunosti izbjeći, dok se subjektivni mogu u potpunosti izbjeći prevencijom u sustavu. Kao osnovni nedostatak svih metoda kvantifikacije rizika navodi se visok stupanj subjektivnosti koju je nemoguće izbjeći, te kao zaključak može se reći da sigurna metoda kvantifikacije ne postoji, da nema potpuno sigurne zaštite te da na rizike treba uvijek računati.

Informacijska tehnologija pruža različite mogućnosti u poslovnom i osobnom svijetu, ali i velike mogućnosti zloporabe i kriminalnih djelatnosti. Kako bi mogli definirati informacijsku sigurnost, prvo ćemo definirati sigurnost. Sigurnost bi bila skup postupaka i procesa za održavanje prihvatljivog rizika. Informacija je imovina za poslovanje organizacije te kao takva mora uvijek biti prikladno zaštićena.

"Informacijska sigurnost je stanje povjerljivosti, cjelovitosti i raspoloživosti podatka, koje se postiže primjenom propisanih mjera i standarda informacijske sigurnosti te organizacijskom potporom za poslove planiranja, provedbe, provjere i dorade mjera i standarda".[8] Informacijska sigurnost postaje važan faktor u modernom društvu. Svi podaci, povjerljivi i tajni, nalaze se u računalnom oblaku koji ovisi o stalnoj zaštiti, isto tako koristimo ju kako bi zaštitili informacije od prijetnji, kako bi smanjili rizik i povećali broj poslovnih prilika te kako bi zaštiti svoje poslovanje.

Postoje tri aspekta informacijske sigurnosti, a njihova povezanost prikazana je na slici 5. kroz sigurnosni trokut (eng. CIA triad). Aspekti se sastoje od povjerljivosti, integriteta i dostupnosti.

[7] Panian Ž., Strugar I. (2013). Informatizacija poslovanja. Zagreb. str. 237
[8] Ured vijeća za nacionalnu sigurnost, URL: https://www.uvns.hr/hr/sto-je-to-informacijska-sigurnost (n.d.)



Slika 5. Sigurnosni trokut

Izvor: https://blufreview.com/2018/05/05/what-is-the-cia-triad/

Povjerljivost podataka (eng Confidentiality) se odnosi na tajnost i dostupnost podataka samo ovlaštenim osobama. Najčešće prijetnje koje ugrožavaju povjerljivost podataka su hakiranje i trojanski konji, dok su dvije metode očuvanja povjerljivosti podataka, a one su kontrola pristupa i metoda enkripcije.

Integritet podataka (eng Integrity) se odnosi na podatke koji moraju ostati u istom obliku, drugim riječima ne smiju se mijenjati bez dopuštenja ovlaštene osobe. Isto kao i povjerljivost, integritet se održava upotrebom kontrole pristupa i enkripcijom.

Treći aspekt se odnosi na dostupnost podataka (eng Availability). Cilj ovog aspekta je pružiti prave podatke u pravo vrijeme. Najčešći razlog uskraćivanja dostupnosti je nemogućnost osiguravanja podataka u vrijeme prirodnih katastrofa.

Kao zaključak možemo navesti da najviše prijetnji ima povjerljivost odnosno tajnost podataka ili informacija. Neovlašteni upadi narušavaju integritet podataka, dok prekid rada sustava uzrokuje nedostupnost podataka ili informacija. IS je siguran kada se zadovolje navedeni aspekti.

3. KIBERNETIKA

Kibernetika je znanstvena disciplina novijeg nastanka. Temelj odnosno otac moderne kibernetike u današnjem obliku je Norbert Wiener. Ovo poglavlje govori o pojmu kibernetici te njezinim sastavnicama.

3.1. Pojam kibernetike

"Kibernetika je znanost koja istražuje opće zakonitosti procesa upravljanja i veza u bilo kojim sustavima (tehničkim, biološkim, ekonomskim, socijalnim, administrativnim i dr.)".[9] Engleski naziv je Cybernetics. Prijevod za riječ cyber ne postoji. "Prema pojmovniku National Security Agency (NSA) cyber je prefiks koji se koristi kako bi se osoba, stvar ili ideja svrstala kao dio računalnog ili informacijskog doba. Dakle, kibernetika je znanstvena disciplina, a cyber se, kako je navedeno u pojmovniku NSA-e, odnosi na svijet koji nastaje pomoću računala".[10] Dolazi od grčke riječi kibernien što znači upravljati. Norbert Wiener je 1948. Godine objavio knjigu o kibernetici u kojoj je opisao razmatranja i zaključke o metodama i komunikaciji tehničkih uređaja i živih bića.

Općenito, kibernetika je znanost o upravljanju strojeva i živih bića. S informacijsko – sustavnog gledišta, kibernetika znatno utječe na razvoj mnogih područja znanosti koji dovodi do novog pristupa analizi te razvitka ideja. Kibernetika svoja promatranja gradi na sustavima koji imaju određene ciljeve. Svaki sustav je cjelina koja je povezana s okolinom uz pomoć ulaznih i izlaznih jedinica. Kibernetika se isto tako bavi i proučavanjem organiziranih sustava s unutrašnjim i vanjskim informacijama. Razvojem kibernetike ljudi su počeli razvijati sredstva za upravljanje stvarima i energijom, što je ujedno i tehnologija uporabe informacije. Područje primjene kibernetike je veliko, stoga su se razvile različite grane kibernetike. Najvažnije grane su teorija informacije, teorija kodiranja, teorija igara, matematička logika, stohastički procesi, robotika, teorija pouzdanosti. Kibernetika ne nudi gotova rješenja problema, već samo nudi mogućnosti za njihovo uspješno rješavanje.

[9] Leksikografski zavod Miroslav Krleža URL: http://enciklopedija.lzmk.hr/clanak.aspx?id=18859 (n.d.)
[10] Vuković H.: Kibernetska sigurnost i sustav borbe protiv kibernetskih prijetnji u Republici Hrvatskoj, vol.*13*, br.3, str. 15, 2012., URL: https://hrcak.srce.hr/100728

3.2. Kibernetski prostor

Kibernetski prostor (eng Cyberspace) je ukratko elektronički medij koji olakšava internetsko komuniciranje. Koristi se za opisivanje virtualnog svijeta računala. Primjerice, ukoliko pošaljemo e-mail s jednog računala na drugo, možemo reći da smo ga poslali preko kibernetskog prostora. William Gibson je prvi put upotrijebio tu riječ u svojoj knjizi "Neuromancer" napisane 1984. godine. Osnovna značajka za cyberspace je interaktivnost te virtualno okruženje za velik broj korisnika. Ljudi, informacijski prostor i kibernetski prostor često isto definiraju, ali postoji razlika. Razlika je u tome što je informacijski prostor širi pojam od kibernetskog prostora.

"U listopadu 2006. Združeni stožer oružanih snaga SAD-a definirao je kibernetski prostor kao „područje koje karakterizira upotreba elektroničkog i elektromagnetskog dijapazona za pohranjivanje, modificiranje i razmjenjivanje podataka putem mrežnih sustava i povezanih fizičkih infrastruktura". Korisnici kibernetskog prostora poput domaćinstva, korporacija, sveučilišta, vlada, oružanih snaga itd. kreću se kibernetskim prostorom kako bi izgradili ili dostigli informacijska odredišta koja se dijele, stječu i nadziru putem mrežnih sustava u kojima povezanost čine obične telefonske linije, mikrovalni uređaji, satelitske uzlazne i silazne veze, optička vlakna, kablovi, tranzistori i mikročipovi. Internet je najpoznatiji i najrasprostranjeniji mrežni sustav. U kibernetskom prostoru, informacije su dostupne u realnom vremenu i njihova bitna odrednica postaje temporalnost, ovisnost o vremenu, a ne o prostoru. Za brze promijene u kibernetskom prostoru potrebno je vrlo malo vremena".[11]

Kibernetski prostor postaje novo polje u međunarodnim odnosima. Virtualan je, ali sve više postaje realna stvarnost u kojoj osim pristupa, prijenosa i raspodjele podataka i informacija dolazi i do blokiranja i manipulacije istih. Kibernetski napadi na digitalne sustave različitih institucija i organizacija danas su jedna od najvećih prijetnji i opasnosti za nacionalnu sigurnost. Kibernetske aktivnosti dijele se na četiri područja, a ona su kibernetski kriminal, kibernetska špijunaža, kibernetski terorizam te kibernetski rat. Navedene prijetnje i aktivnosti detaljnije će se obraditi u sljedećem poglavlju.

3.3. Derivati kibernetike

"Kibernetika je općenita, temeljna (fundamentalna) znanost koja se bavi općim pitanjima, a ne pojedinostima funkcioniranja sustava i upravljanja njime. Kako se, međutim, sustavi u stvarnosti mogu po mnogo čemu međusobno razlikovati, razlikovat će se i načini upravljanja takvim sustavima.

[11] Vuković H.: Kibernetska sigurnost i sustav borbe protiv kibernetskih prijetnji u Republici Hrvatskoj, vol.*13*, br.3, str. 16, 2012., URL: https://hrcak.srce.hr/100728

Imajući to u vidu, znanstvenici, suvremenici N. Wienera prionuli su istraživanju brojnih aspekata i načina upravljanja sustavima različitih vrsta, svojstava i tipova. Tako je u razmjerno kratkom vremenu nakon pojave kibernetike razvijeno nekoliko desetaka različitih novih teorija koje svoje uporište nalaze u kibernetici, a nastoje objasniti pojedine aspekte procesa upravljanja sustavima. Takve su izvedene, specijalizirane znanstvene discipline nazivaju derivatima (izvedenicama) kibernetike".[12]

Sa stajališta razvitka znanstvene discipline – informatike, od posebnog su interesa sljedeći derivati kibernetike:[13]

- teorija komunikacija
- teorija odlučivanja
- teorija programiranja
- teorija povratne veze
- opća teorija sustava.

Teorija komunikacija definira različite odnose te istražuje i iskorištava zakonitosti slanja, prijenosa, primanja i tumačenja signala. Dijeli se na teoriju informacija, teoriju kodiranja i teoriju znakova. Teorija informacija se bavi istraživanjem informacija kod prijenosa između komunikacijskih partnera. Teorija kodiranja bavi se prikazivanjem informacijskog sadržaja, dok teorija znakova definira elemente informacijskog sadržaja, njihove odnose i povezivanje informacijskog sadržaja u cjeline.

Teorija odlučivanja omogućuje izbor najpovoljnije opcije, a zasniva se na obradi informacija potencijalnih opcija. Dijeli se na teoriju racionalnog odlučivanja, teoriju intuitivnog odlučivanja i heuristiku. Teorija racionalnog razmišljanja određuje načine postupanja te donošenja odluka kada se ima pouzdana i potpuna informacija, dok se teorija intuitivnog odlučivanja definira kada se nema dovoljno ili uopće nema informacija. Heuristika je teorija odlučivanja koja nastoji uvažiti i upotrijebiti i teoriju racionalnog odlučivanja i teoriju intuitivnog odlučivanja.

Teorija programiranja definira načine sustavnog korištenja znanja kod upravljanja sustava. Dijeli se na teoriju algoritma i teoriju automata. Teorija algoritma određuje načine prikazivanja znanja u obliku algoritama koji vode do rješenja problema, dok teorija automata definira algoritamske izvedbe uređaja i strojeva za obavljanje operacija.

Teorija povratne veze ima ključnu ulogu kod upravljanja složenim sistemima, a dijeli se na tehničku teoriju povratne veze i soijalnu teoriju povratne veze. Tehnička teorija povratne veze ima cilj ostvariti povratnu vezu u tehničkim sustavima, dok socijalna teorija ostvaruje povratnu vezu u društvenim skupinama i zajednicama.

[12] Panian, Ž. (2001). Poslovna informatika (Koncepti, metode i tehnologija). Zagreb. str. 9
[13] Ibidem

3.4. Kibernetička kartografija

"Kibernetička kartografija je organizacija, prezentacija, analiza i komunikacija prostorno referenciranih informacija o velikom broju društveno interesantnih tema u interaktivnom, dinamičkom, multisenzorskom formatu upotrebom multimedije i multimodalnih sučelja".[14] D. R. Fraser Taylor je zaslužan za objašnjenje naziva, kako bi osvijestio promjene u teoriji i praksi kartografije. Projekt razvijanja kibernetičke kartografije je osmišljen i predstavljen da istakne korist kibernetičke kartografije za informacijsko gospodarstvo. Za razvoj važna je potpora te multidisciplinarni tim koji se sastoji od ljudi iz privatnog i javnog sektora te različitih vrsta organizacija. Temelj projekta su karte i kartografija. Karte se koriste u multimedijskim formatima, dok kartografiramo mozak, budućnost te kreiramo mentalne mape. Rezultat kibernetičke kartografije je kibernetički kartografski atlas kojega definiramo kao metaforu za informacije povezanih lokacijom. (Frančula, 2015).

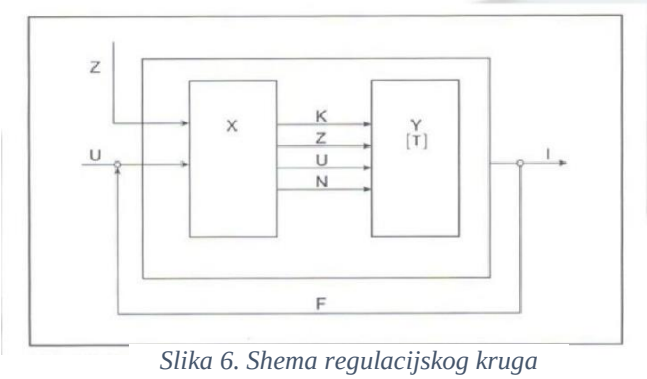
Kibernetička kartografija ima sedam glavnih svojstava. Kibernetička kartografija:[15]

- je multimedijalna pomoću vida, sluha, dodira i eventualno mirisa i okusa
- koristi se multimedijskim formatima i novim komunikacijskim tehnologijama poput weba
- je interaktivna i korisnici karata ubrzo postaju kreatori karata
- primjenjuje se na širok raspon društveno interesantnih tema uključujući teme koje se obično ne kartografiraju
- je informacijsko/analitički paket i organizacijski okvir za proizvode i procese koji nastaju u eri web 2.0 društvenog računalstva
- stvara proizvode koje sastavljaju timovi individualaca iz različitih disciplina ne samo kartografi te
- uključuje partnerstvo s vladom i industrijom u novim istraživanjima i razvoju proizvoda.

3.5. Kibernetski model sustava

Wiener je sva svoja istraživanja te rezultate tih istraživanja objasnio i sažeo u jednostavan model kojeg je nazvao regulacijski krug. Regulacijski krug prikazuje se uz pomoć metode crne kutije. Crnom kutijom se proučavaju odnosi ulaza i izlaza u sustave bez ozbira na unutarnju građu sustava. Shema regulacijskog kruga prikazan je na slici 6.

[14] Nedjeljko Frančula.(2015). Kibernetička kartografija. URL: https://bib.irb.hr/datoteka/771538.Kibernetika_kartografija.pdf
[15] Ibidem



Slika 6. Shema regulacijskog kruga

Izvor:https://slideplayer.com/slide/14513303/

Slika 6. prikazuje dijagram kibernetskog modela sustava." U sustav ulaze regularni ulazi i smetnje. Prihvaća ih upravljački član, analizira ih i, popraćene naredbama o načinu izvođenja procesa transformacije, prosljeđuje izvršnom članu. Izvršni član provodi proces transformacije stvarajući sustavski izlaz. Etalon (reprezentativni uzorak) generiranog sustavskog izlaza vraća se u obliku povratne veze kao dodatni ulaz u sustav. Povratnom vezom (engl. Feed-Back) ostvaruje se funkcija kontrole (samokontrole) nad radom sustava i vrsnoćom njegova izlaza. Utvrdi li se na temelju povratne veze da sustav ne proizvodi izlaze željene kvantitete (količine) i/ili kvalitete (vrsnoće), upravljački će član definirati dodatne naredbe (korektive) kojima će nastojati poništiti (kompenzirati) možebitni negativni utjecaj smetnji na djelovanje sustava. Postupak se ponavlja sve dok se sustavski izlaz ne dovede u željene okvire".[16]

Elementi regulacijskog kruga su:[17]

- regulirani ulaz (U)
- smetnje (Z)
- upravljački član (X)
- naredbe (N)
- dodatne naredbe (K)
- izvršni član (Y)
- proces transformacije (T)
- sustavski izlazi (I)
- povratna veza (F).

U današnje vrijeme regulacijski krug se uobičajeno naziva upravljačkim sustavom. Zadaća odnosno funkcija upravljačkog sustava ostvaruje se mehanizmom povratne veze na način izravnog uvida u obilježja sustava ili prijenosom informacija o izlazu sistema.

[16] Panian, Ž. (2001). Poslovna informatika (Koncepti, metode i tehnologija). Zagreb. str. 8
[17] Ibidem

4. PRIJETNJE KIBERNETSKOJ SIGURNOSTI

Da bi bilo moguće podijeliti kibernetske prijetnje, prvo je potrebno objasniti pojmove prijetnja, rizik te ranjivost. Općenito prijetnja bi bila potencijalni uzrok negativnog događaja koji se izvršava ukoliko se iskoristi ranjivost nekog sustava te se zatim prouzroči neželjena šteta. Rizik je vjerojatnost nekog događaja i njegove posljedice dok bi općenito ranjivost bila pogreška ili slabost resursa koji može naštetiti sigurnosti sustava.

S obzirom na cilj, napadi mogu biti usmjereni na podatke ili nadzorne sustave (Vuković, 2012: 17). Ukoliko je napad usmjeren na podatke, njegov cilj je ukrasti ili uništiti podatke i informacije neke organizacije. Ukoliko je napad usmjeren na nadzorni sustav, njegov cilj je penetracija u postrojenja, primjerice elektroenergetski sustav.

Vuković (2012: 18) u svom radu navodi dobar primjer Lecha J. Janczewskog i Andrewa M. Colarika koji cyber napade uspoređuju s provalom u bolničku bazu podataka. Navode da ako netko provali u tu bazu podataka i prepiše lijek pacijentu koji je na njega alergičan, pacijent će umrijeti. Riječ je o kaznenom dijelu izvedenom pomoću računalne tehnologije, a koje se može protumačiti kao kibernetski kriminal. Ako se dogodi da taj isti napadač kasnije objavi da je to tek početak odnosno da je spreman počiniti još takvih djela, ukoliko mu se ne ispune zahtjevi, tada je riječ o kibernetskom terorizmu. Ako je nadalje napadač odnosno cyber kriminalac još i agent strane protivničkih strukutra, primjerice strane obavještajne agencije, tada se govori o kibernetskom ratovanju.

Iz gore navedenog primjera prema autoru Vukoviću maliciozne kibernetske aktivnosti možemo podijeliti na: [18]

- kibernetski kriminal
- kibernetska špijunaža
- kibernetski terorizam
- kibernetsko ratovanje.

Navedenoj podjeli se može dodati i u novije vrijeme raširen oblik hibridnog rata.

[18] Vuković H.: Kibernetska sigurnost i sustav borbe protiv kibernetskih prijetnji u Republici Hrvatskoj, vol.*13*, br.3, str. 17, 2012., URL: https://hrcak.srce.hr/100728

4.1. Kibernetski kriminal

Pojam kibernetskog kriminala javlja se krajem prošlog stoljeća, a definira se kao kriminal koji se izvodi uz pomoć računalne tehnologije u kibernetskom prostoru. Kibernetski kriminal se najčešće povezuje s prijevarama na području internet bankarstva i raznim prijevarama na internetu korištenjem tuđih, nelegalno stečenih, kreditnih kartica. Vuković (2012: 20) u svojem radu navodi da je s godišnjom stopom rasta od oko 40 posto i s trenutnom zaradom od oko 100 milijardi dolara riječ o najbrže rastućem sektoru globalnog organiziranog kriminala.

Pretpostavka je da će u budućnosti kibernetski kriminal još više rasti zato što za izvršenje napada tog oblika nije potrebna fizička prisutnost napadača, već se napadač može nalaziti na drugom kraju svijeta odnosno udaljen od svoje mete. Danas je moguće kupiti oružje ili upasti u informacijske sustave raznih organizacija i institucija samo klikom miša na računalu. Vjerojatnost da će napad obaviti amater odnosno nepismeni pojedinac je vrlo mala, vještine koje su potrebne kao i znanje za napad ne uči se na fakultetima ili seminarima, već se u današnje vrijeme sve uči preko interneta. Zahvaljujući informacijama kojima internet (pogotovo dark web) ima velika je vjerojatnost da će kriminalac steći potrebna znanja na forumima i online vodičima.

Pod pojmom kibernetski kriminal treba svrstati samo kaznena djela kod kojih je upotreba računala ključna za napad, a ne ona kaznena djela kod kojih se računalo pojavljuje samo kao sredstvo napada. Kao primjer Vuković (2012: 21) navodi da kazneno djelo krivotvorenja novca ne spada pod kibernetski kriminal bez obzira što se počinitelj prilikom krivotvorenja novca služio računalnom tehnologijom.

Konvencija o kibernetskom kriminalu donijelo je Vijeće Europe 23. studenoga 2001. godine, a stupila je na snagu 1. srpnja 2004. godine. Konvencija predstavlja oblik međunarodnog ugovora, a međunarodnim ugovorima se uređuju odnosi između subjekata međunarodnog prava.

4.2. Kibernetska špijunaža

Kibernetska špijunaža je metoda koja se koristi preko interneta, a njezino glavno obilježje je odavanje tajni u obliku predaje, objave ili obavijesti povjerljivih podataka. Cyber špijunaža je akt ili praksa dobivanja tajne bez odobrenja nosioca informacija (osobnih, osjetljivih, vlasničkih ili tajnih) od pojedinca, konkurenata, vlade i slično za ekonomsku, političku ili vojnu prednost koristeći nelegalne metode na internetu, mreži ili pojedinačnim računalima (Ugren, 2012: 11).

Kibernetska špijunaža najčešće se izvodi pomoću špijunskih programa, trojanskih konja (zlonamjerni softver napravljen za špijunažu korisnika u svrhu ostvarivanja novčane koristi od strane napadača) i drugim virusima. Kibernetska špijunaža može biti i jedan od elemenata informacijskog i/ili kibernetskog rata. Najčešće se koristi u industriji, ali i u vojsci i na razini država ili obavještajnih agencija neke zemlje. U industriji se koristi kako bi se stekla prednost nad konkurencijom u smislu da se istraže pojedinosti o proizvodu koji nudi konkurencija te da se nakon toga napravi bolji proizvod od konkurencije. U vojne svrhe koristi se da bi se saznalo s kojim resursima raspolaže ciljana država.

Primjer jednog od najvećeg slučaja kibernetske špijunaže je operacija "Shady RAT", niz cyber napada koji su počeli sredinom 2006. godine. Operaciju je otkrila kompanija McAfee u kolovozu 2011. godine. Operacija je trajala pet godina i došlo je do krađe intelektualnog vlasništva i strateških informacija u više od 70 multinacionalnih korporacija, vladi i organizacija i 14 zemalja. Popis žrtava visokih profita uključuje SAD, Tajvan, Južnu Koreju, Vijetnam, Indiju i Kanadu. Napad je bio usmjeren i na Ujedinjene narode, Međunarodni olimpijski odbor, Svjetsku antidoping agenciju i mnoge kompanije sa visokim vojnim ugovorima. Većina napada započela je slanjem e-mailova sa virusom na ciljane kompanije. Klikom na zaraženi link haker je preuzeo kontrolu nad računalom. Ukradeni podaci uključuju državne tajne, pregovaračke planove, podatke o nafti, ugovore, arhiva e-mailova i mnogo drugih dokumenata. Optužbe su bile usmjerene prema Kini, ali na kraju se ne zna tko je stajao iza napada.



Slika 7. Zemlje koje su bile mete napada špijunaže

Izvor: https://www.zdnet.com/article/operation-shady-rat-five-things-to-know/

4.3. Kibernetski terorizam

Kibernetski terorizam su planirani napadi na računalne sisteme ili mreže te politički motivirani napadi od strane nacionalnih skupina. Prema definiciji autora Vukovića "Kibernetski terorizam označava promišljene, političke motivirane napade izvršene od strane nacionalnih skupina ili

prikrivenih čimbenika, odnosno pojedinaca, usmjerene protiv informacijskih ili računalnih sustava, računalnih programa, te podataka, a koji rezultiraju nasiljem nad neborbenim metama".[19] Ciljevi kibernetskog terorizma su prijetnje vladi ili građanima neke zemlje i stvaranje ekonomskih gubitaka. Kibernetski terorizam podrazumijeva i fizičke napade te uništavanje infrastrukture i važnih sustava u organizacijama. Kibernetski terorizam događa se u kibernetskom prostoru, uključuje i fizičko uništavanje sustava i uređaja u kojem je informatička komponenta.

Zahvaljujući razvoju računalne tehnologije terorističke organizacije koriste internet za širenje svojih ideja. Koriste web stranice za privlačenje novih članova, ali i za prikupljanje potrebnih sredstava. Jedna od najpoznatijih skupina danas je tzv. Islamska država Iraka i Levanta (ISIL). Skupina je poznata po regrutiranju sljedbenika preko društvenih mreža i web stranica na kojima dogovaraju napade.

Danas se je teško boriti protiv kibernetskog terorizma iz razloga što alati za cyber kriminal ne identificiraju napadača za vrijeme njegovih napada. Za očekivati je da će navedeni oblik terorizma napredovati te da će svaki napad putem računala rezultirati ljudskim žrtvama. Upotreba kibernetskog i fizičkog terorizma pokazala se kao najdjelotvornija kombinacija. Vuković (2012: 19) navodi da je za pretpostaviti kako teroriste kibernetski napadi sve više privlače jer zahtijevaju manje ljudstva i manje resursa, nadalje obrazlažuje kako teroristima navedeni napadi dopuštaju fizičku odsutnost od mjesta napada, kao i veću mogućnost da ostanu nepoznati.

4.4. Kibernetski rat

Kibernetski rat (eng. Cyberwar) je rat koji se provodi uz pomoć računala i računalne mreže. Uglavnom se poduzima od strane država, a vodi se protiv drugih država, njihove vlade i vojne mreže sa ciljem uništavanja ili ometanja njihove upotrebe. Često ga uspoređuju sa informacijskim ratom u kojem se krađom protivničkih podataka i informacija i njihovom razmjenom pokušava postići prednost nad protivnikom u ratu.

U prošlosti je kibernetsko ratovanje podrazumijevalo samo podbadanje između zemalja (npr. tražile su se sigurnosne rupe), danas su se zbog veće upotrebe ekonomskih, komunikacijskih i vojnih sistema stvorili uvjeti za pravi kibernetski rat. Kao glavne zemlje navode se Kina i SAD. Kako Ugren (2012: 15) navodi, kibernetski rat između dvije navedene zemlje nije samo digitalni rat nego su u sukob uključene i najveće svjetske internet kompanije kao što su Facebook, Google.

[19] Vuković H.: Kibernetska sigurnost i sustav borbe protiv kibernetskih prijetnji u Republici Hrvatskoj, vol.*13*, br.3, str. 18, 2012., URL: https://hrcak.srce.hr/100728

Kibernetsko ratovanje nebi se trebalo poistovjetiti s terorističkim korištenjem kibernetskog prostora, kibernetskom špijunažom i kibernetskim kriminalom. Vuković (2012: 20) navodi da iako su taktike slične, pogrešno bi bilo sve poistovjetiti s djelima kibernetskog ratovanja. Kao primjer navodi da neke države koje su se upustile u kibernetsko ratovanje isto tako mogu se upustiti i u kibernetsku špijunažu, no objašnjava kako te djelatnosti same po sebi ne čine kibernetski rat.

4.5. Hibridni rat

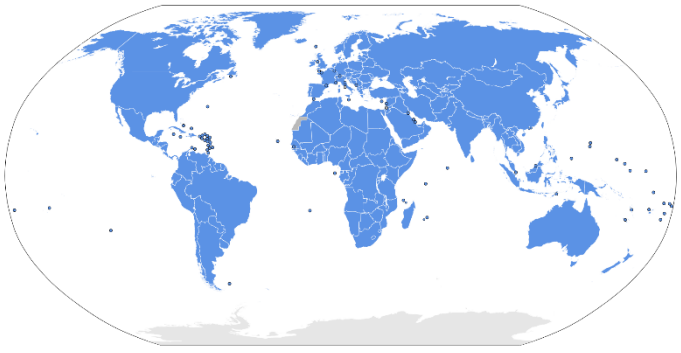
Hibridni rat je novi model ratovanja koji uključuje ekonomske, vojne i obavještajne sile kako bi se postigli određeni gospodarski, politički ili drugi ciljevi. Hibridni rat se može opisati kao veza između kibernetskog i informacijskog ratovanja. Kao glavno sredstvo koriste se informacije odnosno dezinformacije uz pomoć kojih se nastoji naštetiti državnim institucijama. Zaraćane strane mogu ratovati na raznim područjima, primjerice na gospodarskom, diplomskom, kibernetskom, ali isto tako se često koriste i terorizmom i organiziranim kriminalom.

5. MEĐUNARODNA SURADNJA I AKTIVNOSTI

Razvoj informacijske tehnologije, uz svoje prednosti, ima za posljedicu i brojne zlouporabe kibernetskog prostora. Analiza globalne situacije u borbi protiv kibernetskih prijetnji pokazuje sporost u realizaciji nacionalnih pravnih sustava, dok nasuprot raste trend krimimalnog ponašanja u kibernetskom prostoru. Međunarodna suradnja javlja se u obliku specijaliziranih organizacija. U ovom poglavlju navest će se i objasniti specijalizirane organizacije u borbi protiv kibernetskih prijetnji i kibernetskih napada.

5.1. Ujedinjeni narodi

Ujedinjeni narodi su vodeća organizacija na globalnoj međunarodnoj razini. Službena stranica Ministarstva vanjskih i europskih poslova navodi da su "Ujedinjeni narodi međunarodna organizacija čiji su članovi suverene države. Ona je gotovo univerzalna po članstvu, nadležnostima i globalnim ciljevima. Okrenuta je, u prvom redu, očuvanju međunarodnog mira i sigurnosti, razvoju prijateljskih odnosa među državama, promicanju međunarodne suradnje na rješavanju problema ekonomskog, socijalnog, kulturnog i humanitarnog karaktera, uključujući zaštitu ljudskih prava i osnovnih sloboda".[20] Sjedište organizacije je u New Yorku, dok se posebni dijelovi nalaze na lokacijama po cijelom svijetu. Danas ima 193 članice, a Republika Hrvatska je postala članicom 22. svibnja 1992. godine. UN je organizacija koja potiče i predlaže rješavanje problema na globalnoj razini te se stručnjaci nadaju da će poslužiti kao podrška vladama i znanstvenicima za donošenje pravila i uspostavu dogovora kako bi se izbjegli veći sukobi.



Slika 8. Države članice UN-a

Izvor: https://hr.wikipedia.org/wiki/Dr%C5%BEave_%C4%8Dlanice_Ujedinjenih_naroda

[20] Republika Hrvatska, Ministarstvo vanjskih i europskih poslova, URL: http://www.mvep.hr/hr/vanjska-politika/multilateralni-odnosi0/multi-org-inicijative/ujedinjeni-narodi/o-un/ (n.d.)

5.2. INTERPOL

Interpol je međunarodna i najaktivnija organizacija sa sjedištem u Lyonu u Francuskoj. Kako navodi Ministarstvo unutarnjih poslova „Međunarodna organizacija kriminalističkih policija (International criminal police organization ICPO-INTERPOL) osnovana je 1923. godine, a ima 190 država članica. Svrha rada ICPO - INTERPOL-a (u daljnjem tekstu Interpol) omogućavanje je i olakšavanje prekogranične policijske suradnje te pomaganje i potpora svim organizacijama i službama čija je zadaća prevencija i borba protiv kriminaliteta".[21] Jedina je to međunarodna organizacija koja ima sustav međunarodnih tjeralica na globalnoj razini, a Republika Hrvatska je postala članicom u studenom 1992. godine.

Tjeralice i objave se raspisuju bojama i to crvenom tjeralice, a plavom, žutom, zelenom, crnom, ljubičastom i narančastom objave te specijalne objave UN-a i Interpola. Crvene tjeralice se raspisuju za osobama koje se međunarodno potražuju zbog vođenja kaznenog postupka protiv njih ili zbog izdržavanja kazne zatvora, svrha je osobu privremeno uhititi i izručiti državi koja ju potražuje. Plave objave se raspisuju za osobe o kojima je potrebno prikupiti više informacija. Žute objave se raspisuju za nestalim osobama. Zelene objave se raspisuju za osobama koje su počinile kaznena djela u tri ili više država ili kaznena djela koja se tiču tri ili više država. Zelene objave ne mogu biti javno objavljene već je svrha upozoriti policiju i druge agencije za suzbijanje kriminaliteta država članica Interpola na te osobe. Crne objave se raspisuju kod identifikacije neidentificiranih leševa. Kao i zelene, crne se isto ne objavljuju već se uspoređuju s podacima iz žutih objava. Narančaste objave se razlikuju od crvenih na način da se odnose isključivo na predmete, a ne sadrže podatke o počiniteljima. Svrha narančastih objava jest dostavljanje podataka policiji i ostalim službama za borbu protiv kriminaliteta, službama osiguranja u zračnim lukama i slično, te o eksplozivnim napravama i oružju. Ljubičaste objave raspisuju se kako bi upozorili države članice na postupke, uređaje i mjesta kojima se koriste počinitelji.



Slika 9. Povezano trenutno 194 članica Interpola
Izvor: https://www.interpol.int/Who-we-are/What-is-INTERPOL

[21] Republika Hrvatska, Ministarstvo unutarnjih poslova, URL: https://policija.gov.hr/o-ravnateljstvu/ustroj/uprava-kriminalisticke-policije/interpol-422/422 (n.d.)

5.3. EUROPOL

Europol, odnosno Europski policijski ured osnovan je 1992. godine sa sjedištem u Haagu u Nizozemskoj. Europol je agencija EU-a za provedbu zakona u borbi protiv međunarodnih zločina i terorizma. Pomaže članicama u borbi protiv terorizma, trgovine ljudima i novcem, krijumčarenja ukradenim vozilima, organiziranim prijetnjama te sve prisutniji kibernetički kriminal.

5.4. NATO

Prema web stranici Ministarstva vanjskih i europskih poslova "Organizacija Sjevernoatlantskog sporazuma predstavlja savez 29 država iz Sjeverne Amerike i Europe koje su se obvezale da će ispunjavati odrednice Sjevernoatlantskog sporazuma potpisanog u Washingtonu 4. travnja 1949. godine".[22] Republika Hrvatska je u NATO savez ušla 2009. godine. Glavna uloga je osigurati i očuvati mir i sigurnost vojnim i političkim putem. Politički, NATO zagovara suradnju kako bi se izgradilo i održalo povjerenje te izbjegao sukob. Vojno, NATO je usredotočen na mirno rješavanje sporova i konflikata.

Organiziran je kao međudržavna organizacija (svaka država ima svoju samostalnost), obvezao se na obranu zemalja članica u slučaju agresije, nema vlastite operativne oružane snage, već one snage koje mu pružaju članice za potrebe određene misije. Najvažnije tijelo NATO saveza je Sjevernoatlansko vijeće koje se sastoji od veleposlanika, ministara i šefova vlada.

Glavne zadaće su kolektivna obrana, krizno upravljanje i kooperativna sigurnost. Kolektivna obrana odnosi se na uspješno rješavanje eskalacije Hladnog u "vrući" rat, poboljšanje gospodarskog rasta te uživanje u prednostima demokratskog izbora i vladavine prava. Krizno upravljanje odnosi se na sudjelovanje u završetku rata u BiH i implementaciji mirovnog sporazuma, zaustavljanje masovnih ubojstava na Kosovu, sigurnost stanovništva Libije, borbi protiv pomorskog piratstva, podrška migrantskoj krizi, borbi protiv trgovine ljudima te pomoć prilikom prirodnih katastrofa. Kooperativna sigurnost odnosi se na globalnu mrežu koju je NATO razvio za borbu protiv terorizma, kibernetskog ratovanja, piratstva i izradu oružja za masovna uništenja. Globalna mreža sigurnosnih partnera obuhvaća 40 zemalja iz cijelog svijeta te međunarodne organizacije (EU, UN, OESS i Afričku uniju).

NATO savez radi na ostvarenju suradnje s Rusijom, pokušava proširiti suradnju s Ukrajinom i ostalim zemljama partnerima te zemljama Mediteranskog dijaloga i Bliskog Istoka.

[22] Republika Hrvatska, Ministarstvo vanjskih i europskih poslova, URL: http://www.mvep.hr/hr/vanjska-politika/multilateralni-odnosi0/multi-org-inicijative/nato/o-nato-u/ (n.d.)



Slika 10. NATO zastava i države članice

Izvor:https://thestrategybridge.org/the-bridge/2019/4/16/reconsidering-nato-and-us-foreign-policy

5.5. Vijeće Europe

Prema web stranici Ministarstva vanjskih i europskih poslova "Vijeće Europe najstarija je europska organizacija sa sjedištem u Strasbourgu. Obuhvaća 47 država članica (sve europske države osim Bjelarus), a glavni joj je cilj jačanje suradnje i jedinstva na europskom kontinentu, promicanjem ljudskih prava i temeljnih sloboda te demokracije i vladavine prava".[23]

Vijeće obrane se bavi i društvenim temama vezano za socijalnu isključenost, trgovinu ljudima, nasiljem nad ženama, rasnim i nacionalnim netrpljivostima, terorizmom, pravima djece, zaštitom kulture i prirodne baštine i drugim suvremenim problemima europskih država. Uz pomoć politike susjedstva, Vijeće Europe pokušava ojačati politički utjecaj i promicanje europskih vrijednosti izvan Europe. Vijeće Europe je 2001. godine donijelo Konvenciju o kibernetičkom kriminalu. Konvecija je stupila na snagu 1. srpnja 2004. godine i do danas ostaje vodeći međunarodni ugovor o računalnim zločinima. Republika Hrvatska je postala članicom Vijeća Europe 6. studenog 1996. godine te je jedna od prvih država koja je potpisala i ratificirala Konvenciju o kibernetičkom kriminalu.



Slika 11. Članice Vijeća Europe

Izvor: https://www.bljesak.info/vijesti/politika/sramota-ostajemo-jedina-drzava-bez-izaslanstva-u-vijecu-europe/277672

[23] Republika Hrvatska, Ministarstvo vanjskih i europskih poslova, URL: http://www.mvep.hr/hr/vanjska-politika/multilateralni-odnosi0/multi-org-inicijative/vijece-europe/opcenito-o-vijecu-europe/ (n.d.)

5.6. CEPOL

CEPOL je agencija EU koja je posvećena osposobljavanju službenika za provedbu zakona. Cilj CEPOL-a je pomoći u rješavanju Europske i globalne sigurnosti uz pomoć razmjene znanja, prakse i iskustva za izvršavanje zakonodavstva. Sjedište CEPOL-a je u Budimpešti, Mađarska. Izvršni direktor je na čelu koji odgovara Upravnom odboru. Upravni odbor se sastoji od predstavnika država članica EU i Komisije EU. CEPOL omogućuje suradnju i razmjenu znanja između policijskih službenika zemalja EU, okuplja mrežu instituta za osposobljavanje službenika za provedbu zakona u državama članicama EU-a, surađuje s međunarodnim organizacijama, nudi inovativne i napredne aktivnosti obučavanja. Kontakt točka za CEPOL u Republici Hrvatskoj je nacionalna jedinica ustrojena unutar Policijske akademije MUP-a RH u Zagrebu.

5.7. EC3

Europol je identificirao da je EU zbog svoje mrežne infrastrukture ključna meta kibernetičkog kriminala, te je 2013. godine osnovao EC3 odnosno Europski centar za kibernetički kriminal (eng. European Cybercrime Centre). Cilj EC3-a je ojačati reakciju provedbe zakona kibernetičkog kriminala u EU te tako pomoći u zaštiti građana, poduzeća i vlade, ima trostrani pristup u borbi protiv kibernetičkog kriminala (forenzika, strategija i operacije). Tim za forenziku se fokusira na operativnu potporu, istraživanje i razvoj. Tim za strategiju se fokusira na pružanje pomoći i podrške te strategiju i razvoj. Tim za operacije se fokusira na cyber kriminal, internetsko seksualno iskorištavanje djece te prijevare s plaćanjem. EC3 je izravno vezan za napade na računalnu i mrežnu infrastrukturu te online kriminal, odnosno većinu napada kaznenih djela računalnog kriminaliteta (upadi u sustav, phishing, zloporabu kreditnih kartica, krađu identiteta itd.). Kontakt točka EC3 centra u Republici Hrvatskoj je Služba kibernetičke sigurnosti unutar Ravnateljstva policije.

5.8. ENISA

ENISA (eng. European Network and Information Security Agency) je stručni centar za kibernetsku sigurnost u Europi i agencija EU za mrežnu i informacijsku sigurnost. Sjedište agencije je u Heraklionu, Grčka. Pomaže članicama EU u pripremi za sprječavanje, otkrivanje i odgovor na prijetnju informacijske sigurnosti. Glavna skupina ENISA-e jesu organizacije iz javnog sektora (vlade država članica EU-a i institucije EU-a).

Agencija pomaže i javnosti, poslovnoj zajednici, industriji IKT-a, stručnjacima za mrežn i informacijsku sigurnost. ENISA blisko surađuje s Europolom i EC3-om, različitim agencijama EU vezano za problem kibernetske sigurnosti te također savjetuje sve članice EU o korištenju i provedbi Nacionalne kibernetske strategije.



Slika 12. ENISA

Izvor: https://www.enisa.europa.eu/

6. KIBERNETSKA SIGURNOST U REPUBLICI HRVATSKOJ

Kibernetski napadi na globalnoj razini provode se svakodnevno protiv pojedinaca, organizacija i država. Upravo zbog toga analize pokazuju kako Republika Hrvatska i njezini građani mogu postati žrtvom kibernetskih napada. Posljedice kibernetskih napada za građane Republike Hrvatske mogu biti velike. Uloga države je da zaštiti svoje resurse, da usmjeri i upravlja odgovornim akterima u ostvarenju kibernetske sigurnosti svih razina u društvu.

6.1. Kibernetska sigurnost u Republici Hrvatskoj

U Republici Hrvatskoj ne postoji jedinstven sustav borbe protiv kibernetskih prijetnji koji bi djelovao na svim razinama i dijelovima gdje prijetnje postoje, ali postoje sigurnosni sustavi gdje se ubraja i borba protiv kibernetskih prijetnji. Kao primjer navodi se bankarski sektor koji ima vlastite sigurnosne sustave, pa tako i sustave borbi protiv kibernetskih prijetnji. Takvi sustavi se ne oslanjaju na druge sigurnosne sustave. Regulativni okvir sustava borbe protiv kibernetskih prijetnji u Republici Hrvatskoj predstavlja skup propisa koji se svrstaju pod regulativni okvir informacijske sigurnosti, a čije je donošenje u nadležnosti državnog sektora (Vuković, 2012, 21).

Upad u informacijske sustave i mreže je jedan od najučinkovitijih načina prikupljanja velike količine informacija. Pojedine države se koriste provaljivanjem u zaštićene informacijske i komunikacijske sustave drugih zemalja kako bi dobili podatke i informacije o donošenju odluka od tih zemalja. Republika Hrvatska je bila meta takvih pokušaja u kibernetskom prostoru. Namjera napadača je bila prikupiti podatke o političkim, sigurnosnim, gospodarskim i drugim procesima te podatke euroatlanskih agencija. Sigurnosno-obavještajna agencija (SOA) aktivno sudjeluje u otkrivanju i rješavanju takvih napada.

Tijela u Republici Hrvatskoj koja se bore protiv kibernetskih prijetnji 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).

Ured Vijeća za nacionalnu sigurnost (UVNS) je središnje državno tijelo za Republiku Hrvatsku za informacijsku sigurnost. Iz njega proizlaze nacionalne i međunarodne obveze i nadležnosti u području informacijske i kibernetske sigurnosti. UVNS propisuje, koordinira i usklađuje donošenje te isto tako nadzire primjenu mjera i standarda informacijske sigurnosti.

"Zavod za sigurnost informacijskih sustava (ZSIS) središnje je državno tijelo za obavljanje poslova u tehničkim područjima informacijske sigurnosti državnih tijela Republike Hrvatske, koji obuhvaćaju standarde sigurnosti informacijskih sustava, sigurnosnu akreditaciju informacijskih sustava, upravljanje kriptomaterijalima koji se koriste u razmjeni klasificiranih podataka te koordinaciju prevencije i odgovora na računalne ugroze sigurnosti informacijskih sustava".[24] ZSIS je nadležan za aktivnosti vezane za upravljanje kriptomaterijalima koji se koriste u razmjeni klasificiranih podataka između državnih tijela, stanih tijela i organizacija, za sigurnost informacijskih sustava državnih tijela te za poslove istraživanja i razvoja tehnologija za zaštitu klasificiranih podataka. ZSIS je zadužen i za reguliranje standarda tehničkih područja sigurnosti informacijskih sustava u Republici Hrvatskoj, njihovo usklađivanje te sudjelovanje u nacionalnoj normizaciji područja sigurnosti informacijskih sustava.

Nacionalni CERT (nCERT) je osnovan s ciljem prevencije i zaštite u Republici Hrvatskoj od računalnih prijetnji sigurnosti javnih informacijskih sustava. Nacionalni CERT provodi proaktivne i reaktivne mjere. Proaktivnim mjerama djeluje se prije incidenta koji mogu prijetiti sigurnosti informacijskih sustava, cilj je sprječavanje mogućih šteta. Reaktivnim mjerama se djeluje na incidente u Republici Hrvatskoj i incidente koji mogu ugroziti računalnu sigurnost javnih informacijskih sustava u Republici Hrvatskoj.

Odjel za visokotehnički kriminalitet je ustrojen unutar Službe gospodarskog kriminaliteta i korupcije Uprave kriminalističke policije Ministarstva unutarnjih poslova Republike Hrvatske. Odjel analizira, prati i predlaže rješenja za podizanje učinkovitosti rada u suzbijanju kibernetskog kriminala. Ovaj odjel je središnja jedinica za postupanje po kaznenim djelima iz Konvencije o kibernetičkom kriminalu i Protokolu uz Konvenciju.

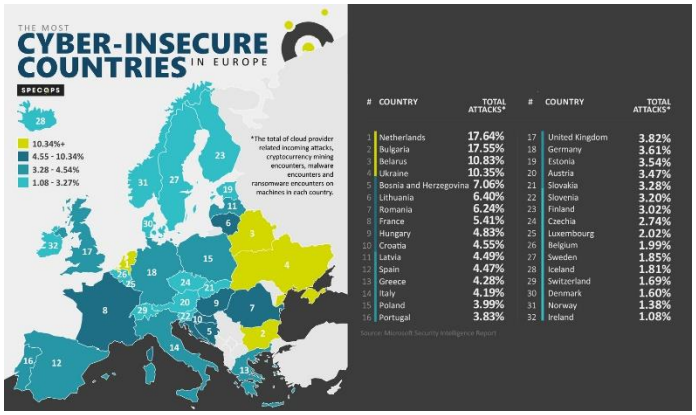
Centar za sigurnosnu suradnju RACVIAC je regionalno središte za kibernetsku sigurnost regija Jugoistočne Europe. Cilj osnivanja je dovesti do povećanja sigurnosne suradnje u regiji Jugoistočne Europe, a najznačajnija dobit je unaprjeđenje sposobnosti stručnjaka iz kibernetske sigurnosti da brže i bolje odgovore prijetnjama u kibernetskom prostoru, da ih riješe ili umanje njihovu razornost.

[24] Republika Hrvatska, Zavod za sigurnost informacijskih sustava, URL: https://www.zsis.hr/default.aspx?id=13 (n.d.)

Agencija za zaštitu osobnih podataka (AZOP) je pravna osoba s javnim ovlastima. Osnovana je Zakonom o zaštiti osobnih podataka te samostalno i neovisno djeluje o izvršnoj i zakonodavnoj vlasti. Misija AZOP-a je izvršavanje nadzora nad provođenjem propisa o zaštiti osobnih podataka i ostvarivanje tog prava svakoj osobi u Republici Hrvatskoj te predlaganje mjera za poboljšanje zaštite osobnih podataka.

6.2. Kibernetski napadi u Republici Hrvatskoj

Prema podacima koje je napravila kompanija Specops Software, Republika Hrvatska se našla na desetom mjestu sa 4,55 posto rizika za kibernetske prijetnje odnosno prijetnja kibernetskih napada.



Slika 13. Cyber-insecure countries

Izvor: https://www.itpro.co.uk/security/cyber-security/354818/uk-among-countries-most-likely-to-encounter-cloud-attacks

Neki od najpoznatijih kibernetskih napada u Republici Hrvatskoj su:

a) Napad na naftnu kompaniju INA-u
b) Ransomware
c) Napad na internet bankarstvo
d) SOA.

a) Napad na naftnu kompaniju INA-u dogodio se u veljači ove godine. Hakeri su napali računalnu mrežu kompanije te izazvali probleme u plaćanju računa te izdavanju bonova i vinjeta. Slučaj je prijavljen nadležnim institucijama, a pomoć su ponudili i stručnjaci iz SAD-a. INA je naknadno objavila da napad nije ugrozio poslovanje kompanije, prodaja goriva je kontinuirana, opskrba tržišta neprekidna te plaćanja (gotovina, INA kartice ili bankovne kartice) su sigurna.

b) "Ransomware je vrsta trojanaca/zlonamjernog programa koji šifrira podatke korisnika te zahtjeva uplatu otkupnine u slučaju da korisnik želi ponovni pristup svojim podacima. Ostali nazivi za ransomware su ucjenjivački trojanci, ransom trojanci, trojanci ili kripto enkripcijski trojanci".[25] Ransomware je stvarao Hrvatima najviše problema. Prema istraživanju koje je provela kompanija za cyber sigurnost, Kaspersky Lab (2016), Republika Hrvatska je bila druga u svijetu po postotku zaraženih računala, odmah iz Japana. Prema njihovom istaživanju napadnuto je 3,71 posto korisnika koji su barem jednom doživjeli ransomware napad. Hakeri koji upravljaju ransomwareom od korisnika traže da plati otkupninu u virtualnoj valuti Bitcoin kako bi dobio ključ za dešifriranje podataka.

c) Napad na internet bankarstvo se dogodio 2014. godine gdje su nepoznati hakeri ubacivali zloćudne programe poput virusa i trojanca na računala korisnika sa ciljem dolaska do osobnih i povjerljivih podataka te lozinkama koje su korisnici koristili za pristup internet bankarstvu. Prema izvješću Hrvatske narodne banke, hakeri su uspješno oštetili žrtve i ukrali 1,8 milijuna kuna.

d) SOA se je bila jedna od meta napada hakera kada su hakeri ukrali 400 GB elektroničke pošte iz tvrtke Hacking Team iz Milana, Italije, koja prodaje softver za prisluškivanje komunikacija. Među elektroničkom poštom pronađeno je da je naša Sigurnosno-obavještajna agencija (SOA) htjela kupiti softvere za nadgledanje komunikacije između korisnika WhatsAppa, Vibera i Skype-a.

6.3. Nacionalna strategija kibernetičke sigurnosti

Nacionalna strategija kibernetičke sigurnosti donesena je 07. listopada 2015. godine. Primarni cilj je prepoznati organizacijske probleme u njezinoj provedbi, te širenje važnosti problema kibernetskih prijetnji u društvu.

Svrha je kontinuirano provoditi aktivnosti koje su potrebne za razvoj i podizanje sposobnosti Republike Hrvatske na području cyber sigurnosti i izgradnja sigurnog društva u kibernetskom prostoru, dok je glavna uloga povezivanje ove problematike u različitim sektorima društva te tijelima i pravnim osobama koji imaju različite potrebe i interese.

Kao osnovna načela pristupu kibernetičke sigurnosti, Nacionalna strategija kibernetičke sigurnosti vidi:

- Sveobuhvatnost
- Integracija
- Proaktivni pristup

[25] Anti-botnet, URL: http://www.antibot.hr/ransomware/info.html (n.d.)

- Jačanje otpornosti, pouzdanosti i prilagodljivosti
- Primjena zakona
- Razvoj usklađenog zakonodavnog okvira
- Primjena načela supsidijarnosti
- Primjena načela proporcionalnosti (Vlada RH, 2015: 6).

Kao opće ciljeve strategije, Nacionalna strategija kibernetičke sigurnosti vidi:

1. Sustavni pristup u primjeni i razvoju nacionalnog zakonodavnog okvira
2. Provođenje aktivnosti i mjera u svrhu povećanja sigurnosti, otpornosti i pouzdanosti kibernetičkog prostora
3. Uspostavljanje učinkovitijeg mehanizma razmjene, ustupanja i pristupa podacima
4. Jačanje svijesti o sigurnosti
5. Poticanje razvoja usklađenih obrazovnih program
6. Poticanje razvoja e-usluga
7. Poticanje istraživanja i razvoja
8. Sustavni pristup međunarodnoj suradnji (Vlada RH, 2015: 7).

7. ZAKLJUČAK

U ovom završnom radu detaljnije se obradila i analizirala opća teorija IS-a, kibernetike, njezine prijetnje te prevencije odnosno odgovore na prijetnje kibernetskoj sigurnosti.

Za uspješan rad poslovnog sustava potrebne su točne informacije koje su dostupne u pravo vrijeme. Svaki IS je dio poslovnog sustava koji prikuplja, obrađuje, pohranjuje, čuva i isporučuje informacije važne za organizaciju. Kako bi informacija bila korisna ona mora imati aspekte integriteta, povjerljivosti i dostupnosti. IS je siguran kada se zadovolje navedena tri aspekta.

S druge strane, kibernetika kao znanstvena disciplina utječe na razvoj mnogih područja znanosti koji dovode do novog pristupa analizi te razvijanja ideje. Ona nudi mogućnost za uspješno rješavanje problema. Kao znanost bavi se općim pitanjima, a ne kako sustav funkcionira. S obzirom da se sustavi razlikuju, razlikuje se i način upravljanja, upravo zbog toga su nastali derivati kibernetike koji pokušavaju objasniti načine upravljanja pojedinim sustavom. Kibernetski prostor, iako virtualan, postaje realna stvarnost u kojoj često dolazi do manipulacije podataka.

Najznačajnije specifičnosti kibernetskih prijetnji je kibernetski prostor te tehnologija koja olakšava provedbu kaznenih djela. Kibernetski napadi su jedna od najvećih prijetnji koji uz pomoć tehnologije sve više rastu, a dijele se na kibernetski kriminal, kibernetsku špijunažu, kibernetski terorizam, kibernetski rat te hibridni rat. Kibernetski kriminal su kaznena djela poput prijevara na području internet bankarstva, odnosno sva djela kod kojih je upotreba računala ključna za napad. Kibernetska špijunaža je odavanje tajni ili povjerljivih podataka pomoću špijunskih programa. Nadalje, za kibernetski terorizam se može reći da su to planirani napadi na računalne sustave od strane nacionalnih skupina, dok je kibernetski rat, rat koji se poduzima od strane država, a vodi se protiv drugih država sa ciljem uništavanja njihove upotrebe. Novi oblik ratovanja je hibridni rat čiji je cilj postići gospodarski, politički i slični cilj.

Borba protiv navedenih kibernetskih prijetnji javlja se u obliku međunarodne suradnje specijaliziranih organizacija. Kao odgovor na konstantna ugrožavanja sigurnosti, Konvencija o kibernetičkom kriminalu koju je donijelo Vijeće Europe, je dobar temelj za uspostavu učinkovite borbe kibernetskog kriminala, ali i općenito kibernetskih prijetnji. Hrvatska prati sve Direktive, Uredbe i smjernice EU, te je potpisala i ratificirala navedenu Konvenciju. Osim toga osnovala je i institucije za osiguranje sigurnosti informacija. To su Nacionalni CERT sa ciljem prevencije i zaštite od računalnih prijetnji u Republici Hrvatskoj, Zavod za sigurnost informacijskih sustava koje je glavno tijelo za tehnička područja sigurnosti, Odjel za visokotehnički kriminalitet za suzbijanje kibernetskog kriminala, Ured Vijeća za nacionalnu sigurnost kao središnje tijelo za informacijsku sigurnost u Republici Hrvatskoj, Agencija za zaštitu osobnih podatak koja se bavi zaštitom podataka građana Republike Hrvatske te Centar za sigurnosnu suradnju RACVIAC kao regionalno središte za kibernetsku sigurnost regija Jugoistočne Europe.

Cilj završnog rada bio je pokazati važnost informacije u poslovnom sustavu, o njezinoj kvaliteti, dostupnosti, integritetu i pravovaljanosti za organizaciju, isto tako prikazati prijetnje i radnje koje ugrožavaju sigurnost računala. Kao zaljučak može se reći kako poduzeće odnosno organizacija mora težiti konstantnom ulaganju i unaprjeđivanju svojih sigurnosnih sustava, ali i ulaganja u znanje i obrazovanje svojih zaposlenika, kako bi u budućnosti mogla predvidjeti, sprječiti ili obraniti se od kibernetskih napada.

8. IZJAVA

Izjava o autorstvu završnog rada i akademskoj čestitosti

Ime i prezime studenta:	**Maja Hercigonja**
Matični broj studenta:	**6-215/17-ITR**
Naslov rada:	**KIBERNETSKA SIGURNOST**

Pod punom odgovornošću potvrđujem da je ovo moj autorski rad čiji niti jedan dio nije nastao kopiranjem ili plagiranjem tuđeg sadržaja. Prilikom izrade rada koristio sam tuđe materijale navedene u popisu literature, ali nisam kopirao niti jedan njihov dio, osim citata za koje sam naveo autora i izvor te ih jasno označio znakovima navodnika. U slučaju da se u bilo kojem trenutku dokaže suprotno, spreman sam snositi sve posljedice uključivo i poništenje javne isprave stečene dijelom i na temelju ovoga rada.

Potvrđujem da je elektronička verzija rada identična onoj tiskanoj te da je to verzija rada koju je odobrio mentor.

Datum	Potpis studenta
28.03.2020.	Maja Hercigonja

9. POPIS LITERATURE

9.1. Knjige i članci

1. Antoliš, K. (2010). Internetska forenzika i cyber terorizam. Policija i sigurnost, 19 (1), 121-128.
2. Bača, M. i Ćosić, J. (2013). Prevencija računalnog kriminaliteta. Policija i sigurnost, 22 (1), 146-158.
3. Čerić, V. i Varga, M. (2004). Informacijska tehnologija u poslovanju. Zagreb: Element
4. Frančula, N. (2015). Kibernetička kartografija. Geodetski list : glasilo Hrvatskoga geodetskog društva, 69 (92) 2; 144-144
5. Hlača, S. (2018). KIBERNETIČKA SIGURNOST U HRVATSKIM MEDIJIMA. Polemos, XXI (42), 167-185.
6. Panian, Ž. (2001). Poslovna informatika (Koncepti, metode i tehnologija). Zagreb: POTECON
7. Panian, Ž. i Strugar, I. (2013). Informatizacija poslovanja. Zagreb: Ekonomski fakultet
8. Popović, P. (2013). Anarhija na petom bojnom polju: kibernetski prostor i međunarodni odnosi. Politička misao, 50 (4), 48-72.
9. Veresha, R. (2018). PREVENTIVE MEASURES AGAINST COMPUTER RELATED CRIMES: APPROACHING AN INDIVIDUAL. Informatologia, 51 (3-4), 189-199.
10. Vojković, G. i Štambuk-Sunjić, M. (2006). Konvencija o kibernetičkom kriminalu i kazneni zakon Republike Hrvatske. Zbornik radova Pravnog fakulteta u Splitu, 43 (1), 123-136.
11. Vuković, H. (2012). Kibernetska sigurnost i sustav borbe protiv kibernetskih prijetnji u Republici Hrvatskoj. National security and the future, 13 (3), 12-31

9.2. Internetski izvori

1. Anti-botnet, Nacionalni centar podrške. (n.d.). Informacije. Preuzeto s **http://www.antibot.hr/ransomware/info.html**
2. Azop. (n.d.). Djelatnost i unutarnje ustrojstvo agencije. Preuzeto s https://azop.hr/djelatnost-agencije
3. Cepol. (n.d.). CEPOL: misija, vizija i vrijednosti. Preuzeto s https://www.cepol.europa.eu/hr
4. CERT.hr. (n.d.). O nacionalnom CERT-u. Preuzeto s https://www.cert.hr/onama/
5. Ekonomski fakultet, Osijek. (n.d.). Poslovni Informacijski sustavi. Preuzeto s http://www.efos.unios.hr/poslovni-informacijski-sustavi/wp-content/uploads/sites/216/2013/04/1.-POSLOVNI-INFORMACIJSKI-SUSTAVI.pdf

6. Europol. (n.d.). O EUROPOLU. Preuzeto s https://www.europol.europa.eu/hr/about-europol
7. Europol. (n.d.). Europski centar za kibernetički kriminal–EC3. Preuzeto s https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3
8. Europska unija. (n.d.). Agencija Europske unije za kibersigurnost (ENISA). Preuzeto s https://europa.eu/european-union/about-eu/agencies/enisa_hr
9. Fakultet prometnih znanosti. (n.d.). Informacijski sustavi mrežnih operatera. Preuzeto s https://www.weboteka.net/fpz/Informacijski%20sustavi%20mre%C5%BEnih%20operatera/04_-_Podjele_vrste_i_elementi_informacijskih_sustava.pdf
10. Fakultet prometnih znanosti. (n.d.). O kibernetici. Preuzeto s https://www.fpz.unizg.hr/ztos/AUTOM/2autom-uvod_u_kibern.pdf
11. Fakultet prometnih znanosti. (n.d.). Uvod u informacijske sustave Preuzeto s https://www.fpz.unizg.hr/ztos/iszp/a2.pdf
12. Hrvatski leksikon. (n.d.). Kibernetika značenje. Preuzeto s https://www.hrleksikon.info/definicija/kibernetika.html
13. Leksikografski zavod Miroslav Krleža (n.d.). Kibernetika. Preuzeto s http://enciklopedija.lzmk.hr/clanak.aspx?id=18859
14. Prom web portal. (n.d.). Hrvatska druga u svijetu po ransomware napadima. Preuzeto s https://www.fpz.unizg.hr/prom/?p=5341
15. Republika Hrvatska, Ministarstvo unutarnjih poslova, Ravnateljstvo policije. (n.d.). Interpol. Preuzeto s https://policija.gov.hr/o-ravnateljstvu/ustroj/uprava-kriminalisticke-policije/interpol-422/422
16. Republika Hrvatska, Ministarstvo vanjskih i europskih poslova. (n.d.). Općenito o Vijeću Europe. Preuzeto s http://www.mvep.hr/hr/vanjska-politika/multilateralni-odnosi0/multi-org-inicijative/vijece-europe/opcenito-o-vijecu-europe/
17. Republika Hrvatska, Ministarstvo vanjskih i europskih poslova. (n.d.). O NATO-u. Preuzeto s http://www.mvep.hr/hr/vanjska-politika/multilateralni-odnosi0/multi-org-inicijative/nato/o-nato-u/
18. Republika Hrvatska, Ministarstvo vanjskih i europskih poslova. (n.d.). O Ujedinjenim narodima. Preuzeto s http://www.mvep.hr/hr/vanjska-politika/multilateralni-odnosi0/multi-org-inicijative/ujedinjeni-narodi/o-un/
19. Republika Hrvatska, Sigurnosno-obavještajna agencija. (n.d.). Kibernetička sigurnost. Preuzeto s https://www.soa.hr/hr/podrucja-rada/kiberneticka-sigurnost/
20. Republika Hrvatska, Ured vijeća za nacionalnu sigurnost. (n.d.). Uvodna riječ. Preuzeto s https://www.uvns.hr/hr/o-nama/uvodna-rijec
21. Republika Hrvatska, Ured Vijeća za nacionalnu sigurnost. (n.d.). Što je to informacijska sigurnost. Preuzeto s https://www.uvns.hr/hr/sto-je-to-informacijska-sigurnost

22. Republika Hrvatska, Zavod za sigurnost informacijskih sustava. (n.d.). O nama. Preuzeto s https://www.zsis.hr/default.aspx?id=13
23. Sveučilište Josipa Jurja Strossmayera u Osijeku, Građevinski fakultet Osijek. (n.d.). Kibernetika - što je to. Preuzeto s https://repozitorij.gradst.unist.hr/islandora/object/gradst%3A981/datastream/FILE0/view
24. Veleučilište u Rijeci. (n.d.): Sigurnost informacijskih sustava-skripta. Preuzeto s https://www.veleri.hr/files/datotekep/nastavni_materijali/k_sigurnost_s2/Sigurnost_informacijskih_Vukelic.pdf
25. Vlada RH. (7.10.2015.). Nacionalna strategija kibernetičke sigurnosti. Preuzeto s https://www.uvns.hr/UserDocsImages/dokumenti/Nacionalna%20strategija%20kibernetickе%20sigurnosti%20(2015.).pdf

9.3. Završni radovi, diplomski radovi

1. Botonjić, A. (2015). Unified modeling language (UML): Use case diagram. Završni rad. Pula: Fakultet ekonomije i turizma, Informatika
2. Bukovac, T. (2016). Sigurnost informacijskih sustava. Diplomski rad. Zagreb: Filozofski fakultet, Informacijske znanosti – Istraživačka informatika
3. Hlača. S. (2018). Kibernetička sigurnost u hrvatskim medijima: između normativnog i empirijskog. Diplomski rad. Zagreb: Filozofski fakultet, Odsjek za sociologiju
4. Kezerić, A-M. (2017). Analiza prijetnji i rizika cyber sigurnosti Republike Hrvatske: ranjivost informacijske infrastructure. Diplomski rad. Zagreb: Fakultet političkih znanosti, Novinarstvo
5. Malčić, A. (2018). Analiza i modeliranje informacijskog sustava. Završni rad. Šibenik: Veleučilište u Šibeniku, Informatički menadžment
6. Mikulin, R. (2019). Kaznenopravna zaštita od kibernetičkog kriminala i uloga davatelja telekom usluga. Diplomski rad. Zagreb: Fakultet prometnih znanosti

7. Nikolić, T. (2017). Cyber prijetnje u zračnom prometu. Završni rad. Zagreb: Fakultet prometnih znanosti
8. Profozić, M. (2018). Informacijska sigurnost u poslovanju. Završni rad. Karlovac: Veleučilište u Karlovcu, Poslovno upravljanje
9. Protrka, N. (2018). Međunarodna suradnja i sigurnost u suzbijanju kriminaliteta u kibernetičkom prostoru. Doktorski rad. Zadar: Sveučilište u Zadru, Međunarodni odnosi
10. Rakonić, I. (2019). Kaznenopravni aspekti kibernetičkog ratovanja. Diplomski rad. Zagreb: Pravni fakultet
11. Sić, M. (2017). Računalna forenzika. Seminarski rad. Zagreb: Sveučilište u Zagrebu, Fakultet elektronike i računarstva
12. Šimić, D. (2017). Sistemski pristup. Diplomski rad. Split: Pomorski fakultet
13. Tomić, M. (2019). Cyber kriminalitet – novo područje za socijalnopedagoške intervencije. Diplomski rad. Zagreb: Edukacijsko-rehabilitacijski fakultet
14. Ugren, V. (2012). Cyber kriminal. Master rad. Beograd: Univerzitet Singidunum, Departman za postdiplomske studije i međunarodnu saradnju

10. POPIS SLIKA

Slika 1. Informacijski sustav 5
Slika 2. Elementi informacijskog sustava 6
Slika 3. Slojevi informacijskog sustava 7
Slika 4. Strukturna razina informacijskog sustava 8
Slika 5. Sigurnosni trokut 10
Slika 6. Shema regulacijskog kruga 15
Slika 7. Zemlje koje su bile mete napada špijunaže 18
Slika 8. Države članice UN-a 21
Slika 9. Povezano trenutno 194 članica Interpola 22
Slika 10. NATO zastava i države članice 24
Slika 11. Članice Vijeća Europe 24
Slika 12. ENISA 26
Slika 13. Cyber-insecure countries 29

ŽIVOTOPIS

europass Životopis

OSOBNE INFORMACIJE Maja Hercigonja

Augusta Šenoe 3, 49290 Klanjec (Hrvatska)
0989557898
majah9973@gmail.com

OSOBNI PROFIL Studentica smjera Informacijske tehnologije

RADNO ISKUSTVO

02. svibnja 2019.–30. kolovoza 2019.
Administrativni asistent / administrativna asistentica
Ministarstvo unutarnjih poslova RH, Zabok (Hrvatska)
- odnosi s kupcima
- administrativni poslovi
- arhiviranje dokumenata

24. listopada 2017.–25. veljače 2018.
Anketar/anketarka za istraživanje tržišta
IPSOS d.o.o., Split (Hrvatska)
- telefonsko anketiranje

OBRAZOVANJE I OSPOSOBLJAVANJE

02. listopada 2017.–danas
Student - Informacijske tehnologije
Veleučilište Baltazar Zaprešić, Zaprešić (Hrvatska)

10. rujna 2013.–15. lipnja 2017.
Komercijalist
Srednja škola Zabok, Zabok (Hrvatska)

OSOBNE VJEŠTINE

Materinski jezik: hrvatski

Strani jezici

	RAZUMIJEVANJE		GOVOR		PISANJE
	Slušanje	Čitanje	Govorna interakcija	Govorna produkcija	
engleski	C1	C1	C1	C1	C1
talijanski	B1	B1	B1	B1	B1

Stupnjevi: A1 i A2: Početnik - B1 i B2: Samostalni korisnik - C1 i C2: Iskusni korisnik
Zajednički europski referentni okvir za jezike - Ljestvica za samoprocjenu

Komunikacijske vještine: Dobre komunikacijske vještine prilikom rada u timu te sklonost timskom i suradničkom radu i učenju

Digitalne vještine

SAMOPROCJENA				
Obrada informacija	Komunikacija	Stvaranje sadržaja	Sigurnost	Rješavanje problema

europass Životopis Maja Hercigonja

Samostalni korisnik	Samostalni korisnik	Samostalni korisnik	Samostalni korisnik	Samostalni korisnik

Digitalne vještine - Tablica za samoprocjenu

- vješto upravljanje Office alatima
- dobro znanje kod kreiranja web stranica (HTML/CSS)
- vještine izrada baza podataka (SQL, Acess)
- osnovno znanje programiranja u JAVA programskom jeziku