# Sigurnost informacija u domeni pomorstva

**Radmilo, Ivana**





**SVEUČILIŠTE U SPLITU**

**POMORSKI FAKULTET**

**IVANA RADMILO**

# SIGURNOST INFORMACIJA U DOMENI POMORSTVA

**DIPLOMSKI RAD**

**SPLIT, 2016.**

Split, 22.9.2016.

Zavod/studij: POMORSKI FAKULTET, POMORSKI MENADŽMENT

Predmet: RAČUNALNE MREŽE

## *D I P L O M S K I  ZADATAK*

Student/ca: IVANA RADMILO
Matični broj: 0171246999
Zavod/studij: POMORSKI MENADŽMENT

**ZADATAK:**
Diplomski rad na temu „Sigurnost informacija u domeni pomorstva“

**OPIS ZADATKA:**
Istraživanje provedeno anketiranjem unutar različitih sustava pomorstva. Ispitivana su ponašanja i običaji vezani za sustave informacija i informacijske sigurnosti. Rezultati prikupljeni na uzorku od 20 ispitanika (tvrtki, agencija i slično).

**CILJ:**
Cilj istraživanja je ukazati na problematiku unutar informacijskog svijeta i pomorskog sektora kao kritičnog kada se radi o protoku informacija i njihovom presretanju od strane napadača. Također je cilj i ukazati na needuciranost kadra zaposlenog u pomorskim sustavima, njihova nedovoljna informiranost u pogledu cyber kriminala i nedovoljna ulaganja u načine zaštite informacijskih sustava (još uvijek se koriste oni primitivni i već po malo zastarjeli načini zaštite).

**Zadatak uručen studentu/ci:** IVANA RADMILO

**Potpis studenta/ce:** _____

**Mentor:** dr. sc. Anita Gudelj

**SVEUČILIŠTE U SPLITU**

**POMORSKI FAKULTET**

**STUDIJ: POMORSKI MENADŽMENT**

# SIGURNOST INFORMACIJA U DOMENI POMORSTVA

**DIPLOMSKI RAD**

**MENTOR:** **STUDENT:**

**dr. sc. Anita Gudelj** **Ivana Radmilo**

**SPLIT, 2016.**

*„ Najgore je vjerovati da imaš sigurnost,*
*a ne poduzimati ništa da je zadržiš “*

# SAŽETAK

Informacijski sustavi i sustavi informacijske sigurnosti u okviru pomorstva dio su kritične infrastrukture kada je riječ o mogućnosti napada ili prijetnji. Kako bi se stvorila svijest o pomorskom sektoru kao meti neželjenih događaja, potrebno je educiranje već postojećeg kadra i onog koji tek treba doći. Trenutno stanje što se informiranosti, educiranosti i postupanja u određenim situacijama tiče daleko je od zavidne razine, tj., od razine ostalih država članica Europske Unije. Takav zaključak temelji se na relevantnim podatcima koji su prikupljeni za izradu diplomskog rada anketiranjem različitih sektora poslovanja unutar sustava pomorstva. Svi podatci prikupljeni su anonimno, a odnose se na sektor agencija za zapošljavanje pomoraca, charter agencije, malih brodogradilišta i škverova, proizvodnje, servisa brodova i brodske opreme, sektor uslužnih djelatnosti (lučka uprava) i to na uzorku od 20 ispitanika. Na temelju provedenog istraživanja, zaključuje se kako sigurnost i zaštita informacijskih sustava unutar sustava pomorstva još uvijek uvelike odskače od europskog i svjetskog prosjeka te kako su promjene nužne i to u što kraćem mogućem roku.



**Ključne riječi:** informacija, informacijski sustavi, pomorski sustavi, sigurnost, zaštita



# ABSTRACT

Information systems and information security systems within maritime affairs are a part of a critical infrastructure when it comes to the possibility of attacks or threats. In order to develop awareness of the maritime sector being a target of adverse events, it is necessary to educate the existing staff and those that are yet to become a part of it. Current situation regarding awareness, education and actions in certain situations is far from an enviable level, i.e. from the level in other Member States of the European Union. This conclusion is based on the relevant data collected for the purpose of writing this thesis by interviewing various business sectors within the maritime affairs sector. All data were collected anonymously from a sample comprising 20 respondents, and refer to the sector of agencies for placement of seamen, charter agencies, smaller and bigger shipyards, manufacturing, ship and ship equipment repairing , the service sector (port authority). Based on the conducted research, it can be concluded that the safety and security of information systems within the maritime affairs sector still greatly deviate from the European and global average, as well as that changes need to be introduced as soon as possible.



**Key words:** information, information systems, maritime systems, security, protection

# SADRŽAJ


**1. UVOD ..... 1**

**1.1. PROBLEM, PREDMET I OBJEKT ISTRAŽIVANJA ..... 2**

**1.2. RADNA HIPOTEZA ..... 2**

**1.3. SVRHA I CILJEVI ISTRAŽIVANJA ..... 3**

**1.4. ZNANSTVENE METODE ..... 3**

**1.5. STRUKTURA RADA ..... 3**

**2. INFORMACIJSKA SIGURNOST I SIGURNOST INFORMACIJSKIH SUSTAVA ..... 5**

**2.1. DEFINICIJA SIGURNOSTI INFORMACIJA I INFORMACIJSKIH SUSTAVA ..... 6**

**2.2. PRIJETNJE INFORMACIJSKOJ SIGURNOSTI ..... 7**

2.2.1. Vrste prijetnji ..... 7

2.2.2. Kategorije prijetnji ..... 7

**3. RAČUNALNE MREŽE KAO DIO INFORMACIJSKIH SUSTAVA ..... 9**

**3.1. RAČUNALNA MREŽA BRODA ..... 9**

**3.2. PODJELA RAČUNALNIH MREŽA ..... 9**

**4. ZAŠTITA RAČUNALNIH MREŽA ..... 12**

**4.1. VRSTE ZAŠTITE RAČUNALNE MREŽE ..... 12**

4.1.1. Antivirus ..... 12

4.1.2. Vatrozid ..... 12

4.1.3. Lozinke – *Password* ..... 13

4.1.4. Sigurnosni protokoli ..... 14

4.1.5. Fizička zaštita ..... 14

4.1.6. WPA/WPA2 ..... 15

**5. RANJIVOST POMORSKIH INFORMACIJSKIH SUSTAVA ..... 21**

**5.1. GMDSS – GLOBAL MARITIME DISTRESS AND SAFETY SYSTEM ..... 21**

**5.2. MSSIS – MARITIME SAFETY AND SECURITY INFORMATION SYSTEM 21**

**5.3. AIS - AUTOMATIC IDENTIFICATION SYSTEM ..... 22**

5.3.1. GPS „najslabija karika“ AIS sustava ..... 25

5.3.2. Napadi na AIS sustave ..... 26

5.3.3. Otvorena komunikacija uz pomoć AIS sustava ..... 27

**5.4. SAFESEANET ..... 28**

5.4.1. Opći koncept elektroničkih ..... 28

5.4.2. Upravljanje, način rada i održavanje ..... 29

5.4.2.3. Razmjena i dijeljenje podataka ..... 30

**6. ANALIZA *CYBER* SIGURNOSTI U POMORSKOM SEKTORU ..... 32**

**6.1. ENISA ..... 32**

**6.2. POMORSKI SEKTOR KAO KRITIČNA INFRASTRUKTURA ..... 32**

**6.3. KONTEKST POLITIKE U SLUČAJEVIMA KRITIČNE INFORMACIJSKE INFRASTRUKTURE ..... 33**

**6.4. NISKA SVIJEST I FOKUS NA POMORSKU CYBER SIGURNOST ..... 34**

**6.5. SLOŽENOST POMORSKOG ICT OKRUŽENJA ..... 35**

**6.6. PREPORUKE KAKO SPRIJEČITI MOGUĆE NAPADE ..... 36**

6.6.1. Globalna razina ICT okruženja ..... 37

6.6.2. Preporuke za djelovanje na globalnoj razini ..... 37

6.6.3. Poveznica između nacionalnog i regionalnog ICT okruženja ..... 38

**6.7. NEDOVOLJNA POSVEĆENOST CYBER SIGURNOSTI UNUTAR POMORSKIH REGULATIVA ..... 39**

**7. SVIJEST O POMORSKOM DOBRU U OKVIRU INFORMACIJSKE SIGURNOSTI ..... 40**

**7.1. SIGURNOST INFORMACIJA U OKVIRU NATO-A ZA POMORSKO OKRUŽENJE ..... 40**

**8. PROVEDENO ISTRAŽIVANJA SIGURNOSTI INFORMACIJA UNUTAR POMORSKIH SUSTAVA ..... 43**

**8.1. ANALIZA ANKETE ..... 43**

8.2. ANALIZA REZULTATA ..... 49
9. ZAKLJUČAK ..... 58
LITERATURA ..... 59
POPIS SLIKA ..... 61
POPIS TABLICA ..... 62
POPIS GRAFIKONA ..... 63
POPIS KRATICA ..... 64
PRIMJER ANKETE ..... 65

# 1. UVOD

Današnje, moderno doba od čovjeka zahtjeva da sve aktivnosti prepusti strojevima i da se oslanja na njihovu preciznost i učinkovitost prilikom obavljanja velikog broja zadataka. Bez obzira na to što su strojevi uglavnom ispravni u radu i gotovo uopće nisu skloni greškama, njihovo ponašanje moguće je predvidjeti. Predviđanjem radnji strojeva dolazi do mogućnosti vrlo lake manipulacije. Upravo zbog toga, moderna tehnologija postaje izrazito ranjiva i metom različitih oblika napada.

Uporaba računalnih tehnologija zadnjih desetljeća dovela je do toga da je gotova sva komunikacija i automatizacija na brodovima uznapredovala do razine da se njima može upravljati i nadzirati s kopna. Napredovanjem u razvoju satelitskih komunikacija došlo je do usavršavanja i na sustavima koji služe za pozicioniranje brodova.

U trenutku kada je potrebna procjena sigurnosti ili donošenja odluka, ukoliko se radi o mogućim rizicima, prepuštena je zapovjedniku broda koji se sve više oslanja na računalne sustave. U slučaju da se dogodi proboj unutar računalnog sustava, tencijalni napadač u mogućnosti je da preuzme brod na način da upravlja svim njegovim vitalnim sustavima. Kod ovakve mogućnosti ugroze sigurnosti broda, dolazi do nestabilnosti cjelokupnog pomorskog sustava, koji bi za posljedice mogao imati nesreće na moru, gubitak flote i gubitak ljudskih života, onečišćenje, financijske gubitke (kako brodske kompanije, tako i svega vezanog za pomorski sektor), otmice od strane pirata, itd.

Imajući u vidu kako pomorski promet nije samo vezan za nacionalne granice, već se on proteže i na regionalnu i globalnu razinu, njegovi dionici oslanjaju se na norme međunarodnih konvencija i pravnu regulativu.

Pa tako Međunarodna pomorska organizacija (eng. *International Maritime Organizatio*, IMO) propisuje konvenciju o sigurnosti života na moru (eng. *Safety of Life at Sea*, SOLAS) prema kojoj je svaki putnički i transportni brod, koji je teži od 300 tona bruto, obvezan primjenjivati GMDSS sustav (eng. *Global Maritime Distress and Safety System*).

Da bi se na brodu postigla zadovoljavajuća razina sigurnosti, uz brojne druge čimbenike potrebno je osigurati sigurnost brodskih računalnih sustava jer su upravu oni kritične točke preko kojih bi mogli doći mogući napadi.

## 1.1. PROBLEM, PREDMET I OBJEKT ISTRAŽIVANJA

Problem istraživanja koje je ključno za ovaj rad jest pitanje vezano uz sigurnost informacija u sustavima pomorstva. Provedeno je istraživanje korištenjem anketa kako bi se došlo do što relevantnijih informacija iz poslovne (realne) okoline te se temeljem njih stvorila slika o ponašanjima i navikama zaposlenika pomorskih sustava u pogledu informacijske sigurnosti. Rezultati su u objašnjeni su u posljednjem poglavlju ovog rada uz prikaz izgleda ankete sa svim njenim pitanjima.

Ključan problem vezan je uz nedovoljno istraženo područje kada govorimo o informacijama, sigurnosti i pomorstvu u kombinaciji. Uz navedeno, pojavljuje se iznimno važan problem, a on se tiče kritične infrastrukture pomorskog sektora i njegove ranjivosti (prvenstveno se misli na neželjene radne, napade, uništavanje imovine, ugroza ljudskih života).

Iz ovakve prethodno navedene problematike, definira se predmet istraživanja. A on bi bio, ispitati i istražiti načine funkcioniranja u realnim situacijama, koje se u ovom istraživanju odnose na korištenje informacijskih sustava elektroničkim putem u svrhu poslovanja. Nadalje, predmet istraživanja jesu navike, educiranost i svijest zaposlenika pomorskog sektora na temu sigurnosti informacija.

Objekti istraživanja su informacije kao dio svakodnevne poslovne komunikacije, sigurnost općenito te sigurnost informacija, načini zaštite informacijskih sustava u okviru pomorskih sustava, ali i prakse temeljene na odlukama Europske Unije i NATO-a.

## 1.2. RADNA HIPOTEZA

Postavljena je radna hipoteza temeljem koje se pretpostavlja da se na uzorku od 20 ispitanika može dokazati postojanje svjesti o važnosti zaštite pomorskih informacijskih sustava, kao i mogućnostima napada na istoimene sustave. Provjerava se razina svijesti korisnika informacijskih sustava, kao i postojanje razvijene svijesti o pomorskom sektoru kao kritičnom dijelu infrastrukture dkada je riječ o mogućim napadima, odnosno terorizmu. Nadalje, dokazuje se razina educiranosti i informiranost cjelokupnog kadra za područje računalnih/informacijskih sustava unutar pomorskog sektora.

## 1.3. SVRHA I CILJEVI ISTRAŽIVANJA

Svrha provedenog istraživanja jest utvrditi na koje se sve načine postupa prema informacijama, na koje se načine provodi informacijska komunikacija te koji su to sve oblici zaštite koji se koriste. Nadalje, svrha jest i utvrditi postupke prilikom neželjenih radnji, ukoliko oni postoje.

Cilj istraživanja je ukazati na problematiku unutar informacijskog svijeta i pomorskog sektora kao kritičnog kada se radi o protoku informacija i njihovom presretanju od strane napadača. Također je cilj i ukazati na needuciranost kadra zaposlenog u pomorskim sustavima, njihova nedovoljna informiranost u pogledu *cyber* kriminala i nedovoljna ulaganja u načine zaštite informacijskih sustava (još uvijek se koriste oni primitivni i već po malo zastarjeli načini zaštite).

## 1.4. ZNANSTVENE METODE

Znanstvene metode koju su korištene prilikom izrade ovog rada jesu metoda indukcije pomoću koje se analizom pojedinih činjenica dolazi do općenitog zaključka, zatim je korištena metoda dedukcije kojom su objašnjene činjenice i zakonski okvir, metoda analize i sinteze te metoda dokazivanja.

## 1.5. STRUKTURA RADA

Diplomski rad sastoji se od devet poglavlja. Prvo poglavlje jest uvodno u kojem se opisuju problemi, predmet i objekt istraživanje kao i ciljevi istraživanja koje je provedeno, radna hipoteza te znanstvene metode koje su se koristile prilikom izrade rada.

Drugo poglavlje „Informacijska sigurnost i sigurnost informacijskih sustava“ odnosi se na definiranje termina informacijska sigurnost i sigurnost informacijskih sustava te se navode vrste prijetnji koje su mogućem kod ovakvih sustava.

U poglavlje broj tri opisane su računalne mreže, ali s posebnim osvrtom na računalne mreže broda i njihovu podjelu.

Poglavlje četiri odnosi se zaštite računalnih mreža općenito, kao i vrsta zaštite koje je moguće upotrebljavati.

U petom poglavlju analizirana je ranjivost prethodno navedenih pomorskih informacijskih sustava (GMDSS, MSSIS, AIS, SAFESEANET).

Poglavljem broj šest analizirana je *cyber* sigurnost u aspektu pomorstva. Unutar ovog poglavlja daje se jasnija slika o nedovoljno razvijenoj svijesti kada je riječ o prijetnjama i opasnostima, ali i o nerazumijevanju pomorskog sektora kao kritične infrastrukture. Nadalje, opisane su preporuke kako spriječiti moguće napade i to na globalnoj, regionalnoj i nacionalnoj razini.

Sedmo poglavlje opisuje informacijsku sigurnost unutar NATO okvira, ali prije svega orjentirano na pomorsko okruženje.

U osmom poglavlju prikazani su rezultati provedenog istraživanja. Prikazana su sva pitanja i ponuđeni odgovori iz ankete uz pomoć koje su se prikupljale informacije.

Deveto, odnosno posljednje poglavlje jest zaključak.

# 2. INFORMACIJSKA SIGURNOST I SIGURNOST INFORMACIJSKIH SUSTAVA

Pomorski sustavi spadaju u skupinu rizičnih sustava zbog ranjivosti njihove infrastrukture. Još uvijek se ne pridaje dovoljna važnost zaštiti informacija u sektoru pomorstva te se sve odvija na zastarjeli način, koji danas ne predstavlja dovoljan stupanj zaštite i sigurnosti. U današnje vrijeme sve prisutno je nanošenje štete informacijskim sustavim u obliku računalnog hakiranja ili uskraćivanja usluga. Na taj način onesposobljuje se jedan čitav sektor komuniciranja čime se mogu prouzročiti goleme štete. Kada je riječ o količini i obliku štete koja može uslijed takvog nečega nastati, tada se može reći kako se šteta kreće od financijskih, preko internih do nacionalnih (a ponekad i globalnih) problema.

Ako se uzme u obzir da je pomorstvo usko povezano sa svim ostalim granama prometa, gospodarstva, turizma, ... može se pretpostaviti koliko bi razmjeri štete mogli biti.

Kako bi bilo moguće prepoznati da se radi o ugrozi informacijske sigurnosti, potrebno je detektirati faktore koji na to upućuju. To bi bili različiti oblici prekida unutar sustava komunikacije, presretanja ili izmjene. Kako bi se to izbjeglo, potrebno je znati kako je sigurnost proces kojim se smanjuje rizik ili barem umanjuje vjerojatnost nastajanja nekog oblika štete. Aspekti informacijske sigurnosti kojima se sprječava nastanak štete jesu [2]:

- pristup informacijama
- identifikacija korisnika podataka
- autentifikacija
- autorizacija.

Nadalje, tu se mogu uvrstiti i [2]:

- odgovornost svih sudionika u procesu razmjene informacija
- podizanje svijesti
- upravljanje, kao dodatni aspekti kojima se provodi sigurnost.

## 2.1. DEFINICIJA SIGURNOSTI INFORMACIJA I INFORMACIJSKIH SUSTAVA

U daljnjem tekstu bit će navedene neke od definicija informacijske sigurnosti. Stoga, informacijska sigurnost bila bi sljedeće [2]:

*„Informacijska sigurnost ponekad se povezuje s informacijskim operacijama koje štite i brane informacijski sustav, a sve u svrhu osiguranja njegove raspoloživosti, integriteta, autentifikacije, povjerljivosti i neosporivosti. Dio informacijske sigurnosti jest i oporavak informacijskih sustava kroz sposobnost za zaštitu, detekciju i reakciju.“*

*„Informacijska sigurnost je zaštita informacija od velikog broja prijetnji radi osiguranja kontinuiteta poslovanja, smanjenja poslovnog rizika i povećanja prihoda od investicija i poslovnih prilika. Ona se postiže primjenom osiguravajućeg skupa kontrola, politika, procesa, procedura, organizacijske strukture i softverske i hardverske funkcije.“*

*„Informacijska sigurnost omogućuje ostvarenje ciljeva poslovanja na siguran način, u kojem su zadovoljeni regulatorni i sigurnosni zahtjevi kroz ugradnju odgovarajućih kontrola, upravljanje rizicima, te kroz podizanje sigurnosne kulture i svijesti u organizaciji.“*

Sigurnost informacijskih sustava dio je sveobuhvatne zaštite podataka. To mogu biti podaci koji su u procesu obrade, koji su pohranjeni ili oni čiji je prijenos u tijeku. Sigurnost informacijskih sustava štiti sustav od gubitka povjerljivosti, cjelovitosti i raspoloživosti, ali i sprječava gubitak sustava u cijelosti.

Eugene Spafford, voditelj odjela za kompjuterske operacije i sigurnosnu tehnologiju na sveučilištu Purdue u SAD-u dao je definiciju koja sadržava značajke sigurnosti informacijskih sustava, a ona glasi [2]

*„Jedini informacijski sustav koji je zaista siguran je onaj koji je ugašen, isključen iz napajanja, zaključan u sefu od titana, zakopan u betonskom bunkeru, te okružen nervnim plinom i dobro plaćenim naoružanim čuvarima. Čak ni tad, ne bih se baš kladio na njega.“*

Na temelju navedenih definicija može se zaključiti kako je to dio jako osjetljive komunikacijske infrastrukture kojom je svaki segment slaba karika. Kako bi se što više spriječili mogući napadi ili kakvi neželjeni događaji potrebna je razvijena svijest o ranjivosti, prijetnji i rizicima svih sustava informacijske sigurnosti. Ranjivost, prijetnja i rizik tri su glavna čimbenika uz pomoć kojih je moguće osigurati sigurnost na zadovoljavajućoj razini.[2]

***Ranjivost*** *(eng. vulnerability)* je stanje, slabost ili nedostatak unutar procedura informacijskih sustava.

Također odnosi se na tehničke fizičke i druge sustave kontrole, zatim na dizajn i implementaciju istih a sve u svrhu rezultiranja provedbe sigurnosti i sigurnosne politike. Sve to zajedno može uzrokovati operativne i financijske gubitke za organizaciju.

***Prijetnja*** *(eng. threat)* jest svaki onaj izvor mogućnosti da se iskoristi ranjivost sustava bilo da se radi o slučajnim ili namjernim postupkom.

***Rizik*** *(eng.risk)* je slaba karika od strane onoga koji upravlja sustavom (vlasnik, administrator), a uključuje vjerojatnost kako sustav u određenim uvjetima neće moći funkcionirati. Ne funkcionalnost sustava očituje se u ne provođenju sigurnosne politike te kritičnih operacija. [2]

## 2.2. PRIJETNJE INFORMACIJSKOJ SIGURNOSTI

### 2.2.1. Vrste prijetnji

Prijetnje informacijskoj sigurnosti mogu se kategorizirati u četiri opće vrste koje vrijede za sve računalno/informacijske sustave. To su [2]:

- prirodne prijetnje
- nenamjerne (nesreća)
- namjerne aktivne (ljudski faktor)
- namjerne pasivne (ljudski faktor).

Prirodne prijetnje jesu one na koje se ne može utjecati, a to bi bili potresi, poplave, požari, atmosferske neprilike, vremenski ekstremi...

Nenamjerne prijetnje su korisničke pogreške, pogreške operatera i administratora, greške koje nastaju uslijed pripreme podataka, greške izlaza, računalnih sustava, aplikacija i sve one pogreške u procesu komunikacije.

Namjerni aktivni napadi koji su uzrokovani ljudskim faktorom jesu neovlašteni pristup, sabotaža (terorizam), gomilanje lažnog prometa (DoS napadi).

Namjerni pasivni napadi, također uzrokovani ljudskim faktorom su prisluškivanje, neovlašteno korištenje računala i mrežnih komponenti, presretanje,...

### 2.2.2. Kategorije prijetnji

Kada je riječ o kategorizaciji vrsta mogućih prijetnji informacijskim sustavima, se može govoriti o šest vrta prijetnji. Prijetnje su kategorizirane na način da obuhvaćaju sve mogu segmente koji mogu biti uključeni o neželjene događaja. Također se odnose i na sve one načine koji se koriste ili se mogi koritstiti. Kategorizacija bi bila sljedeća [2]:

1. Odbacivanje usluga ili tzv. DoS (eng. *Denial of Service* ) koje se mogu podijeliti na nekoliko segmenata:

- fizičko uništenje mrežnog segmenta ili podmreže
- neoperabilnost mrežnih segmenata ili podmreže zbog greške na uređaju ili programu te zbog sabotaže
  - degeneracija performansi u slučajevima prevelikog zasićenja sustava, zatim zbog grešaka na liniji ili zbog nekog od vanjskih faktora (poput vremenskih nepogoda/neprilika),
  - mogućnost ovlaštenih korisnika da spriječe fizički pristup mrežnim uređajima i uslugama informacijskih sustava
  - svi ostali uvjeti ili događaji koji će izazvati neraspoloživost informacija i informacijskih sustava ovlaštenim korisnicima.

2. Neovlašteno otkrivanje također ima svoje podsegmente, a to su:

- svaki nenamjerni postupak izazvan od strane korisnika ili operatera, u slučajevima kod pripreme podataka, prilikom greške izlaza, sustava u cijelosti ili greške u komunikaciji
- kršenje postojećih pravila i propisa vezanih uz procedure prilikom kontrole pristupa (dozvola pristupa neovlaštenoj osobi)
- zlonamjerne radnje ovlaštenih osoba
- aktivni pokušaji napada ovlaštenih osoba.

3. Neovlaštene modifikacije dijele se na:

- postupci zaposlenika koji nisu odgovorni i zaduženi za informacijske sustave (osoblje, djelatnici, unutarnji dionici koji aktivno sabotiraju rad informacijskih sustava)
- osoblje koje nenamjerno izlazi s informacijskim sustavima, uslugama ili mrežnim operacija
- vanjski suradnici koji namjerno remete sustav (hakeri, krekeri, računalni kriminalci i drugi).

4. Prijetnje na LAN komunikaciji
5. Prijetnje na WAN komunikaciji
6. Uključeno osoblje
   - amateri
   - hakeri
   - krekeri
   - računalni kriminalci.

# 3. RAČUNALNE MREŽE KAO DIO INFORMACIJSKIH SUSTAVA

## 3.1. RAČUNALNA MREŽA BRODA

Unutar integriranog informacijskog sustava broda, brodski sustavi i uređaji povezani su međusobno računalnom mrežom. Računalna mreža broda povezana je na način da omogućuje podacima nastalim na bilo kojem mjestu prosljeđivanje na svako od umreženih računala. To bi se moglo objasniti na primjeru, ukoliko imamo informacije iz sustava za nadzor i upravljanje nekog od brodskog proces, a one su dostupne i obrađuju se u sustavima koji vode administrativne poslove. Odnosno, svi sustavi su koliko god odvojeni bili ili obavljali najrazličitije vrste poslova, međusobno povezani brodskom računalnom mrežom. Također, ukoliko se radi o podatcima nadzora, dijagnostike ili održavanja nekog od brodskih sustava, svi su oni dostupni na računalima na kopnu. Dakle, integrirani informacijski sustavi broda međusobno su povezani i djeluju kao jedna jedinstvena cjelina, a sve u svrhu što efikasnije i brže razmjene informacija.

Računalna mreža broda sastoji se i većeg broja segmenata. Svaki od njih realizira se na pojedinim razinama umrežavanja. Odnosno, zbog složenosti svakog od segmenata, koriste se i različiti načini umrežavanja. Ovako opisana mreža na brodu, hijerarhijski je organizirana i sastoji se od sljedećih razina umrežavanja [30]:

- umrežavanje na razini procesa
- umrežavanje na razini sustava
- umrežavanje na razini administracije
- umrežavanje koristeći Internet s kopna, koja na taj način čini jedinstvenu računalnu mrežu broda.

## 3.2. PODJELA RAČUNALNIH MREŽA

Razvojem računala pa samim tim i računalnih mreža tijekom desetljeća, došlo je do ostvarenja mogućnosti prijenosa velike količine podataka i multimedijalnog sadržaja, što je u samim počecima razvoja bio jedan od ključnih problema.

To se primjenilo prvo na malim udaljenostima unutar lokalnih mreža (LAN), a nakon toga i na puno većim udaljenostima (WAN).

Temeljem navedenog, računalne mreže mogu se podijeliti prema veličini, a to jesu sljedeće [30]:

- PAN (eng. *Personal Area Network*) jest mreža koja se koristi za povezivanje manjih komunikacijskih uređaja (telefon, fax...) na računalo. Ovakav oblik mreže odnosi se na korištenje od strane najčešće jednog korisnika, na udaljenosti od nekoliko metara.
- LAN (eng. *Local Area Network*) jest računalna mreža gdje su računala smještena na manje udaljenosti. Tu se uglavnom radi o računalima unutar ureda, doma ili nekih bliže smještenih objekata, koji se služe u osobne svrhe te je prijenos podataka njihovim korištenjem besplatan. Također, za ove mreže poznata je značajka da imaju jako veliku brzinu prijenosa podataka (eng. Gpbs – *Giga bit per second*).
- MAN (eng. *Metropolitan Area Networks*), mreža unutar koje su računala smještena na malo većim udaljnostima za razliku od računala lokalne mreže. One su u vlasništvu većeg broja osoba (uglavnom su to jedna ili više organizacija) i brzina prijenosa podataka je nešto manja u odnosu na lokalne mreže.
- WAN *(eng. Wide Area Network*) jest ona računalna mreža koja se proteže na veću površinu, bilo da se radi o površini grada, regije ili države. Kako bi se računala mogla međusobno povezati, koriste se usmjerivači, tzv. *routeri* ili javne komunikacijske mreže. WAN mreže se razlikuju od prethodno navedenih po tome što nisu u vlasništvu osobe ili organizacije, te prijenos podataka njihovim korištenjem nije ograničen ni brzinom ni količinom, a ni cijenom. [30]

Nadalje, mreže se mogu još podijeliti i prema tehnologiji sklopovlja koja se koristi. U tim slučajevima dijele se na [30]:

- Optičke mreže; za prijenos podataka koriste optička vlakna. Njihova brzina prijenosa i udaljenosti jest izrazito velika, a mogućnost pogreške prilikom prijenosa jest izrazito mala. Nedostatak ovakvih mreža jest cijena te složen proces instalacije.
- Ethernet; skup tehnologija koje se koriste za prijenos podataka u okvirima. Definira veliki broj standarda za signalizaciju i adresiranje. Za povezivanje prilikom instaliranja koriste se bakreni vodiči ili optika, čija je dostupnost široka, cijene pristupačne, a instalacija jednostavna. Prilikom zamjene podataka koriste se velikim brzinama, ali su im udaljenosti ograničene.
- Bežične mreže; ili *wireless* mreže jesu one mreže koje nastaju povezivanjem većeg broja računala bez upotrebe bilo kakvih fizičkih veza. Prijenos podatak putem *wirelessa* odvija se infracrvenim zrakama ili radiovalovima. Ovakav oblik umrežavanja, razvojem i napretkom tehnologije postaje sve dostupniji.

To je prije svega zbog jednostavnosti instalacije, mogućnosti korištenja od stranje velikog broja korisnika koji nisu u svakom trenutku u mogućnosti spajati se na fiksirane mrežne sustave. Prijenos podataka i udaljenost kod ovakvog tipa mreže jeste donekle ograničen, te podložan smetnjama od strane različitih radio frekvencija.

- Power line comunication (PLC); ovaj oblik umrežavanja predstavlja prijenos podataka korištenjem naponskih vodova. Ova vrsta tehnologije mogla bi u budućnosti zauzeti vodeće mjesto zbog široke rasprostranjenosti strujnih vodova. Međutim, još uvijek nije dovoljno rasprostranjena [30].

Osim navedenih, računalne mreže možemo još podijeliti i prema funkcionalnim povezanostima između pojedinih elemenata koji tvore mrežu. To bi bili sljedeći [30]:

- Active networking; predstavlja oblik komunikacijskog modela čija je funkcija da paketima koji prolaze kroz telekomunikacijsku mrežu daje mogućnost dinamičke promjene rada mreže.
- Klijent-server; kod ovakve mreže uloge klijenta i poslužitelja su razdvojene. Klijent ima ulogu da uputi zahtjev za određenom radnjom, dok poslužitelj te radnje treba i ispuniti (elektronička pošta).
- Peer-to-peer; u ovakvom obliku mreže, svi njeni članovi su ravnopravni. Nema podjelekao kod prethodno navedene mreže (klijent-server), već su svi članovi istovremeno i klijenti i poslužitelji [30].

# 4. ZAŠTITA RAČUNALNIH MREŽA

Sigurnost unutar računalnih mreža jedan je od problema koji se najčešće zanemaruje. Uglavnom se takvo što događa zbog neinformiranosti, neznanja ili nedostatka svijesti o opasnostima koje vrebaju sustave računalnih mreža.

Što su računalni sustavi veći i kompleksniji to se više pažnje treba posvetiti upravo njihovoj zaštiti. Jedan od takvih sustava jest i sustav računalnih mreža na brodovima preko kojih se odvija velik broj razmjene informacija. Najizloženiji napadima jesu sustavi bežićne komunikacije zbog njihovog neusmjerenog i nekontroliranog odašiljanja u svim smjerovima. Kao takvi, iznimno su ranjivi te izloženi presretanju od strane bilo koga tko nema direktnu vezu s izmijenjenim podacima. To se odnosi na korištenje bežićnih lokalnih računalnih mreža (WLAN- eng. *Wireless Local Area Network*) [22].

U nastavku rada bit će objašnjen svaki od mogućih oblika zaštite, uz poseban naglasak na WPA protokol zaštite podataka, budući da je danas to najnaprednije sigurnosno rješenje. Osim toga, WPA protokol zaštite istiknuo se tijekom provođenja istraživanja za ovaj rad, čiji će rezultati biti prikazani u poglavlju 4.1.6.

## 4.1. VRSTE ZAŠTITE RAČUNALNE MREŽE

### 4.1.1. Antivirus

Antivirus, antivirusni program ili softver je računalni softver za zaštitu računala, identifikaciju i/ili ukljanjanje virusa koji se pojavljuju na računalima. Njihova funkcija služi i zaštiti svih drugih programa koji mogu prouzročiti probleme prilikom korištenja računala, oštetiti softver ili podatke na računalu. Današnji antivirusni programi, dizajnirani su na način da sustav štite od što većeg broja različitih prijetećih, odnosno malicioznih problema ili phishing napada. Neki od problema koji se pojavljuju, a antivirusi ih uspješno otklanjaju jesu crvi, trojanski konji, različite vrste virusa, rootkita, spywarea, adwarea [25].

### 4.1.2. Vatrozid

Još jedan oblik zaštite računalnih mreža jest vatrozid (*eng. firewall*). Vatrozid je naziv za uređaj kojim štitimo privatni dio mreže od javnog. Njegova primarna funkcija jest omogućavanje kontroliranog pristupa iz unutrašnjeg dijela mreže prema vanjskom dijelu mreže (javnom dijelu). To bi značilo da dopušta pristup prema Intranetu ili obrnuto [26].

Kako bi se svrha vatrozida što bolje objasnila, potrebno ga je gledati kao skup mehanizama koji se dijele na dva osnovna principa [12]:

1. princip koji sprječava promet paketa
2. princip koji omogućava promet unutar mreže.

Kako bi omogućio pristup drugim mrežama, vatrozid se postavlja na samoj granici mreže. Njegovim korištenjem omogućena je centralizacija svih sigurnosnih servisa na samo jednom uređaju. Stvaraju se tzv. „uska grla“ (*eng. bottlenecks*) između vanjskih i unutarnjih mreža kako bi se cijeli promet mogao odvijati preko jedne kontrolne točke.

Osnovne funkcije vatrozida su sljedeće [12]:

- paketno filtriranje
- maskiranje mrežnih adresa
- posredna uloga
- virtualne privatne mreže.

### 4.1.3. Lozinke – *Password*

Lozinka, zaporka ili *password* oblik je tajnog podatka čiji je sadržaj potrebno znati kako bi se moglo pristupiti određenim resursima. Dakle, lozinke su oblici zaštite koji se koriste za autentikaciju i dokazivanje identiteta onog korisnika koji želi pristupiti željenim informacijama unutar nekog sustava.

Upravo identifikacija korisnika određenih resursa bitan je preduvjet za osiguranje privatnosti, integriteta i zaštite podataka. Uporaba lozinki predstavlja jednostavnu i najisplativiju metodu zaštite podataka, ali i određivanja identiteta korisnika. Osim navedenih pozitivnih elemenata korištenja lozinke, postoje i neki negativni, a to bi bili npr., krađa lozinke ili zaboravljanje pristupnih podataka korisnika koji zahtjeva ulazak u sustav. Postoji niz tehnika kojima se vrši autentikacija korisnika, a to su sljedeće [6]:

- Korištenje jednokratnih lozinki - korištenjem ove metode smanjuje se mogućnost neovlaštenog pristupa povjerljivim informacijama, datotekama i informacijama zbog nemogućnosti korištenja iste lozinke više od jednog puta. Svakim novim ulaskom u sustav potrebno je formirati novi oblik lozinke.
- Sigurnosni token - ovakav sustav zaštite uglavnom se koristi kod Internet bankarstva. Funkcionira na sličan način kao i jednokratne lozinke, ali uz upotrebu posebnih uređaja kojima utvrđuju svoj identitet. Takvi uređaji rade na principu aktiviranja PIN-a i unosa određene numeričke vrijednosti. Nakon toga korisnik dobiva mogućnost pristupa sustavu.
- Biometrijske metode - ova vrsta zaštite jest oblik provjere identiteta na temelju jedinstvenih fizioloških osobina svakog čovjeka. Tu se uglavnom radi o otiscima prstiju, skeniranju rožnice oka, prepoznavanju DNK i slično. Da bi se pristup nekom sustavu

ostvario, potrebno je da se biometrijski podaci prikupe uz pomoć senzora koji ih šalju na daljnju analizu gdje se stvara biometrijski uzorak koji se uspoređuje s dobivenim uzorkom, koji se mora podudarati.

- Sustav jedinstvene autentikacije - vrsta mehanizma koja korisnicima omogućuje prikaz akreditacijskih podataka samo jednom, nakon čeka slijedi pristup svim podatcima. Glavni nedostatak ovakve vrste zaštite jest nepostojanje jedinstvenog standarda za primjenu pristupa.
- Korištenje ne-tekstualnih zaporki - ovakvom zaštitom podacima se pristupa na način da se koriste različite kombinacije znakova, grafičkih lozinki ili određenim potezima mišem.
- Primjena digitalnih certifikata - digitalni certifikati određuju skup podataka zapisanih u elektroničkom obliku koji na taj način predstavlja jedinstveni elektronički identitet koji omogućava sigurnu komunikaciju Internetom.

### 4.1.4. Sigurnosni protokoli

Pod pojmom sigurni protokol podrazumijeva se vrsta internet zaštite osobnih, korporativnih ili institucionalnih podataka na načine koji će biti objašnjeni u nastavku teksta.

- Provjera autentičnosti porijekla podataka - provjera se svodi na to da svaki datogram mora dolaziti od prethodno navedenog odašiljača.
- Integritet podataka - odnosi se na provjeri sadržaja datograma, kako ne bi došlo do slučajne ili namjerne pogreške zbog koje bi se njihov sadržaj mogao promijeniti.
- Povjerljivost podataka - kako bi se ova funkcija mogla izvršiti, izvode se radnje skrivanja sadržaja poruka. To se radi najčešće na način da se koriste različita šifriranja.
- Zaštita replaya - osiguranje zaštite kako napadač ne bi mogao presresti datogram i izvršavati radnje u nekom drugom trenutku.
- Automatsko upravljanje kriptografskim ključevima i sigurnosnim asocijacijama - ima zadaću osigurati korištenje mrežne politike preko cijele proširene mreže s minimumom ručne konfiguracije [31].

### 4.1.5. Fizička zaštita

Fizička zaštita su sve mjere zaštite kojima se sprječavaju neovlašteni pristupi informacijama koji se pohranjuju na fizičkim medijima. Ovakav oblik zaštite je najosnovniji aspekt zaštite koji obuhvaća kontrolu zaštite postrojenja, prostorija, zgrada ili neke druge imovine. Mjere koje uključuju fizičku sigurnost su [7]:

- Pasivne mjere - upotreba arhitekture i okoliša kako bi se postigla što bolja sigurnost kroz olakšanu detekciju prijetnji.
- Aktivne mjere - sustavi i tehnike koje su dizajnirane isključivo za detekciju i reakciju u slučaju prijetnje ili napada.

Ovakav oblik zaštite osigurava da samo ovlaštene osobe imaju pristup određenim resursima, bilo da se radi o nekretninama ili informacijama. Prijetnje fizičkoj sigurnosti moguće je svrstati u dvoje kategorije: prirodne nepogode i ljudski faktor.

Prirodne nepogode su [7]: meteorološke nepogode, geofizičke nepogode, sezonski fenomeni, astrofizički fenomeni, biološke prijetnje.

Ljudski faktor koji utječe na fizičku zaštitu su: neposlušnost, sabotaža, otkrivanje povjerljivih podataka, zlouporaba ovlasti, nenamjerna oštećenja, neovlašten pristup podatcima, krađa podataka.

### 4.1.6. WPA/WPA2

Najraširenij sustav zaštite bežičnih lokalnih mreža jest WPA2. Ovaj sustav razvijen je u okviru Wi-Fi Alliance udruženja 2004. godine kao poboljšana inačica WPA protokola, koji je također nastao u okviru iste organizacije.

#### 4.1.6.1. Wi-Fi

Wi-Fi Allianca, udruženje osnovano 1991. godine koje radi na principu neprofitnog globalnog udruženja tvrtki s ciljem unaprjeđenja i promicanja takve vrste tehnologije na tržištu. Udruženje do danas broji prelazi brojku od tristo članova u više od 20 zemalja.

Wi-Fi Alliance može biti objašnjena kao bežična mreža uz pomoć koje se vrši razmjena podataka između dva ili više računala korištenjem radio frekvencije (2.4 GHz i 5 GHz) i odgovarajućih antena. Wi-Fi se razvija primjenjujući standarde IEEE 802.11 koji su sljedeći [4]:

- 802.11a, standard čija je teoretska brzina 52 megabita (Mb) u sekundi, međutim najčešće ta brzina iznosi 30 megabita u sekundi (Mbps). Ova varijanta standarda je skuplja.
- 802.11b, brzina iznosi 11 Mbps, međutim zbog utjecaja velikog broja prepreka i smetnja brzina može pasti na svega 1 do 2Mbps. Ovaj standard je najjeftinija varijanta Wi-Fi mreže.
- 802.11g, objedinjuje prethodna dva standarda. Radi na frekvenciji od 2.4 GHz, a njegova brzina jednaka je brzini 802.11a standarda.

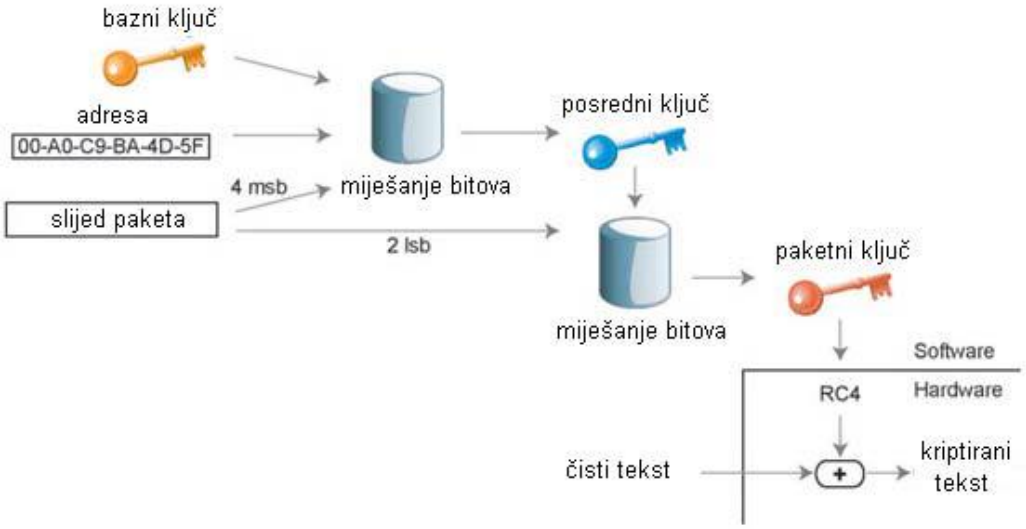
Unutar okvira IEEE 802.11 postoji još i niz obveznih certifikacijskih programa koji uključuju sljedeće [4]:

- Od obveznih programa to bi bila provjera u svrhu zadovoljavanja svih IEEE specifikacija u jednostrukom (način rada odnosi se na provjeru specifikacija 802.11a, 802.11b, 802.11g) ili dvostrukom (802.11b i 802.11g) načinu rada te u višepojasnom (frekvencije 2.4GHz i 5GHz) načinu rada.
- Zatim provjera zadovoljavanja sigurnosnih protokola WPA (eng. *Wi-Fi Protected Access*) i WPA2 (eng. *Wi-Fi Protected Access2*), kako za osobnu primjenu tako i za poslovne korisnike.
- Te provjeru identiteta mrežnih uređaja, odnosno provjeru EAP (eng. *Extensible Authentication Protocol*).

#### 4.1.6.2. WPA

*Wi-Fi Protected Access*, WPA je sustav zaštite bežićnih mreža koje su opisane u okviru standarda poznatih pod nazivom IEEE 802.11i. Navedeni standardi omogućuju enkripciju podataka te provjeru identiteta korisnika. Kako je prethodno objašnjen sustav WEP, tako i WPA za svoj rad koristi RC4 sustave kriptiranja podataka. Rad RC4 sustava kod WPA koristi 128-bitni ključ i 48-bitni inicijalizacijski vektor (IV). Tim je onemogućeno da se dva paketa enkriptiraju uz pomoć istog IV-a [4].

Razlika između WEP i WPA, ujedno i glavna prednost jest korištenje TKIP protokola (eng. *Temporal Key Integrity Protocol*), uz pomoć kojeg dolazi do mijenjanja ključeva u razdoblju korištenja sustava. Korištenjem TKIP protokola u kombinaciji s dugačkim inicijalizacijskim vektorom, sustav je moguće vrlo lako obraniti od mogućih napada. Lakoća obrane korištenjem ovog protokola jest zbog njegove složenosti funkcije kojom se stvaraju nizovi bitova uz pomoć kojih se vrši kriptiranje teksta. Tim se napadaču otežava mogućnost otkrivanja tajnog ključa u slučaju prisluškivanja mrežnog prometa. TKIP također jamči da svaki paket u mreži bude kriptiran drugačijim ključem. U studenom 2008. godine došlo je do otrića ranjivosti protokola TKIP. Radilo se o načinu na koji napadač ipak može otkriti niz bitova kojima je kriptiran paket. Takav oblik napada odnosio se samo na kratke poruke kojima je sadržaj uglavnom poznat. Takve poruke jesu ARP (Address Resolution Protocol) poruke kojima se otkrivaju sklopovske adrese temeljem mrežnih adresa uređaja. Ovakav oblik ranjivosti odnosi se samo na WPA protokol, ali ne i na WPA2 protokol [4].




**Slika 1. Shematski prikaz TKIP protokola [4]**

Osim već spomenutih poboljšanja, WPA protokol sadrži sigurniji sustav provjere poruka u odnosu na CRC (eng. *Cyclic Redundancy Check*) sustav koji se koristi kod WEP protokola. Kod CRC sustava moguće je od strane napadača promijeniti sustav poruke i vrijednost CRC-a vratiti na izvorni oblik, i to bez poznavanja ključa kojim je poruka kriptirana. Kako bi se takvi scenariji izbjegli, koristi se sigurniji način provjere, tzv. „*Michael*“ (eng. *Message Integrity Code, MIC*). Ovaj način provjere u WPA uključuje brojač okvira, a na taj se način isključuje mogućnost promjene sadržaja poruke u procesu komunikacije. Algoritam zvan Michael izveden je na način da bude dovoljno siguran, ali se ipak vodila sigurnost da bude moguće koristiti ga na starijim mrežnim karticama [4].

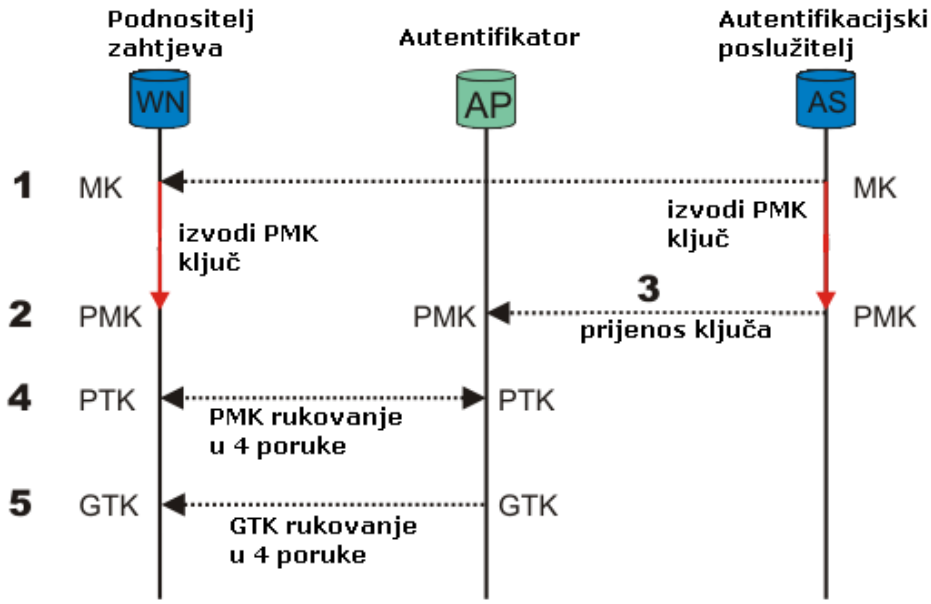
#### 4.1.6.3. WPA2 protokol

Već spomenuti EAP protokol (eng. *Extensible Authentication Protocol*) dio je WPA protokola, pa je kao takav sadržan i u WPA2 protokolu kako bi definirao format poruka prilikom bežične autentikacije. Protokoli koji koriste EAP metodu izvode se na sloju po pod pojmom PPP protokol (eng. *Point-to-Point Protocol*). Ovim protokolom, PPP, dolazi do izravnog povezivanja dvaju čvorova unutar mreže čime se vrši zaštita komunikacije. Odnosno, PPP protokolom dolazi istovremeno do autentikacije i enkripcije. Autentikacijom WPA2 protokola vrši se razmjena ključeva uz pomoć kojih se podatci koji se šalju kriptiraju, a to se odvija unutar četiri koraka [4].

- Master Key (MK), za izvođenje tajnog PMK ključa
- Pairwise Master Key (PMK), za razmjenu PTK tajnog ključa

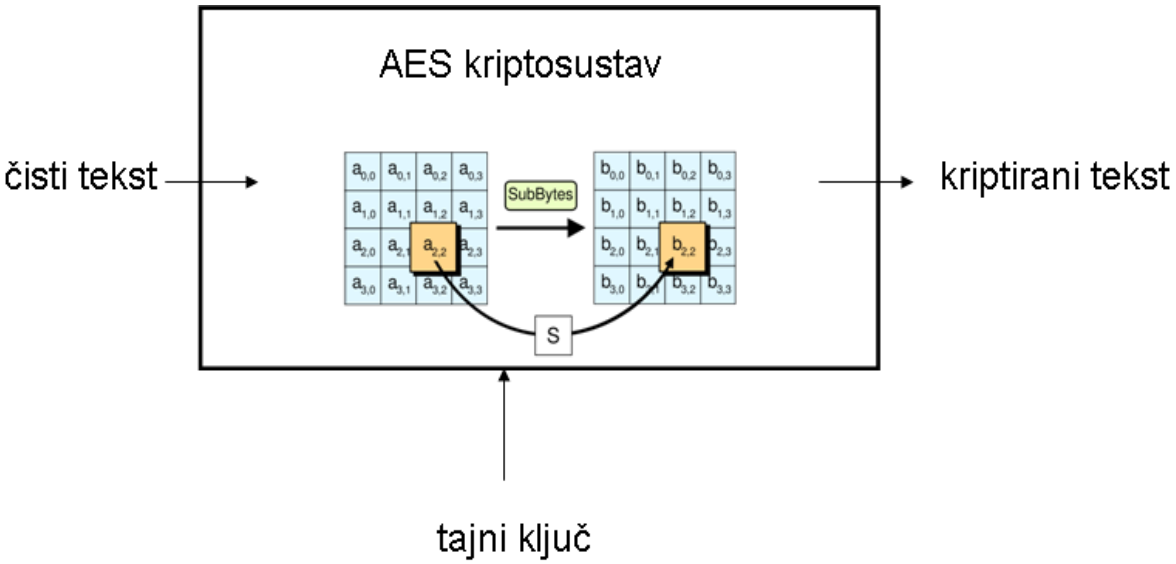
- Pairwise Trainsient Key (PTK), za enkripciju, razmjenu GTK ključa, dokazivanje identiteta
- Group Temporal Key (GTK), za dekripciju multicast i broadcast prometa.

Sljedeća slika prikazuje navedene korake za autentikaciju WPA2 protokola.




**Slika 2. Shematski prikaz autentikacije WPA2 kroz proces razmjene tajnih ključeva unutar četiri koraka [4]**

Za razliku od WPA protokola koji koristi TKIP enkripciju, WPA2 uvodi CCMP (eng. *Counter Mode with Cipher Block Chaining Message Authentication Code Protocol*) enkripciju koja je temeljena na AES (eng. *Advanced Encryption Standard*) algoritmu i kriptiranju blokova na ulančani način. AES, simetrični kriptografski algoritam koji za funkciju ima kriptiranje podataka po blokovima veličine 128 bita, a ključ kojim se koristi za kriptiranje može biti u rasponu veličina od 128, 192 i 256 bita. Ovakav način enkripcije podataka smatra se u potpunosti sigurnim [4].




**Slika 3. AES kriptiranje kod WPA2 protokola [4]**

#### 4.1.6.4. Načini korištenja protokola

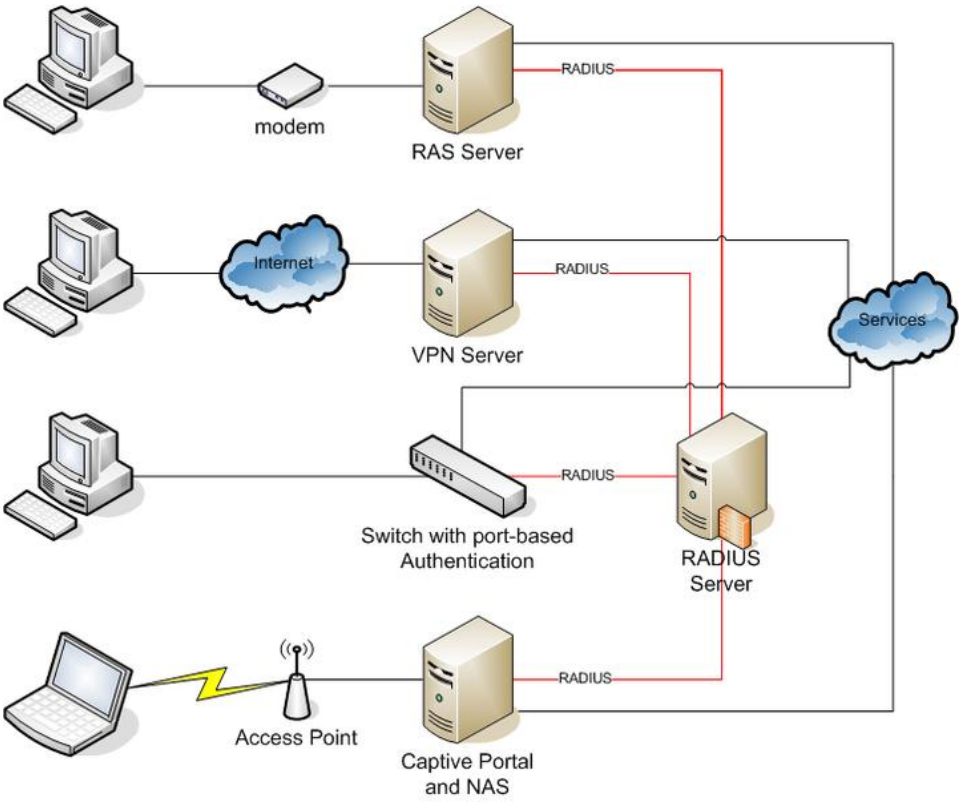
Protokoli WPA i WPA2 koriste se na sljedeća dva načina [4].

1. PSK (eng. *Pre-Shared Key*), odnosi se na prethodnu razmjenu ključeva između klijenata i pristupne točke.

Ovaj način rada još je poznat i pod nazivom privatni jer je upravo njegova namjena vezana uz korištenje privatnih mreža ili nekih manjih poslovnih mreža. Njegova izvedba je iznimno jednostavna, ne zahtjeva autentikacijskog poslužitelja, već je definiran 256 bitni ključ koji služi za kompletnu komunikaciju unutar mreže. Potrebno je unositi što nelogičniju i kompliciraniju kompilaciju nizova znakova prilikom stvaranja ključa kako bi napad bilo nemoguće izvesti.

2. Enterprise, zaseban ključ između klijenata i pristupne točke.

Enterprise je način rada koji sadrži bolju zaštitu upravo zbog toga jer se svaki uređaj unutar mreže mora zasebno autentificirati, tj potrebna je identifikacija svakog. Međutim, ovakav oblik sustava zahtjeva izrazito veći opseg posla. Ovaj oblik autentifikacije poslužitelja koristi RADIUS (eng. *Remote Authentication Dial In User Service*) mrežni protokol kako bi izvodio centraliziranu autentifikaciju [4].




**Slika 4. Prikaz korištenja RADIUS mrežnog protokola [4]**

# 5. RANJIVOST POMORSKIH INFORMACIJSKIH SUSTAVA

## 5.1. GMDSS – GLOBAL MARITIME DISTRESS AND SAFETY SYSTEM

GMDSS sustav jest sustav koji garantira automatsko slanje MSI poruka s obalnih radio postaja prema svim brodovima. Njegovo korištenje propisuje obaveznu ugradnju radio uređaja na svim SOLAS plovilima uzimajući u obzir njihovo područje plovidbe.

Obalne postaje imaju funkciju pomorskih radio postaja koje se nalaze na kopnu. Pod njihovim nadzorom su frekvencije koje su na brodovima namijenjene za odašiljanje obavijesti o pogibelji, zatim vrše koordinaciju radio prometa te su posrednici u komunikaciji između dva ili više plovila ili između plovila i kopna. Obalne postaje uglavnom se služe daljinskim vođenjem na relaciji predajnik/prijemnik, pomoću kojeg imaju veću šansu povećanja dometa VHF DCS signala za određeno područje plovidbe. Međutim, u slučajevima kada postoji samo VHF radio signal, pojedine obalne postaje imaju potrebnu opremu pomoću koje također mogu uspješno locirati plovilo koje se nalazi u pogibeljnoj situaciji.

Da bi sustav GMDSS mogao što bolje funkcionirati, određena su četiri temeljna područja plovidbe prema kojima su definirane radio frekvencije i vrste brodskih radijskih uređaja [1]:

- A1 jest područje GMDSS-a koje se nalazi unutar VHF dosega obalne postaje koje iznosi do 30 milja ili od 156 do 174 Mhz.
- A2 je područje koje se nalazi izvan dosega A1, ali je u dometu one obalne postaje koja radi na području MF, na udaljenosti od 100 do 200 milja ili od 1605 do 4000 KHz.
- A3, područje koje se nalazi izvan područja A1 i A2, ali unutar područja koje je pokriveno HF i INMARSAT-om. Omogućva stalno uzbunjivanje na dometu od 70°N do 70°S.
- A4 jesu sva ona područja koja nisu u dosegu A1, A2 ili A3. To se odnosi na udaljenosti HF od 4000 do 27500 KHz.

## 5.2. MSSIS – MARITIME SAFETY AND SECURITY INFORMATION SYSTEM

Sustav za pomorsku sigurnost i sigurnost informacijskog sustava (eng. *Maritime Safety and Security Information System* - MSSIS) je namijenjen za multilateralnu suradnju i dijeljenje podataka među međunarodnim sudionicima, s primarnim ciljem povećanja pomorske sigurnosti. Izvori podataka mogu sezati od jednog senzora do cijele nacionalne mreže za praćenje brodova.

MSSIS je savršeno pogodan one-stop izvor za prikazivanje pomorskih podataka u globalu. Budući da podatci koje distribuira MSSIS održava svoj izvorni, međunarodno priznati format i dostavlja podatke korisnicima u skoro realnom vremenu, organizacije članice su u mogućnosti koristiti opskrbu kako bi zadovolji zahtjeve u svojim specifičnim misijama [27,28].

Uz pomaganje protočnosti pomorskog prometa, MSSIS je neprocjenjiv alat u borbi protiv krijumčarenja droge, trgovine ljudima, piratstva i globalnog terorizma.

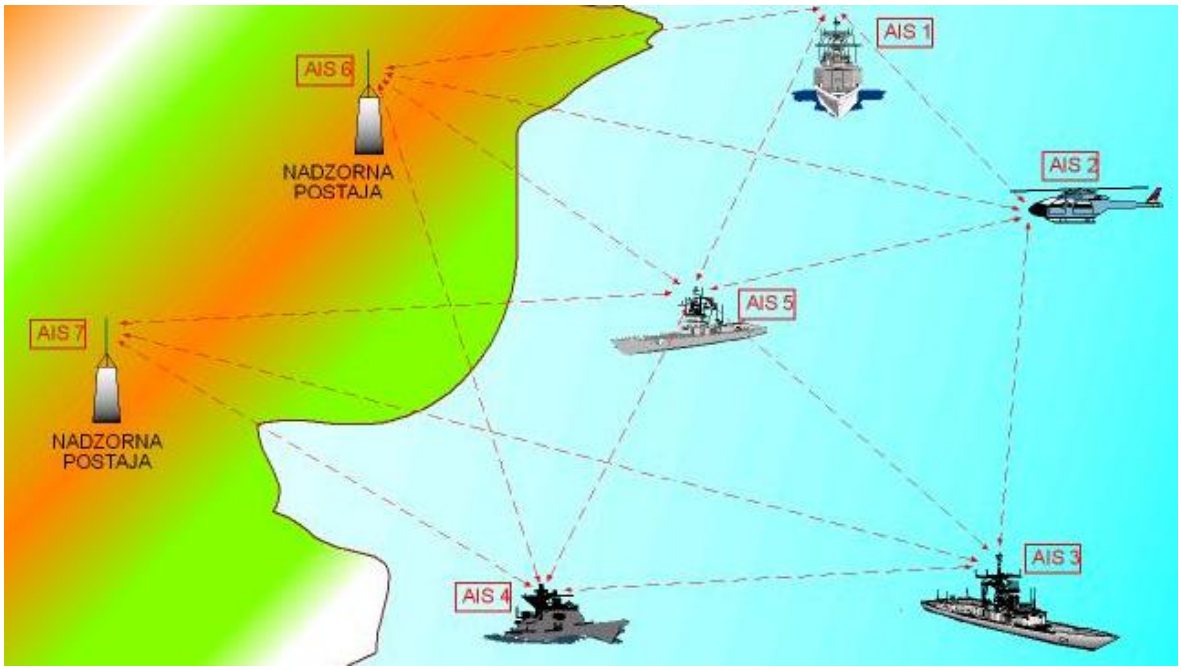
## 5.3. AIS - AUTOMATIC IDENTIFICATION SYSTEM

AIS (eng. *Automatic Identification System*), sustav automatske identifikacije brodova, najbolje je ostvarenje revizije SOLAS konvencije. Prema standardima IMO-a, AIS je brodski ili obalni primopredajnik koji radi na pomorskom području koje obuhvaća VHF (eng. *Very High Frequency*) opseg frekvencija.

AIS sustav osigurava unaprijeđenu sigurnost na područjima plovidbe, te doprinosi radu službe pomorskog prometa (*Vessels Traffic System* – VTS) na način da udovoljava svim zahtjevima sustava, kao što su način rada broda (npr. funkcionalni zahtjevi u slučaju sprječavanja sudara brodova), pružanje različitih informacija o brodu i/ili teretu koji brod prevozi, te upravljanje pomorskim prometom na relaciji brod – kopno ili kopno – brod [9].

AIS pruža brodovima i odgovornim tijelima automatske informacije koje su iznimno zahtjevne točnosti i učestalosti kako bi se pomorski promet odvijao što sigurnije. Ovakav način pružanja informacija zahtjeva minimalna sudjelovanja brodske posade.

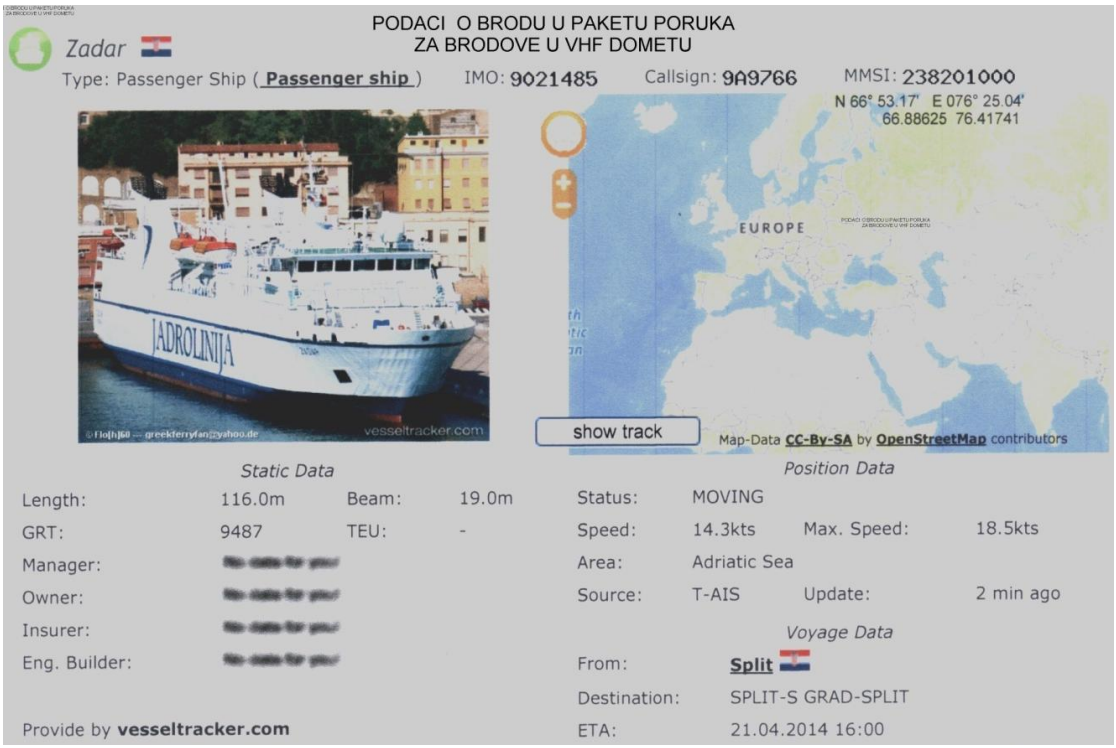
Načinom rada stvara slike određenih pomorskih situacija u realnom vremenu sa svim potrebnim podatcima o brodovima (pozicije drugih brodova u neposrednoj blizini, brzine brodova i kurs njihove plovidbe, različiti drugi statički i dinamički podaci o brodu). Prikupljajući veliki broj „svježih“ informacija na ovaj način, pridonosi se kvalitetnijim upravljanjem plovidbom, bržim i ispravnijim donošenjem odluka kako bi se izbjegli svi neželjeni nesretni slučajevi poput sudara brodova, odnosno kako bi se što više smanjio utjecaj ljudskog faktora. Prvenstveno kako bi se utjecalo na moguće ljudske pogreške i rizike prilikom navigacije [9].




**Slika 5. Prikaz na koji način radi AIS (*Automatic Indentification System*) mreža [13]**

Na slici 5 prikazano je kako svaki brod odašilje pakete različitih informacija vezanih za plovidbu. Svi ostali brodovi i nadzorne postaje na kopnu, koji se nalaze u VHF frekventnom području dometa, primaju te pakete.

Što se tiče područja Republike Hrvatske, temeljem rezolucije IMO-a (*International Maritime Organization*), direktiva Europske unije i Pravilnika o sigurnosti pomorske plovidbe na području unutarnjih morskih voda i teritorijalnog mora, uređajima AIS trebaju biti opremljeni svi putnički brodovi, trgovački od 300 bruto tona i više, kao i svi tankeri. Zatim, AIS uređaje moraju imati svi ribarski brodovi koji su dulji od 15 metara. Osim navedenog, AIS se nalazi instaliran uzduž hrvatske obale na 17 baznih stanica, odnosno na nadzornim postajama VTS-a (*Vessel Traffic Service*) [13].




**Slika 6. Primjer korištenja AIS sustava u RH za putnički brod „Zadar“, 21.4.2014. [33]**

Razmjena informacija između brodova i obalnih nadzornih postaja (VTS) odvija se u potpunosti automatski, u dometu VHS radioveze, vremenskim trajanjem 26,6 milisekunda, redoslijedom koji je sinkroniziran od strane Globalnog sustava satelitske navigacije *(eng. Global Navigation Satellite System* – GNSS), a vremenski signali dobivaju se iz GPS-a (*Global Positioning System*) koji se nalazi u sklopu AIS uređaja. GNSS odašilje sve podatke vezane za informacije i pozicije svakog broda u dometu, a njih prima i GPS prijemnik na brodu. Dakle, bez sinkronizacije podataka iz GNSS-a i GPS-a AIS sustav ne bi mogao funkcionirati. U slučaju kada bi došlo do izostanka prijema vremenskih signala, zbog problema u sustavu GNSS-a ili zbog nastalog kvara, odnosno neispravnosti GPS prijemnika, AIS sustav ne bi mogao funkcionirati [9].

Uvrštavanje AIS sustava u redovnu upotrebu za VTS službe predstavlja znatnu vrijednost jer zbog njega detekcija i praćenje brodova postaje pouzdanije, domet praćenja brodova povećava se do 60 km, moguće je pratiti i manje brodove koje VTS radari nisu bili u mogućnosti pratiti zbog male moći radarskog horizonta i općenito male moći njihovih radara.

Osim navedenih prednosti, upotrebom AIS sustava pojavljuju se i određene mane.

Kako bi se osigurala što bolja učinkovitost ovog sustava, ali i zaštitila njegova sigurnost, institucije pomorske i nacionalne sigurnosti na moru provodile su analiziranja i provjere u različitim uvjetima kako bi što detaljnije pronašle slabosti sustava, te ga na posljetku bile u mogućnosti otkloniti. Tako je AIS sustav ispitan na sve vanjske smetnje, zatim na ometanja, koja mogu biti nenamjerna ili namjerna. Provođenjem navedenih akcija došlo je do postavljanja pitanja može li se dogoditi da se ovakav novonastali sustav (AIS) zloupotrijebi u svrhu ubacivanja nepotrebnih ili krivih informacija u pakete koji se odašilju i odlaze svim brodovima u dometu. Odnosno, postoji li mogućnost da je ovaj sustav najslabija karika u slučaju mogućih piratskih napada, terorizma ili krijumčarenja.

### 5.3.1. GPS „najslabija karika“ AIS sustava

Osim što je najvažniji čvor u mreži AIS sustava, GPS prijamnik je ujedno i najslabiji čvor. Preko GPS-a primaju se najvažniji satelitski signali, koji su temelj funkcioniranja AIS sustava. Međutim, zbog slabe jačine signala i udaljenosti od 20 000 km između zemlje i satelita, do GPS prijamnika dolazi vrlo slab signal koji svaki uređaj nije u mogućnosti primit. Takav signal dolazi samo do prijamnika vrlo visoke osjetljivosti. Zbog ovakvog problema dolazi do mogućnosti primanja različitih interferentnih signala iz okoline, koji mogu utjecat i na sam rad sustava AIS. Naime, stalna otvorenost GPS prijamnika dovodi do učestalog (ako ne i konstantnog) primanja velikog broja različitih informacija koji u pojedinim slučajevima mogu izazvati različite „anomalije“ u daljnjem odašiljanju istih. Netočni ili nepotpuni signali dovode do širenja istih takvih informacija koje mogu utjecati na cjelokupnu navigaciju i svaki idući brod u dometu. Osim toga, moguće je i namjerno emitiranje signala koji nisu u svrhu poboljšanja navigacije ili pružanja potrebnih informacija, već su tu s namjerom da remete rad i dovode do mogućih neželjenih aktivnosti (bilo to piratstvo, terorizam ili krijumčarenje bilo koje vrste) [13].

Primanje različitih signala na GPS prijamnik može izazvati poremećaje u radu AIS sustava ili ga čak u potpunosti onemogućiti.

U slučajevima kada postoje nenamjerni signali koji izazivaju smetnje, oni se uglavnom odnose na lokalne komunikacijske sustave, TV odašiljače, radio prijamnike, radarske ususstave ili neke druge, pomorci ih uočavaju na svojim AIS sustavima te znaju kako postupati. Međutim, kada se radi o namjernom ometanju u te svrhe se koriste ometači znatno male snage. Takvi ometači dostupni su na otvorenom tržištu po vrlo pristupačnim cijenama.

Zbog svega navedenog, ranjivost AIS sustava je dovela do toga da se vrše istraživanja na području njegove zaštite i sigurnosti, te je potakla međunarodne pomorske institucije na detaljnije analiziranje sustava kako bi se bilo kakve nepravilnosti moguće spriječiti ili predvidjeti.

### 5.3.2. Napadi na AIS sustave

Već spomenuta ranjivost AIS sustava dovela je do toga da je nekoliko državnih institucija u Velikoj Britaniji, u razdoblju od 2008. i 2009. godine, provelo istraživanje AIS sustava ometanjem. Naime, njihovi GPS prijamnici bili su izloženi ometanjem već spomenutim šumnim ometačima razmjerno male snage, ali i ometačima znatno jače snage. Tijekom provođenja tog istraživanja, AIS sustavi su bili do te mjere ometani da njihov rad gotovo nije bio moguć. Primali su različite nerazumne signale iz okoline o svim brodovima u dometu što je izazvalo val netočnih informacija. Primjerice, prikazivanje netočnih brzina brodova koje nisu bile zanemarivih razlika već su varirale od nule pa sve do nekoliko stotina čvorova. Funkcioniranje AIS-a na ovakav način, uz ovakve informacije, bilo je u potpunosti nemoguće, odnosno, navigacija nije mogla funkcionirati. Međutim, iako ovakav način nije omogućavao navigaciju, u slučaju ometanja signalima čija je snaga na razini satelitskih signala, netočnosti koje su se pojavljivale nisu bile najvidljivije na AIS-u, pa je u tom slučaju vođenje navigacije bilo moguće. Pokušati normalno funkcionirati i voditi postupke navigacije u ovakvim okolnostima ne bi izazvalo ništa drugo osim velike rizičnosti. Dakle, može se zaključiti da i najmanje ometanje koje primi GPS u obliku signala i dalje ga prenosi na AIS sustav može izazvati onemogućenu navigaciju, ali i moguće katastrofe [13].

Zbog mogućnosti da se počinu velike štete i dovede u opasnost veliki broj brodova (prije svega se misli na veliki broj ljudskih žrtava), u SAD-a prodaja i korištenje ranije opisanih ometača je zakonom zabranjeno. Nadalje, Velika Britanija još uvijek nije donijela zabranu prodaje, a li je njihovo korištenje ilegalno, dok je u Australiji u zadnjih nekoliko godina uništen veliki broj ometača.

Korištenje ometača od strane krive osobe dovodi do stvaranja potencijalnog oružja. Takvo oružje izazvat će kaos na ekranima VTS službi ili bilo kojim drugim elektroničkim motrenjima, odašiljat će krive pakete informacija vezane za netočne kursove brodova, njihovu poziciju i brzinu. Kada se stvori takva kaotična slika, uljez kojemu je cilj poremetiti normalno funkcioniranje bit će gotovo u potpunosti neuočljiv. Kako bi se ovakvi scenariji izbjegli potrebno je unaprijed pripremiti rješenja koja nisu ovisna samo o sustavima satelitske navigaciji.

### 5.3.3. Otvorena komunikacija uz pomoć AIS sustava

Korištenje AIS sustava u svrhu otvorene komunikacije predstavlja ranjivost sustava zbog mogućnosti širenja informacija u različite destruktivne i protuzakonite svrhe. Unos podataka poput identiteta broda, njegove lokacije, kursa i brzine plovidbe, u AIS sustav moguće je vrlo lako promijeniti i/ili falsificirati. Kada se takvo nešto dogodi, pojavi se brod koji ima lažni identitet, u službi VTS neće biti sumnjiv, tako da je uljezima omogućen nesmetani rad i kretanje prema ostvarenju zamišljenog cilja. Približavanjem cilju, brod uljez gasi AIS sustav i nastavlja s planiranim protuzakonitim aktivnostima [13].

Javna mreža AIS sustava funkcionira na način da je otvorena za razmjenu bilo koje vrste podataka, tako da svatko s AIS sustavom može nesmetano doći do svih potrebnih podataka unutar dometa VHF-a. Podaci koje je moguće pročitati mogu biti zanimljivi u slučajevima piratskih napada, mogućim terorističkim napadima ili krijumčarenju. Bilo kakav podatak/informacija koja kruži javnom mrežom može biti iskorištena za protuzakonite radnje jer su podaci poput vrste broda, njegove tonaže, duljine, širine, namjene, kursa, brzine, odredišta, dostupni bilo kome. Kada skupe sve potrebne podatke znaju kada i na koji način izbjeći neželjene susrete (npr., s pomorskom policijom jer ona plovi bez uključenog AIS-a kako ih se ne bi identificiralo u slučajevima kada traže krijumčare i slično) [13].

Pokušajem da se što lakše omogući dostupnost svih potrebnih informacija, kako lukama i brodarima, tako i samim brodovima, stvoreni su različiti internetski portali koji svakodnevno, u realnom vremenu, prate pomorska područja i luke cijelog svijeta, odnosno, prikazuju brodske i lučke AIS simbole u realnom vremenu. Takvi portali osmišljeni su u svrhu dostupnosti korisnih informacija za brodske kompanije, međutim, postali su meta zloupotrebe i kršenja zakona. Pošto su dostupni svima i njihova namjena je široka, u novije vrijeme sve više su ciljana područja za pirate (npr., Somalijski pirati imaju uvid u cjelokupan promet Gibraltarom). Zbog problema koji izazivaju ovakvi portali sve češće se diskutira o mogućnosti njihovog uklanjanja i zabrane.

Iz svega navedenog može se zaključiti kako je korištenje automatske identifikacije brodova iznimno osjetljivo na napade. Stvara slabost brodu i pretvara ga u žrtvu, što za posljedice može imati jako široke razmjere koji se neće ticati samo jednog broda ili kompanije već će utjecati na nestabilnost na području nacionalne sigurnosti [13].

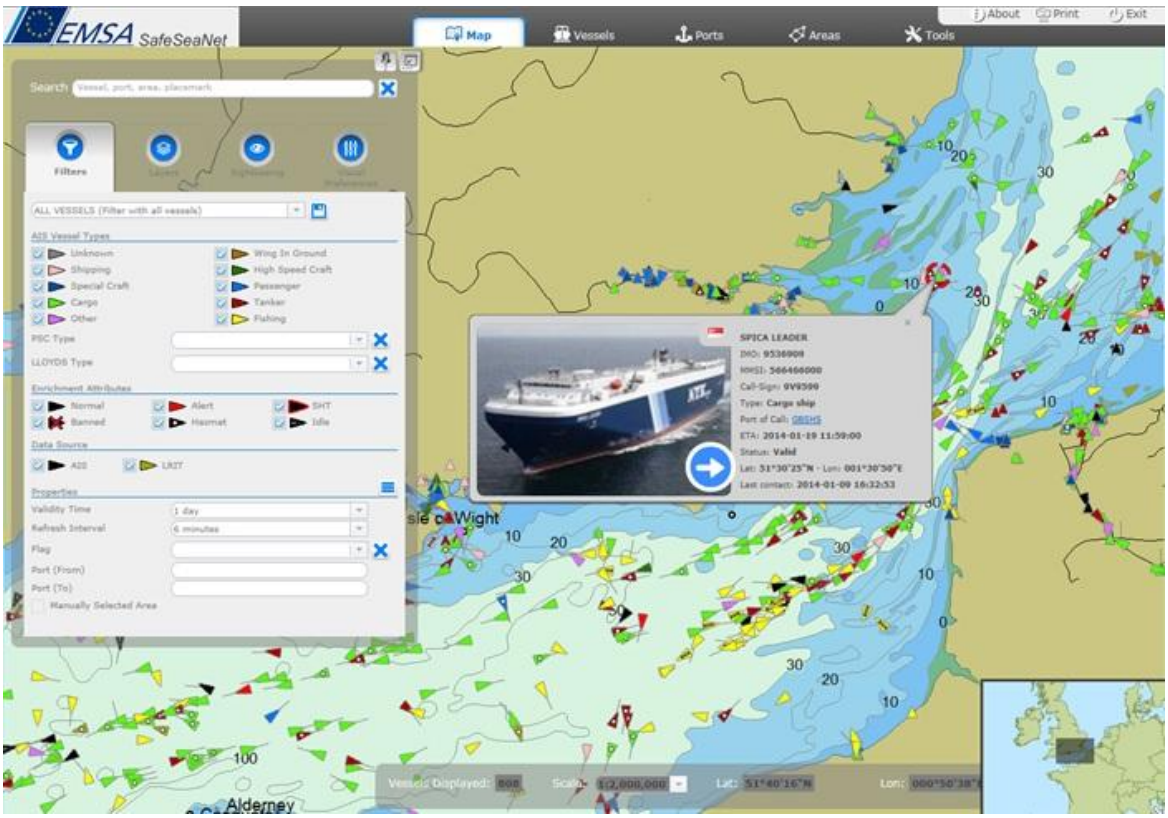
## 5.4. SAFESEANET

### 5.4.1. Opći koncept elektroničkih

SafeSeaNet je europska platforma za razmjenu pomorskih informacija, koji omogućuje primanje, razmjenu, pronalaženje i pohranjivanje svih onih informacija koje su potrebne za sigurnost plovidbe, sigurnosne zaštite u lukama i na moru, zatim zaštitu mora i morskog okoliša, kao i učinkovitost prilikom pomorskog prijevoza i pomorskog prometa. Ovaj sustav prije svega za svrhu ima razmjenu informacija elektroničkim putem u elektroničkom obliku između pomorskih vlasti država članica, a sve to obavlja se u skladu sa zakonodavstvom svih članica Europske Unije. Ima za glavni cilj pomoći prikupljati, širiti i usklađeno razmjenjivati pomorske podatke [20].

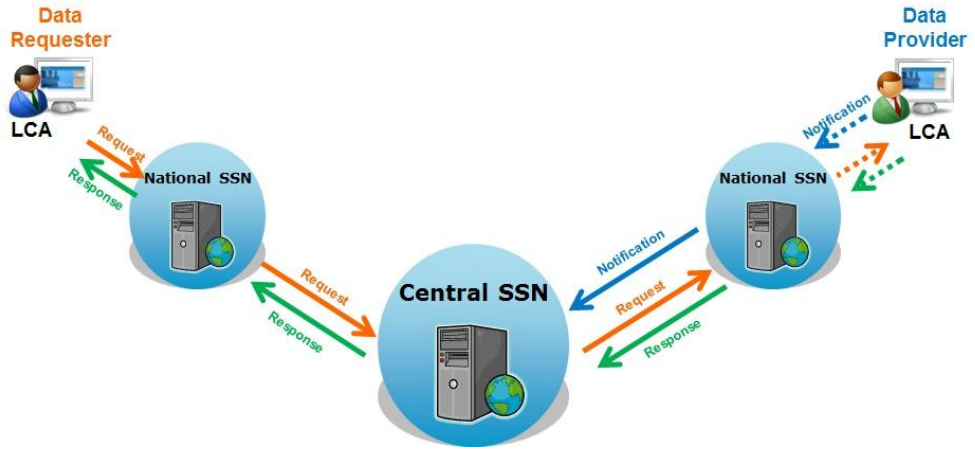
Ova platforma trenutno se provodi pod nadzorom Europske agencije za sigurnost plovidbe (EMSA). To omogućava državama članicama pružanje i primanje informacija o brodovima, rutama i opasnom teretu ukoliko se prevozi.

Ovakvoj mreži pomaže komunikacija između vlasti na lokalnoj i regionalnoj razini te središnjih vlasti, čime se doprinosi sprječavanje nesreća na moru, a samim time, onečišćenja mora, te se postiže provedba propisa pomorske sigurnosti. Prevencija nesreća i onečišćenja mora bitan je dio prometne politike Europske unije [20].




**Slika 7. SafeSeaNet grafičko sučelje [21]**

Od 1993. godine, Komisija je pokrenula više od 15 predloženih direktiva i propisa vezanih za sigurnost putničkih brodova, sprječavanje onečišćenja, nadzora državnih luka, itd. Provedba ovakvih propisa i direktiva uključuje prikupljanje i diseminaciju pomorskih podataka koje platforma SafeSeaNet podržava.




**Slika 8. SafeSeaNet razmjena informacija [21]**

SafeSeaNet se sastoji od mreža nacionalnih sustava SafeSeaNet-a u državama članicama i središnjeg čvorišnog SafeSeaNet sustava. Kao takav, SafeSeaNet implementira Direktiva 2010/65/EU Europskog parlamenta i Vijeća, te nudi nadzor pomorskog prometa i informacijskog sustava čitave zajednice.

### 5.4.2. Upravljanje, način rada i održavanje

#### 5.4.2.1. Nacionalni SafeSeaNet

U okviru nacionalnog sustava SafeSeaNet-a, državama članicama omogućuje se, korištenjem elektroničkih poruka, razmjena pomorskih informacija između korisnika u nadležnosti mjerodavnog nacionalnog tijela (u nastavku NCA). NCA jest odgovoran za sustav upravljanja na nacionalnoj osnovi, koja obuhvaća koordinaciju korisnika podataka i pružatelja podataka. Nadalje, osigurava određivanje oznaka UN LOCODES, kao i uspostavu i održavanje potrebne infrastrukture informacijske tehnologije. Ovaj, nacionalni sustav omogućuje međusobno povezivanje ovlaštenih korisnika koji su u nadležnosti NCA-a, a sve u svrhu kako bi se olakšala elektronička komunikacija [20, 23].

#### 5.4.2.2. Središnji sustav SafeSeaNet

Odgovornost za upravljanje središnjim SafeSeaNet sustavom odnosi se na Komisiju. Međutim, ona odlukom Europske agencije za pomorsku sigurnost surađuje s državama članicama te je kao takva odgovorna za sljedeće [20]:

- dokumentaciju i tehničku podršku sustava
- razvoj, rad i integraciju elektroničkih poruka i podataka
- održavanje sučelja središnjeg sustava
- zaštitu AIS sustava, odnosno podataka prikupljenih preko satelita...

Središnjeg SafeSeaNet sustav funkcionira kao čvorište, a na taj način međusobno povezuje sve nacionalne sustave i uspostavlja potrebnu infrastrukturu za informacijsku tehnologiju.

#### 5.4.2.3. Razmjena i dijeljenje podataka

Unutar sustava razmjene informacija SafeSeaNet-a primjenjuju se industrijski standardi. Međutim, moguća je interakcija i s javnim i privatnim sustavima koji se koriste prilikom izrade sustava ili prilikom pružanja i primanja informacija unutar okvira sustava SafeSeaNet.

Sve države članice ovog sustava, kao i Komisija, surađuju međusobno kako bi zajedničkim snagama ispitale izvedivost i razvoj funkcija koje će osigurati pružateljima podataka da ih dostave samo jednom. To se odnosi na zapovjednike, vlasnike brodova, brodare, zastupnike, krcatelje tereta i sva mjerodavna tijela. Kako bi se takav protok informacija osigurao potrebno je uzimati u obzir obveze koje su navedene u Direktivi 2010/65/EU, ali i svih drugih relevantnih zakonodavstava unutar Unije.

Razvoj i održavanje sučelja unutar sustava SafeSeaNet obavljaju sve države članice, a automatski prijenos podataka odvija se elektroničkim putem.
Radom sustava SafeSeaNet, postiže se cilj koji se odnosi na osiguravanje uspostave i funkcioniranja europskog pomorskog prometa bez prepreka [20].

#### 5.4.2.4. Sigurnost i prava pristupa

Kako bi se postupalo sigurno i temeljem zakonodavstva, bitno je navesti na koje se sve Direktive odnosi sigurnost i pravilno postupanje SafeSeaNet-a.

Zakonski okvir odnosi se na sljedeće [24]:

- *„Direktiva 2000/59/EZ Europskog parlamenta i Vijeća od 27. studenoga 2000. o lučkim uređajima za prihvat brodskog otpada i ostataka tereta, u pogledu njezina članka 12. stavka 3.*
- *Direktiva 2005/35/EZ Europskog parlamenta i Vijeća od 7. rujna 2005. o onečišćenju mora s brodova i uvođenju kazni za prekršaje, u pogledu njezina članka 10.*
- *Direktiva 2009/16/EZ Europskog parlamenta i Vijeća od 23. travnja 2009. o nadzoru države luke, u pogledu njezina članka 24.*
- *Direktiva 2010/65/EU Europskog parlamenta i Vijeća od 20. listopada 2010. o službenom postupku prijave za brodove koji dolaze u luke i/ili odlaze iz luka država članica, u mjeri u kojoj se primjenjuje njezin članak 6.“*

# 6. ANALIZA *CYBER* SIGURNOSTI U POMORSKOM SEKTORU

## 6.1. ENISA

Europska agencija za sigurnost mreža i podataka (eng. *European Network and Information Security Agency* – ENISA) ekspertni je centar za područje Europske unije (EU), njezinih država članica, građana i privatnog sektora za područje EU. Kao agencija koja radi na području EU ima zadaću da radi sa svim državama članicama kako bi se poboljšao razvoj, ali i kako bi prikupile dovoljan broj preporuka koje bi mogle koristiti na području poboljšanja informacijske sigurnosti. Agencija pomaže državama članicama u provedbi relevantnog zakonodavstva EU, te radi na poboljšanju otpornosti na prijetnje sigurnosti kritične europske informacijske i mrežne infrastrukture. U provedbi ovog plana, ENISA nastoji unaprijediti već postojeće znanje država članica podržavajući razvoj prekograničnih zajednica, te se na taj način zalaže za poboljšanje mrežne i informacijske sigurnosti na području cijele EU [10].

## 6.2. POMORSKI SEKTOR KAO KRITIČNA INFRASTRUKTURA

Kritičnost pomorskog sektora za zemlje članice, gospodarstvo i ekonomiju Europske unije jasno ilustriraju sljedeći podaci [10]:

- U Europi, 52% od prometa robe analizirajući podatke iz 2010. godine prevezeno je pomorskim putem, dok je deset godina prije promet robe korištenjem pomorskog transporta iznosio 45%. Ovakvo povećanje pomorskog prometa pokazatelj je njegove važnosti za naše društvo i gospodarstvo. Na temelju podataka iz Europske komisije, oko 90% vanjske trgovine Europske unije i više od 43% njene unutarnje trgovine odvija se putem pomorskog prometa. Tržište industrije i usluga pripada pomorskom sektoru, doprinosi između 3% i 5% od ukupnog bruto domaćeg proizvoda (BDP) EU, dok pomorske regije proizvedu i više od 40% BDP-a Europske unije. 22 države članice EU s granicama na moru upravljaju s više od 1 200 morskih luka koje podržavaju sve djelatnosti pomorskog sektora.
- Promet u tri glavne europske pomorske luke (Rotterdam, Hamburg i Antwerpen) u 2010. godini iznosio je 8% ukupnog obujma svjetskog prometa, što predstavlja više od 27,52 milijuna TEU-a. Osim toga, ove morske luke obrađuju više od 50% ukupne europske kontejnerske trgovine stranih brodova.

Europske gospodarstvo je, dakle, neupitno ovisno o kretanju tereta i putnika pomorskim prometom. S druge strane, pomorska se aktivnost sve više oslanja na informacijske komunikacije i tehnologije (eng. *Information Communication and Technology* - ICT) kojima će optimizirati svoje poslovanje u svim sektorima, a ne samo u sektoru prijevoza i transporta.

ICT se koristi kako bi se omogućilo što sigurnije obavljanje pomorskih operacija, od navigacije do pogona, od teretnog upravljanja do kontrole komunikacije u prometu, itd. Posljednjih godina, ubrzanim napredovanjem tehnologije, pokazalo se kako je *cyber* prijetnja rastući oblik prijetnje, ne bira već se širi na sve moguće sektore pomorstva. Poremećaji na području informacijskih komunikacija i tehnologije (ICT) ili nedostupnost informacija mogu izazvati katastrofalne posljedice. Stoga, postoji povećana potreba da se osigura ICT protiv *cyber* napada i poveća opreznost na nacionalnoj i europskoj razini. Osiguranje kritične infrastrukture pomorskog sektora sve više postaje prioritet za ključne europske dionike, uključujući Europsku komisiju, vlade država članica i glavnih aktera iz privatnog sektora.

## 6.3. KONTEKST POLITIKE U SLUČAJEVIMA KRITIČNE INFORMACIJSKE INFRASTRUKTURE

Kritične informacijske infrastrukture podržavaju vitalne usluge i prijevoz robe. Pod tim se podrazumijeva energija, transport, telekomunikacije, financijske usluge i druge, koje su toliko bitne da njihova nedostupnost može negativno utjecati na dobrobit naroda. Na taj način utječu direktno na nacionalnu sigurnost (ili u slučaju šireg područja EU, na sigurnost unije). Zbog svog značaja, zaštita kritične informacijske infrastrukture potrebna je za daljnje održavanje i poboljšanje dobrobiti europskog društva, ekonomije Europske unije i europskih građana. Dakle, ova tema je postala dio prostora za kreiranje politike na području Europske unije.

Europska komisija usvojila je priopćenje za poboljšanje zaštite Europske kritične infrastrukture (eng. *European Critical Infrastructure* – ECI) od terorizma putem Europskog programa za zaštitu kritične infrastrukture (eng. *European Programme for Critical Infrastructure Protection* – EPCIP) i Direktive o identifikaciji i označavanju europske kritične infrastrukture. 2009. godine Komisija je poslala drugo priopćenje Vijeću u kojem daje svoje mišljenje o tome kako su države članice mogle ojačati sigurnost i otpornost svojih kritičnih točaka i razvijati obranu od *cyber* napada. Cilj je potaknuti i poduprijeti razvoj visoke razine spremnosti, sigurnosti i otpornosti kako na nacionalnoj tako i na europskoj razini [10].

Digitalna agenda za područje Europe usvojena je u svibnju 2010. godine s naglaskom da se svi zainteresirani pridruže u borbi protiv novih i sofisticiranih oblika *cyber* napada i *cyber* kriminala.

ENISA želi razviti širenje suradnje i informacija između država članica i privatnog sektora na području *cyber* sigurnosti. Također, agencija u suradnji s Komisijom skreće pozornost na stalni rast broja, opsega, sofisticiranosti i potencijalnog prijetećeg utjecaja na kritičnu infrastrukturu. To unaprijed donosi postignuća i daljnje korake prema globalnoj *cyber* sigurnosti, strukturno rješavajući cyber opasnosti usmjeravajući ih prije svega na energetiku i promet.

Nadalje, ističe trend pomoću ICT-a za političke, ekonomske i vojne nadmoći, ali i nedovoljnu spremnost za rješavanje izazova koji se nalaze pred nama. Iako je cilj izgradnje koherentnog i kooperativnog pristupa unutar EU isti, potrebno je sve snage položiti u strategiju globalne koordinacije s ključnim partnerima, bilo da se radi o pojedinim narodima ili međunarodnim organizacijama.

Treba napomenuti da osim regulatornim naporima EU, broj zemalja članica također ulaže vlastite napore na ovom području (Francuska, Njemačka, Italija i Velika Britanija).

Osim gore navedenog, napore u svrhu poboljšanja sigurnosti poduzela je Opća uprava za mobilnost i promet (eng. *Directorate General for Mobility and Transport* – DG MOVE) uz pomoć Europske Agencije za sigurnost plovidbe (eng. *European Maritime Safety Agency* – EMSA) kako bi se olakšala sigurna razmjena podataka između pomorskih vlasti država članica, kroz SAFESEANET platformu [10].

## 6.4. NISKA SVIJEST I FOKUS NA POMORSKU CYBER SIGURNOST

Svijest o *cyber* sigurnosti nalazi se na vrlo niskoj razini, a što se tiče pomorskog sektora može se reći kako je ona gotovo nepostojeća. To se odnosi na sve slojeve društva, uključujući državna tijela, lučke vlasti i pomorske tvrtke. Jedan od razloga ovakve ne razvijene svijesti može biti to što postoji jako mali broj poznatih *cyber* sigurnosnih incidenata nastalih unutar nekog sektora, koji nisu stvorili dovoljnu medijsku izloženost. Međutim, bez publiciteta neki incidenti praktički kao da ne postoje.

Ova ukupna izrazito niska svijest predstavlja zabrinutost jer postoji povećana ovisnost o ICT svih ključnih igrača, procesa i aktivnosti unutar pomorskog sektora. Pokazatelji ove ovisnosti jesi veći broj ICT sustava implementacije u lukama diljem svijeta, a kontinuirani rast obujma i složenosti informacija i podataka koji se razmjenjuju povećava se iz dana u dan.

Nedovoljna svijest i fokus na *cyber* sigurnost rezultira niskom ažurnosti u pogledu promjena na neadekvatnim pripravnostima glede ovakve vrste opasnosti. Kao izravna posljedica, efekti potencijalnih *cyber* napada koji ciljaju pomorske ICT sustave mogu donijeti još više zla nego u nekim drugim sektorima, zbog slabe koordinacije odgovora i pitanja učinkovitosti.

Države članice bi trebale razmotriti načine na koje razvijati podizanje svijesti usmjerene na ključne dionike unutar pomorskog sektora. Sve to u svrhu kako bi se naglasila važnost adekvatne zaštite sredstava protiv *cyber* poremećaja imovine, povezane s pomorskim sektorom (brodovi, luke, komunikacijski sustavi, itd.).

ENISA posebnu pozornost daje uputama uz pomoć kojih bi se omogućilo lakše planiranje, organiziranje i izvođenje radnji na području *cyber* sigurnosti podizanjem svijesti o važnosti očuvanja pomorskog sektora. Kao smjernice prema kojima bi bilo dobro postupati ističu se [10]:

- planiranje i procjena
- izvršavanje i upravljanje
- ocjena i prilagodba.

Uz ova navedena postupanja, potrebno je na odgovarajući način ciljano usmjeravati i osposobljavati sve *cyber* sigurnosne aspekte, te razvijati relevantne aktere u pomorskom sektoru, od posade na brodovima do lučkih vlasti na kopnu.

Očekivano je kako će se ukupna stručnost u pomorskim sektorima s obzirom na *cyber* sigurnost povećati, a moći će se i uspješno primijeniti na iskustva akumulirana na nacionalnoj razini vezana za neku drugu vrstu opasnosti (telekomunikacije, energetika, financije, zdravstvo, itd.).

## 6.5. SLOŽENOST POMORSKOG ICT OKRUŽENJA

ICT sustavi podupiru pomorske operacije, od upravljanja brodom do svih oblika pomorske komunikacije. Ovakvi sustavi su općenito vrlo složeni i obuhvaćaju veliki broj vrlo specifičnih elemenata.

Brz razvoj tehnologije i težnja prema potpunoj automatizaciji u pomorskom sektoru ima, u većini slučajeva, smanjen fokus na sigurnosne značajke. Jedan relevantan primjer je kontinuirani rast broja lučkih operativnih ICT elemenata infrastrukture (npr. SCADA uređaj) spojenih na internet.

Ranjivost ovakvih uređaja stvara niz sigurnosnih propusta na ICT sustavima pomorskog sektora, te oni kao takvi mogu utjecati ne samo na usluge koje podržavaju ti sustavi, već i na čitavu infrastrukturu (baze podataka, sustave osjetljivih informacija, itd.).

Nadalje, uočeno je da postoji neadekvatna standardizacija kako bi se na sigurnost ICT sustava gledalo na odgovarajući način. ICT su iznimno kompleksni sustavi, te zahtijevaju veliki stupanj odgovornosti.

Bez dovoljno razvijene svijesti o ranjivosti tih sustava pojavljuju se problemi vezani za šire područje pomorskog sektora, a na taj način se indirektno utječe na moguće napade koji bi prouzrokovali nestabilnost na ovom području.

Povećana ovisnost o ICT sustavima u kombinaciji s operativnim procesima uključuje velik broj pomorskih dionika, što čini postojeće ICT okruženje posebno osjetljivim na *cyber* napade. Sve to bi moglo dovesti do ozbiljnih poremećaja u pružanju pomorske usluge. Primjer bi mogao biti postupak praćenja tereta i identifikacija tereta koja je u novije vrijeme sve više predmet *cyber* sigurnosnih incidenata koji su vidljivi u obliku napada ili kvarova na sustavima praćenja. Isto vrijedi i za automatizirani sustav rukovanja teretom u lukama. Krađa podataka, u kaznene svrhe, može se povećati kao izravna posljedica mjera nedovoljne *cyber* sigurnosti, ili ukoliko se mjere dovoljno ne podudaraju sa složenim ICT okruženjem [10].

## 6.6. PREPORUKE KAKO SPRIJEČITI MOGUĆE NAPADE

Bilo bi korisno za države članice da se dogovore o zajedničkoj strategiji i uspostave specijalizirane radne skupine za rad na razvoju detaljne *cyber* sigurnosti i na taj način stvore praksu za razvoj tehnologije i implementacije ICT sustava u pomorskom sektoru.

Takva radna skupina trebala bi sadržavati ključne dionike iz vlasti država članica koji imaju značajnu ovisnost o pomorskom sektoru, ali isto tako treba uključiti i predstavnike glavnih lučkih vlasti, brodskih poduzeća te relevantnih morskih infrastrukturnih usluga (telekomunikacijske infrastrukture, ICT hardware i software, SCADA sustave). Ovakva široka skupina međunarodnih dionika treba uključiti predstavnike Međunarodne pomorske organizacije (IMO), Europske agencije za sigurnost plovidbe (ENISA), kao i korisnike na području svih zajednica.

Detaljno usmjeravanje na *cyber* sigurnost specijalizirane skupine trebaju fokusirati na osiguravanje sigurnosnog dizajna za sve kritične komponente pomorskih sustava.

Ova strategija treba definirati pristup na temelju rizika kako bi se obuhvatilo cijelo pomorsko ICT okruženje, uz uzimanje u obzir postojećih standarda, politike i prakse koje se primjenjuju za kontekst pomorskih arhitektura.

Ovakav plan treba se baviti kako i minimumom mogućih rizika, tako i cjelokupnom ICT rizičnom području na nacionalnoj razini. Osim toga, treba uzeti u obzir i potrebu za prekograničnom razmjenom informacija i međudržavnom suradnjom [10].

### 6.6.1. Globalna razina ICT okruženja

Na globalnoj razini, relevantni dionici su razne međuvladine organizacije poput Međunarodne pomorske organizacije (IMO), Svjetske carinske organizacije (WCO) i ICC International Maritime Bureau (IMB), koja je specijalizirana podjela Međunarodne trgovačke komore (ICC). Osim toga, bitno je i spomenuti važnost Međunarodne pomorske sigurnosne korporacije (International Maritime Security Corporation (IMSC), koja je fokusirana na aktivnosti vezane za zaštitu brodova, posade na brodovima i tereta.

U slučaju nedostatka koordinacije između gore navedenih dionika i interesnih skupina na drugim razinama donosi velike razlike u načinu očuvanja pomorske sigurnosti.

Trenutna situacija implicira značajan rizik neadekvatne koordinacije koja bi mogla dovesti do neučinkovitosti kao što su praznine prilikom upravljanja ili preklapanja s problemima već viđenim na nižoj razini (nacionalnoj ili regionalnoj). Nadalje, to bi moglo donijeti velike razlike u načinu *cyber* sigurnosnih pitanja upućenih iz jednog akvatorija do drugog, između razina upravljanja [10].

### 6.6.2. Preporuke za djelovanje na globalnoj razini

Preporučeno je da se usklade međunarodne, regionalne i nacionalne politike vezane za pomorske (*cyber*) sigurnosne zahtjeve. Na ovoj razini bila bi poželjna platforma za detaljnu koordinaciju i konzultacije na čelu s Europskom komisijom, uz potporu zemalja članica. Kako bi se ovakva usklađivanja ostvarila, potrebni su napori koji zahtijevaju suradnju svih regionalnih i nacionalnih kreatora politike.

Na europskoj razini, trenutna pomorska politika otežava provođenje zakona koji bi osigurali minimalnu *cyber* sigurnosnu zaštitu.

Iako postoje agencije koje se bave pitanjima vezanim uz more, prema europskoj direktivi, sve države članice odgovorne su za zaštitu svoje pomorske ICT infrastrukture od mogućih *cyber* napada. Također, problem predstavlja i širina europske pomorske

infrastrukture, koja se proteže na različite pomorske zone, koje su predmet velikog broja različitih zakona i propisa.

Fragmentacija europskih pomorskih politika donosi teškoće za jasno definiranje odgovornosti koje bi trebalo poduzeti vezano za *cyber* sigurnost. Na temelju svega navedenog moguće je ostvariti tek minimalnu zaštitu.

Kako bi se ovakvo stanje promijenilo, potrebno je povezati vlasti unutar država članica kako bi se jasno definirale uloge upravljanja i odgovornosti u kriznim situacijama. To se uglavnom odnosi za područje Europe, ali takvo postupanje imalo bi utjecaj i na šire, globalno područje. Razmjena informacija i dobra koordinacija na europskoj platformi mogla bi koristiti i na globalnoj razini [10].

### 6.6.3. Poveznica između nacionalnog i regionalnog ICT okruženja

Tijekom posljednjeg desetljeća na području nacionalne razine primijećen je rastući trend privatizacije morskih luka i lučke infrastrukture. Danas, na području Europe, neke luke su djelomično privatizirane ili u koncesiji, dok su druge u procesu privatizacije. Ovakav trend privatizacije podiže nekoliko opravdanih zabrinutosti vezanih za sigurnosne uvjete propisane za ICT implementaciju i njene uporabe u lukama, zbog toga jer u tom slučaju sve ovisi o trenutnom vlasniku, a ne o samoj luci i njenoj zemlji u kojoj se nalazi. To dovodi u pitanje dodatne sigurnosne izazove zbog međunarodne dimenzije.

Osim navedenog pojavljuje se problem zbog velikog broja međunarodnih dobavljača za različite vrste usluga na području luka, pomorske infrastrukture ili pomorskom sektoru u cjelini. Takvi dobavljači najčešće su izvan granica Europske unije, a samim tim sve ranjivosti postaju izloženije.

Prilikom privatizacije, ICT i sigurnosni standardi postaju ovisni o vlasnicima, a oni uvelike ovise o svijesti vlasnika o mogućim sigurnosnim rizicima, ali i o njegovoj mogućnosti da zaštitu postavi na što veću razinu. To se prije svega shvaća kao financijski teret, što dovodi do problema nerazumijevanja i nezrelosti kad je u pitanju sigurnost i mogući sigurnosni rizici. Kako bi se neželjeni scenariji izbjegli, države članice trebale bi osigurati svojim agencijama i lučkim upravama sve potrebne uvjete (prije svega financijske), dobru koordinaciju između vlade i gospodarskih aktera i uključiti sve dionike iz pomorskog sektora. Na taj način bi se uvelike pridonijelo smanjenju napora i povećanju prioriteta za rješavanje problema *cyber* pomorske sigurnosti [10].

## 6.7. NEDOVOLJNA POSVEĆENOST CYBER SIGURNOSTI UNUTAR POMORSKIH REGULATIVA

Unutar pomorske regulacije, u kontekstu globalne, regionalne i nacionalne razine, još uvijek postoji vrlo malo pozornosti posvećene upravo elementima *cyber* sigurnosti. Većina sigurnosnih propisa sadrže samo one odredbe koje se odnose na pojmove fizičke sigurnosti ili sigurnosti općenito. Sve te odredbe ne smatraju *cyber* napade kao jedne od mogućih prijetnja uz pomoć kojih bi se ostvarile nezakonite radnje.

Organizacijski model što se tiče pomorskog *cyber* sigurnosnog aspekta gotovo pa je nepostojeći unutar zemalja članica Europske unije te zbog toga, ENISA preporučuje da države članice poduzmu odgovarajuće mjere kako bi se kako bi se dodatno razmatrale odredbe usmjerene prema ovakvoj vrsti sigurnosti u okvirima nacionalnih pomorskih regulativa.

Preporuke kako bi smjernice trebale izgledati za svaku zemlju članicu jesu sljedeće [10]:

- analiza postojećeg zakonodavstvenog okvira, kako bi se utvrdilo koliki su napori potrebni da se stvori napredak unutar *cyber* sigurnosnog zakonodavstva – bilo da se radi isključivo o pomorskom sektoru ili kao dio šireg nacionalnog okvira
- uspostava uloga i odgovornosti državnih tijela s obzirom na zaštitu ICT pomorskog sektora
- identifikacija ključnih dionika (javnih i privatnih) unutar pomorskog sektora za *cyber* aspekt
- potrebno je jasno definiranje mehanizme upravljanja, razmjene informacija i suradnje među tijelima državne uprave
- definirati nacionalne i međunarodne mahanizme suradnje
- usvajanje poboljšanih sigurnosnih standarda i postupaka prilikom *cyber* napada.

U tom smislu, očekuje se adekvatna suradnja između svih europskih država članica koje su uključene u pomorski sektor. Odnosno, poželjna bi bila suradnja vlasti na čelu s Europskom komisijom.

# 7. SVIJEST O POMORSKOM DOBRU U OKVIRU INFORMACIJSKE SIGURNOSTI

Pomorski informacijski sustavi pružaju operativnu superiornost unutar oružanih snaga i vladinih agencija prilikom prikupljanja vrijednih podataka potrebnih donositeljima odluka u gotovo realnom vremenu koji se odnose na pomorske sustave. U skladu s tim olakšava se planiranje pomorskih aktivnosti, ali i osigurava njihova sigurnija realizacija. Tim se postiže razvijanje svijesti o pomorskom okruženju, što dovodi do uspostavljanja zajedničkog razumijevanja određenih pomorskih situacija.

Jedan od problema razvijanja ovakvog zajedničkog sustava jest to što se većina platformi pomorskih informacijskih sustava nalazi unutar heterogenog područja. Dijeljenjem informacija između različitih sudionika unutar takvog heterogenog sustava postiže se jačanje svijesti, kako na lokalnog tako i na globalnoj razini, o važnosti zajedničkog rada pri donošenju odluka. Interoperabilnost otvara put do razmjene informacija u pomorskom okruženju gdje heterogeni sustavi postoje. U pomorskim sustavima koji se sastoje od heterogenih podsustava, razmjena informacija funkcionira na način da su podaci protokola i sučelja jako dobro definirani. Ovakvi, heterogeni sustavi svrstavaju se u različite razine sigurnosti, ovisno o vrstama informacija kojima se služe, tj., koje su u protoku. Za pomorske informacijske podsustave, uspostava informacijske sigurnosti veliki je izazov, a sve zbog protoka velikog broja informacija kojima je potrebna različita razina sigurnosti [16].

## 7.1. SIGURNOST INFORMACIJA U OKVIRU NATO-A ZA POMORSKO OKRUŽENJE

Sigurnost informacija je sastavljena od puno različitih perspektiva. Perspektive sigurnosti informacija, navedene su u nastavku [16]:

- fizička sigurnost kako bi ste zaštitili informacije
- prenosiva sigurnost (TRANSEC) za zaštitu osobnih ili privatnih podataka od nenamjernih elektromagnetskih emisija
- komunikacijska sigurnost (COMSEC) za zaštitu podataka na komunikacijskim uređajima
- mrežna sigurnost (NETSEC) za zaštitu podataka u mrežnoj domeni
- sigurnost pristupa i autentifikacije (COMPUSEC) za zaštitu od neovlaštenog pristupa.

Navedeni principi informacijske sigurnosti su oni koje treba slijediti za uspostavu visoke razine informacija sigurnosti.

Principi informacijske sigurnosti su detaljno objašnjeni i u sljedećim crticama [16]:

- Povjerljivost - zaštita informacija u elektronskim medijima od neovlaštenih ljudi i procesa se radi pomoću metoda kao što su šifriranje. U pomorskim informacijskim sustavima, povjerljivost se postiže korištenjem IP i niže rangiranim šifriranim uređajima.
- Integritet - metoda koja osigurava primanje podataka od strane prijamnika, kao što je predviđeno na komunikacijski medij pošiljatelja. U pomorskim informacijskim sustavima integritet se obično postiže *hash algoritmima*.
- Dostupnost - mjere opreza koje omogućuju ovlašteni pristup informacijama, od strane korisnika u svako doba kada je to potrebno. U pomorskim informacijskim sustavima, dostupnost postiže se neprekidnim radom i replikacijama na informacijskim sustavima. Sustavi moraju biti izgrađeni robusno i moraju biti zaštićeni s klasičnim sigurnosnim rješenjima putem odgovarajućih sigurnosnih propisa. Dostupnost je jedan od glavnih izazova kod sigurnosti informacija u pomorstvu. Dostupnost je diferencija zlonamjernih ponašanja (npr : *Denial of Service* (DoS) napada).
- Upravljanje - skladištenje svih elektroničkih incidenata u mreži za buduće analize. U pomorskim informacijski sustavima, koriste se alati za sustavsko upravljanja za otkrivanje anomalija i ispravljanje algoritama.
- Autentikacije i autorizacije - pravilno vrednovanje i pravo upravljanja korisnika za pristup izvorima mreže. U pomorskim informacijskim sistemima, autentikacija i autorizacija mehanizmom sigurnosnih šifri kao što je *One Time Password* (OTP).
- Pouzdanost - dosljednost očekivanog ponašanja i stvarni ishodi mrežnih usluga. U pomorskim informacijskim sustavima pouzdanost se postiže principima sistemskog dizajna.
- Bez rupa - potrebne mjere koje treba poduzeti da ne dođe do prekida komunikacije između pošiljatelja i primatelja. U pomorskim informacijskim sustavima to se postiže digitalnim potpisima.
- Kontrola pristupa - davanje prava pristupa za usluge mreže u informacijskom sustavu. U pomorskim informacijskim sustavima, kontrola pristupa se postiže fizičkom sigurnošću i pravilno regulirana tijela kao što su MAC i IP filtriranje.
- Sigurnost - fizička i tehnička rješenja koja treba poduzeti kako bi zaštitili podatke u sustavu. U pomorskim informacijskim sustavima, sigurnost se postiže regulacijom ljudskih čimbenika.

Sigurnosni principi su uvijek isti i jednako važni za svaki informacijski sustav, za heterogeni sustav pomorskog okruženja, svaki sistem zahtjeva različitu razinu sigurnosnog principa. U okruženjima poput vojnih tehnologija, povjerljivost i kontrola pristupa su par koraka naprijed, a u civilnim trgovačkim agencijama dostupnost i sigurnost dolaze u smanjenom stupnju.

Sve ove informacije sigurnosnih principa su uvrštene kao dio tradicionalnih informacijsko sigurnosnih tehnika. Tradicionalna rješenja su uglavnom softver i hardver rješenja koja se koriste za održavanje potrebnog stupnja sigurnosti među civilnim sustavima koji su raspoređeni na jednakim razinama sigurnosti.

Neki primjeri klasičnih sigurnosnih rješenja za šifriranje na razini komunikacije su [16]:

- firewall
- IDS/IPS
- VPN rješenja na razini mreže
- aplikacija firewall
- aplikacija IDS
- anti virus
- anti spam rješenja na razini aplikacije.

Ta rješenja nisu zadovoljavajuće kvalificirana za sigurnu razmjenu informacija između civilnih i vojnih informacijskih sustava u pomorskom okruženju, tako da su oni raspoređene na različitim razinama sigurnosti.

# 8. PROVEDENO ISTRAŽIVANJA SIGURNOSTI INFORMACIJA UNUTAR POMORSKIH SUSTAVA

## 8.1. ANALIZA ANKETE

Istraživanje koje je provedeno u svrhu prikupljanja informacija na temu *„Sigurnost informacija u domeni pomorstva“* provedeno je anketiranjem relevantnih pomorskih organizacija, tvrtki, udruženja i slično. Anketa se sastojala od 31 konkretnog pitanja, uglavnom uz već ponuđene odgovore ili kratko pisano odgovaranje, a provedena je na uzorku od 20 ispitanika. Anketirani ispitanici jesu iz sljedećih pomorskih djelatnosti:

- pomorske agencije za zapošljavanje
- charter agencije
- uslužne djelatnosti (lučka uprava)
- distribucija brodske opreme
- projektiranje brodova
- servis brodskih pogona i opreme
- brodogradnja.

Cilj ankete je prepoznavanje važnosti informacijski sustava za područje pomorskog sektora, te zaštite istih kako bi se spriječili mogući neželjeni događaji. Nadalje, anketom je utvrđena razina svijesti i informiranosti zaposlenika unutar pomorskog sektora, kao i njihov doživljaj pomorskog sektora kao kritičnog kada se radi o (ne)sigurnosti informacijskih sustava. S obzirom da je naglasak bio na anonimnost ankete, ne može se navesti konkretno ime svakog pojedinog ispitanika. Odgovore na pitanja u anketi isključivo su davale osobe odgovorne za informatiku i informacijske sustave, bilo da se radi o zaposleniku ili o vanjskom suradniku.

U daljem tekstu bit će prikazan originalan izgled ankete s pitanjima i ponuđenim odgovorima.

Prvo pitanje odnosi se na vrstu djelatnosti kojom se bavi poduzeće u kojem je ispitanik zaposlen.

1. **Kojom se djelatnošću bavi poduzeće u kojem ste zaposleni?**

Slijedeća dva pitanja odnose se na računalnu opremu kojem se koriste zaposlenici (hardver, softver) te prikazuju do koje mjere je razvijena svijest o napretku tehnologije i težnji

za unaprjeđenjem iste u vlastitom okruženju, a sve u svrhu boljeg očuvanja sigurnosti i zaštite imovine.

2. **Kolika je prosječna starost računalne opreme (hardvera) organizacije u kojoj radite?**
   a) manje od 1 godine
   b) od 1 do 3 godine
   c) od 3 do 5 godina
   d) od 5 do 10 godina
   e) više od 10 godina
3. **Kolika je prosječna starost računalnih programa (softvera) organizacije u kojoj radite?**
   a) manje od 1 godine
   b) od 1 do 3 godine
   c) od 3 do 5 godina
   d) od 5 do 10 godina
   e) više od 10 godina

Pitanja 4, 5, 6 i 7 daju uvid u učestalost korištenja informacijski sustava te njihovu zaštitu. Naglasak je stavljen na razmjenu poslovnih informacija koje je zbog vlastite sigurnosti i sigurnosti poslovanja potrebno pravovaljano zaštiti. I naposljetku, koliko ozbiljno shvaćaju potrebu za redovitim ažuriranjem zaštite informacija.

4. **Da li organizacija u kojoj radite razmjenjuje poslovne informacije elektroničkim putem? (s dobavljačima, kupcima, zaposlenicima...)**
5. **Da li organizacija u kojoj radite čuva poslovne informacije na računalima?**
6. ***Povezano s potvrdnim odgovorom iz prethodnog pitanja***
   **Na koji način se osigurava čuvanje ili zaštita tih podataka/informacija?**
   a) kopiranjem na neizbrisiv medij
   b) kopiranjem na backup server
   c) drugo
7. ***Povezano s odgovorom iz prethodnog pitanja***
   **Koliko često se to provodi?**
   a) dnevno
   b) tjedno

c) mjesečno

d) drugo

Pitanja koja obuhvaćaju od 8. do 17. dio su utvrđivanja ozbiljnosti, informiranosti i svijesti svih zaposlenika što su to informacijski sustavi i njihova sigurnost. Dakle, u tim pitanjima doznajemo na koji način funkcioniraju unutar poduzeća, postoje li pravilnici za postupanja, kako s opremom tako i u slučajevima zaštite od neovlaštenog korištenja.

Nadalje, ponuđeno je konkretno pitanje o slučaju prijevare, pronevjere, zatajenja ili bilo kojeg drugog oblika zloupotrebe poslovnih informacija. Posljednja grupa pitanja vezana je uz postojanje strateških planova koji se tiču razvoja, rizika i oporavka u slučaju mogućih napada.

8. **Da li u organizaciji u kojoj radite postoji pravilnik o korištenju informatičke opreme i informacijskih sustava?**
9. **Da li u organizaciji u kojoj radite postoje pravila i postupci o zaštiti i čuvanju podataka od neovlaštenog korištenja?**
10. ***Povezano s odgovorom i prethodnog pitanja***

    **Na koji način se čuvaju poslovne informacije?**

    a) antivirusni program

    b) firewall

    c) kriptiranje podataka

    d) digitalni potpis

    e) lozinke

    f) biometrija

    g) zatvoreni tip mreže

    h) fizička zaštita

    i) drugo
11. **Da li se u organizaciji u kojoj radite ikad dogodio slučaj prijevare, pronevjere, zatajenja ili bilo koji drugi oblik namjerne zloupotrebe poslovnih informacija?**
12. ***Povezano s potvrdnim odgovorom iz prethodnog pitanja***

    **U kojem obliku?**

    a) računalna prijevara

    b) računalno krivotvorenje

    c) oštećenje računalnih podataka ili programa

d) računalna sabotaža

e) neovlašten pristup

f) neovlašteno prisluškivanje

g) neovlaštena reprodukcija zaštićenih računalnih programa

h) neovlašteno korištenje zaštićenih računalnih programa

i) drugo

13. **Provjera ranjivosti IT sustava u Vašoj organizaciji provodi se:**

a) jednom mjesečno

b) polugodišnje

c) kvartalno

d) jednom godišnje

e) prema potrebi (rijetko, kada se nađe vremena za provjeru)

f) nakon svake izmjene sklopovlja i/ili programa

g) nakon promjere administratora i/ili sistem inženjera

h) ne provodi se

14. **Da li organizacija u kojoj radite ima strateški plan razvoja informacijskih sustava?**
15. **Da li u organizaciji u kojoj radite postoji podjela odgovornosti vezano za informacijske sustave?**
16. **Da li u organizaciji u kojoj radite postoji svjesnost o mogućim rizicima upotrebe informacijskih sustava?**
17. **Da li postoji plan oporavka informacijskog sustava u slučaju nastanka nepovoljnog događaja?**

Sljedeća dva pitanja odnose se na termin *cyber*. Ispituje se poznavanje pojma te se dolazi do saznanja je li softverska oprema kojom se služe opremljena svim potrebnim kako bi se prevenirali mogući napadi.

18. **Da li vam je poznat pojam *cyber* sigurnosti?**
19. **Da li softverska oprema koju koristite sadrži programe ili aplikacije koji služe prevenciji *cyber* napada?**

Pitanja 20 do 24 dio su internog ponašanja poduzeća, zadovoljstva ili nezadovoljstva zaposlenika kada je riječ o informacijskoj sigurnosti i njihova ocjena iste u sustavu u kojem rade.

20. **Tko provodi nadzor nad informacijskim sustavima u organizaciji u kojoj radite?**

a) interna kontrola

b) odjel interne revizije

c) odjel kontrolinga

d) posebno oformljen odjel za informacijske sustave

e) drugo

**21. S kojom tvrdnjom biste ocjenili sigurnost informacijskog sustava organizacije u kojoj radite?**

a) apsolutno zadovoljan/zadovoljna

b) zadovoljan/zadovoljna

c) srednje zadovoljan/zadovoljna

d) nezadovoljan/nezadovoljna

e) apsolutno nezadovoljan/nezadovoljna

f) drugo

**22.** ***Povezano s odgovorom iz prethodnog pitanja***

**Koji je razlog takve ocjene?**

a) nedovoljna edukacija za rad za sustavom i opremom

b) kvalitetna oprema

c) nedovoljna razumljivost sustava i opreme

d) svijest svih zaposlenih

e) novac

f) uređena sigurnosna politika

g) drugo

**23. Na koji način se provodi autentifikacija i autorizacija korisnika koji pristupa informacijskom sustavu i informacijama?**

a) obveznim upisivanjem korisničkog imena i lozinke

b) posjedovanjem identifikacijskih kartica

c) fizičkom karakteristikom korisnika (glas, otisak prsta...)

d) fizičkom zaštitom (zaključavanje prostorije, video nadzor)

e) drugo

**24. U slučaju upotrebe lozinki pri zaštiti informacija, koliko često se provodi njihova modifikacija?**

a) tjedno

b) mjesečno

c) tromjesečno

d) polugodišnje

e) godišnje

f) samo u slučaju nastanka štetnog događaja

g) nikad

h) drugo

Sljedeća tri pitanja (25., 26., 27.) isključivo se odnose na tehnički dio. Odnosno, na način zaštite koja se koristi u organizacija koja je ispitivana. Isto tako pokušava se dobiti uvid u informiranost o modernim načinima zaštite sustava.

**25. Koristite li u svom poslovanju bežičnu mrežu?**

**26.** ***Povezano s potvrdnim odgovorom na prethodno pitanje***

**Koju razinu zaštite koristite kod bežične mreže?**

a) WEP

b) WPA

c) WPA2

e) bez zaštite

**27. Koristite li neki od navedena dva alata koja služe za sigurnosnu provjeru bežičnih mreža?**

a) Kismet

b)NetStumbler

c) ništa od navedenog

Od 28. pitanja pa sve do kraja saznaje se kolika je razina informiranosti pomorskih organizacija na području politike, strategija Europske Unije, te modernih platforma kojima Europa i zapad u zadnje vrijeme teže kako bi što više poboljšali svoju sigurnost i spriječili moguće neželjene događaje.

**28. Da li ste čuli za ENISA centar (European Network and Information Security Agency)?**

**29.** ***Povezano s potvrdnim odgovorom iz prethodnog pitanja***

**Da li znate koja je njihova politika i kako se provodi?**

**30. Smatrate li pomorski sektor kritičnom infrastrukturom kada je u pitanju sigurnost informacija?**

**31. Da li vam je poznata platforma SafeSeaNet?**

## 8.2. ANALIZA REZULTATA

Kako je već navedeno, anketa je provedena na uzorku od 20 ispitanika, tj., 20 različitih sustava koji se bave jednom ili više djelatnosti u području pomorskog sektora. Rezultati prikazuju realno stanje što se tiče postupanja kada je riječ o informacijskoj sigurnosti, razini informiranosti i educiranosti zaposlenika, a pogotovo onih koji su zaduženi za sigurnost informacija i IT sustave općenito, zatim svijest o mogućim neželjenim događajima ili zloupotrebi informacija relevantnih za normalno poslovno funkcioniranje. Osim navedenog, ispitana je i informiranost o pomorskom sektoru kao dijelu kritične infrastrukture kada govorimo o sigurnosti informacijskih sustava, ali i informiranost o politici zaštite informacija i korištenja novih, suvremenih metoda sigurnosti unutar pomorskih sustava.

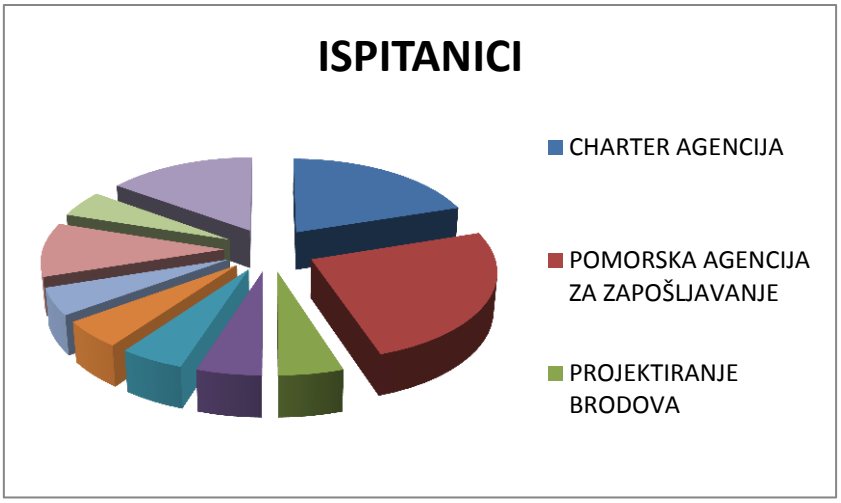
Rezultati dobiveni analiziranom anketom, u nastavku rada su prikazani su korištenjem tablica i grafikona. Tablica 1. prikazuje anketirani uzorak od 20 ispitanih prema vrsti njihove poslovne funkcije unutar pomorskog sektora. Svi ispitanici su sa područja Republike Hrvatske i isključivo vezano za pomorske sustava.

**Tablica 1. Uzorak na kojem je prevedeno istraživanja**

| ANKETIRANI UZORAK | BROJ UZORAKA | POSTOTAK |
|---|---|---|
| CHARTER AGENCIJA | 4 | 0,20 |
| POMORSKA AGENCIJA ZA ZAPOŠLJAVANJE | 5 | 0,25 |
| PROJEKTIRANJE BRODOVA | 1 | 0,05 |
| SERVIS BRODSKIH POGONA I OPREME | 1 | 0,05 |
| PROIZVODNJA | 1 | 0,05 |
| USLUŽNA DJELATNOST; LUČKA UPRAVA | 1 | 0,05 |
| ORGANIZACIJA POSLODAVACA | 1 | 0,05 |
| DISTRIBUCIJA BRODSKE OPREME | 2 | 0,10 |
| CHARTER, SERVISIRANJE I PRODAJA | 1 | 0,05 |
| BRODOGRADNJA | 3 | 0,15 |
| | **20** | |

Iz grafikona 1. vidljivo je kako najveći broj onih koji su se odazvali anketi jest vezan za sektor pomorskih agencija koje se bave zapošljavanjem. Zatim charter agencije te sektor brodogradnje (škverovi i mala brodogradilišta).

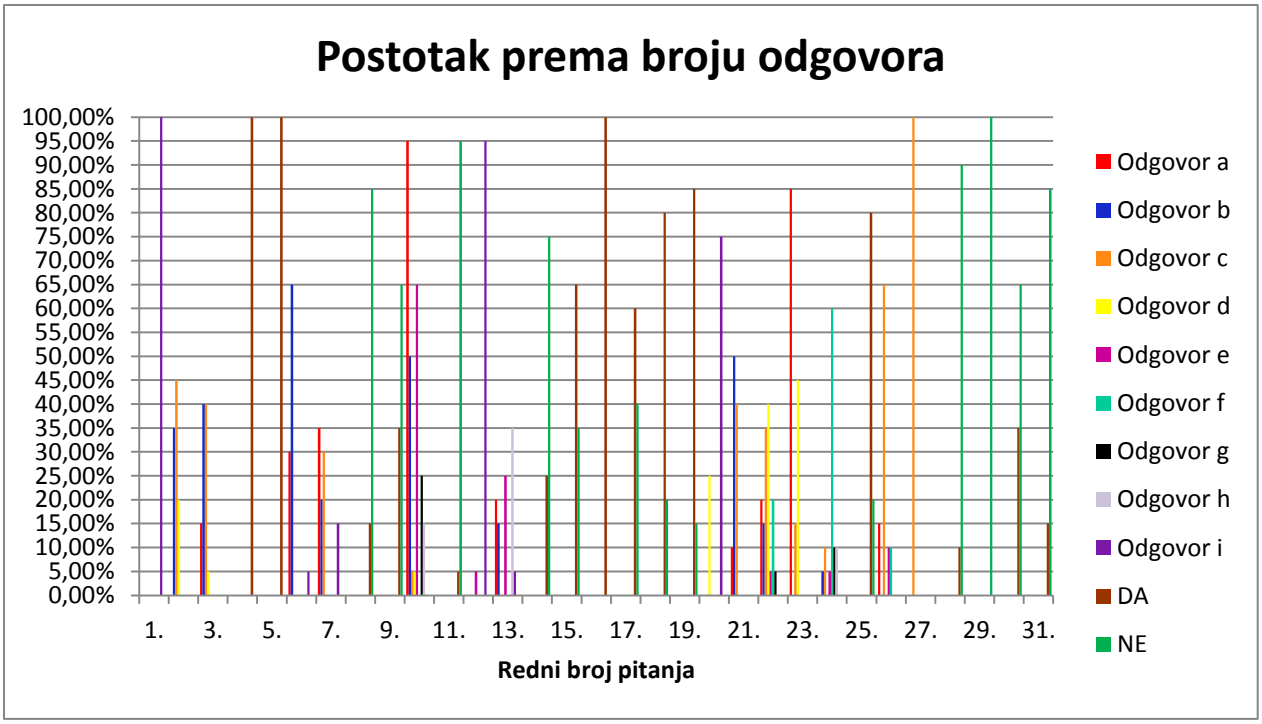
Tablica 2. prikazuje postotak prema broju odgovora na sva postavljena pitanja, koja su u prethodnom poglavlju navedena i opisana.




**Grafikon 1. Zastupljenost prema odazivu anketiranih**

**Tablica 2. Odgovori na sva ponuđena pitanja prema postotku**

| a | b | c | d | e | f | g | h | i | DA | NE |
|---|---|---|---|---|---|---|---|---|---|---|
| 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 100% | 0% | 0% |
| 0% | 35% | 45% | 20% | 0% | 0% | 0% | 0% | 0% | 0% | 0% |
| 15% | 40% | 40% | 5% | 0% | 0% | 0% | 0% | 0% | 0% | 0% |
| 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 100% | 0% |
| 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 100% | 0% |
| 30% | 65% | 0% | 0% | 0% | 0% | 0% | 0% | 5% | 0% | 0% |
| 35% | 20% | 30% | 0% | 0% | 0% | 0% | 0% | 15% | 0% | 0% |
| 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 15% | 85% |
| 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 35% | 65% |
| 95% | 50% | 5% | 5% | 65% | 0% | 25% | 15% | 0% | 0% | 0% |
| 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 5% | 95% |
| 0% | 0% | 0% | 0% | 5% | 0% | 0% | 0% | 95% | 0% | 0% |
| 20% | 15% | 0% | 0% | 25% | 0% | 0% | 35% | 5% | 0% | 0% |
| 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 25% | 75% |
| 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 65% | 35% |
| 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 100% | 0% |
| 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 60% | 40% |
| 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 80% | 20% |
| 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 85% | 15% |
| 0% | 0% | 0% | 25% | 0% | 0% | 0% | 0% | 75% | 0% | 0% |
| 10% | 50% | 40% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% |
| 20% | 15% | 35% | 40% | 5% | 20% | 5% | 0% | 0% | 0% | 0% |
| 85% | 0% | 15% | 45% | 0% | 0% | 0% | 0% | 0% | 0% | 0% |
| 0% | 5% | 10% | 0% | 5% | 60% | 10% | 10% | 0% | 0% | 0% |
| 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 80% | 20% |
| 15% | 0% | 65% | 0% | 10% | 10% | 0% | 0% | 0% | 0% | 0% |
| 0% | 0% | 100% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% |
| 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 10% | 90% |
| 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 100% |
| 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 35% | 65% |
| 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 15% | 85% |




**Grafikon 2. Postotak svih odgovorenih pitanja**

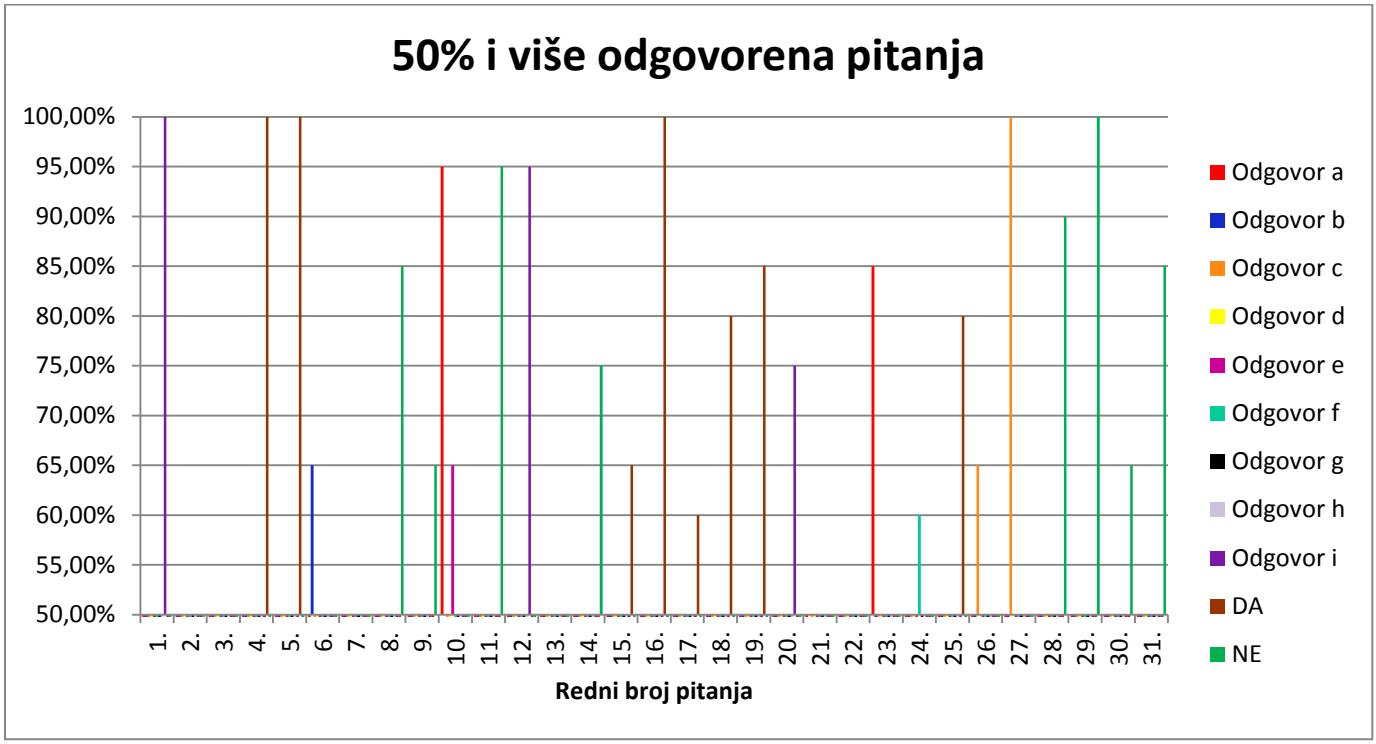
Grafikon 2. predstavlja prikaz svih ponuđenih odgovora te učestalosti odabira istih. Odnosi se na kompletnu anketu. Dakle, svih 31 pitanje uz moguće odgovore.

Tablica broj 3 prikazuje odgovore prema rednom broju pitanja s naglaskom na odgovore preko 50 %. Odgovori koji imaju 50 i više % označeni su „*bold*“.

**Tablica 3. Odgovori koji su zastupljeni s 50 % i više**

| | a | b | c | e | f | i | DA | NE |
|---|---|---|---|---|---|---|---|---|
| **1** | 0% | 0% | 0% | 0% | 0% | **100%** | 0% | 0% |
| **4** | 0% | 0% | 0% | 0% | 0% | 0% | **100%** | 0% |
| **5** | 0% | 0% | 0% | 0% | 0% | 0% | **100%** | 0% |
| **6** | 30% | **65%** | 0% | 0% | 0% | 5% | 0% | 0% |
| **8** | 0% | 0% | 0% | 0% | 0% | 0% | 15% | **85%** |
| **9** | 0% | 0% | 0% | 0% | 0% | 0% | 35% | **65%** |
| **10** | **95%** | **50%** | 5% | **65%** | 0% | 0% | 0% | 0% |
| **11** | 0% | 0% | 0% | 0% | 0% | 0% | 5% | **95%** |
| **12** | 0% | 0% | 0% | 5% | 0% | **95%** | 0% | 0% |
| **14** | 0% | 0% | 0% | 0% | 0% | 0% | 25% | **75%** |
| **15** | 0% | 0% | 0% | 0% | 0% | 0% | **65%** | 35% |
| **16** | 0% | 0% | 0% | 0% | 0% | 0% | **100%** | 0% |
| **17** | 0% | 0% | 0% | 0% | 0% | 0% | **60%** | 40% |
| **18** | 0% | 0% | 0% | 0% | 0% | 0% | **80%** | 20% |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **19** | 0% | 0% | 0% | 0% | 0% | 0% | **85%** | 15% |
| **20** | 0% | 0% | 0% | 0% | 0% | **75%** | 0% | 0% |
| **23** | **85%** | 0% | 15% | 0% | 0% | 0% | 0% | 0% |
| **24** | 0% | 5% | 10% | 5% | **60%** | 0% | 0% | 0% |
| **25** | 0% | 0% | 0% | 0% | 0% | 0% | **80%** | 20% |
| **26** | 15% | 0% | **65%** | 10% | 10% | 0% | 0% | 0% |
| **27** | 0% | 0% | **100%** | 0% | 0% | 0% | 0% | 0% |
| **28** | 0% | 0% | 0% | 0% | 0% | 0% | 10% | **90%** |
| **29** | 0% | 0% | 0% | 0% | 0% | 0% | 0% | **100%** |
| **30** | 0% | 0% | 0% | 0% | 0% | 0% | 35% | **65%** |
| **31** | 0% | 0% | 0% | 0% | 0% | 0% | 15% | **85%** |
| | 2 | 1 | 2 | 1 | 1 | 3 | 8 | 8 |




**Grafikon 3. Pitanja s 50 % i više odgovora**

Kako je u prethodnom tekstu navedeno, ovaj grafikon predstavlja rezultate gore prikazane tablice u kojoj se navode svi oni odgovori koje su ispitanici odabirali u slučajevi od 50 % ili većem postotku. Sva ta pitanja i odgovori nadalje će biti objašnjena.

Pitanje broj 4. glasi:

**Da li organizacija u kojoj radite razmjenjuje poslovne informacije elektroničkim putem? (s dobavljačima, kupcima, zaposlenicima...)**

Svih 20 ispitanika, odnosno 100 % je odgovorilo s DA. Tim ukazuju kako je svijest o širenju informacija u poslovnom svijetu, putem elektroničkih uređaja od presudne važnosti kada je riječ o brzini, točnosti i efikasnosti poslovanja.

Pitanja broj 5. i 6. glase:

**Da li organizacija u kojoj radite čuva poslovne informacije na računalima?**

Kao i kod prethodnog pitanja, svih 20 ispitanika dalo je pozitivan odgovor, tj., DA. Dakle, 100 % ispitanih unutar svog poslovnog sustava čuva poslovne informacije na računalima.

**Na koji način se osigurava čuvanje ili zaštita tih podataka/informacija?**

65 % ispitanika odgovorilo je kako svoje poslovne informacije koje pohranjuje na računala čuva na način da se one kopiraju na backup servere.

Pitanja 8., 9. i 10 glase:

**Da li u organizaciji u kojoj radite postoji pravilnik o korištenju informatičke opreme i informacijskih sustava?**

**Da li u organizaciji u kojoj radite postoje pravila i postupci o zaštiti i čuvanju podataka od neovlaštenog korištenja?**

85 % i 65% ispitanika na navedene pitanja odgovorilo je negativno, odnosno NE. To nam daje za naslutiti kako nemaju dovoljno razvijenu svijest o negativnim utjecajima korištenju informacijskih sustava, ali i kako još uvijek nisu dovoljno educirani.

**Na koji način se čuvaju poslovne informacije?**

Kada je riječ o načinima čuvanja informacija, još uvijek se koristite „najprimitivniji“ i najjednostavniji načini poput antivirusnih programa. 95 % ispitanika upravo taj odgovor je navelo kao način čuvanja, a njih 65 % još navodi i korištenje lozinki. Gotovo kod svih ispitanika koriste se oba načina, a ne isključivo jedan.

Zaključuje se kako nemaju dovoljnu educiranosti, kao ni informiranost. Osim toga, ne teže poboljšanju načina zaštite informacija upravo zbog nerazvijene svijesti o postojanju opasnosti.

Pitanja 11. i 12. Glase:

**Da li se u organizaciji u kojoj radite ikad dogodio slučaj prijevare, pronevjere, zatajenja ili bilo koji drugi oblik namjerne zloupotrebe poslovnih informacija?**

**U kojem obliku?**

Na jedanaesto pitanje koje se tiče konkretnih slučajeva prijevare, pronevjere, zatajenja ili nekog drugog oblika namjerne zloupotrebe poslovnih informacija, od 20 ispitanika, njih 19 je odgovorilo negativno, odnosno, 95 % je odgovorilo s NE. Što bi značilo kako ne postojanje svijesti o mogućim opasnostima izazvano je upravo ovim. Dakle, ne postojanje realne opasnosti dovodi do ne postojanja svijesti o njenoj mogućnosti.

Ispitanik koji je potvrdno odgovorio na jedanaesto pitanje, konkretan odgovor na dvanaesto nije dao. Odgovor je zaokružen pod *i) drugo,* te temeljem toga ne možemo znati o kakvoj se vrsti neželjenog događaja radilo.

Pitanja 14. i 15. glase:

**Da li organizacija u kojoj radite ima strateški plan razvoja informacijskih sustava?**

**Da li u organizaciji u kojoj radite postoji podjela odgovornosti vezano za informacijske sustave?**

Čak 75 % ispitanika na četrnaesto pitanje odgovorilo je negativno, NE. Iz toga je vidljivo kako ne poznaju termin *„strateški plan“* te kako ne smatraju da je njegovo postojanje od presudne važnosti kada je riječ o zaštiti i sigurnosti informacija. Vjeruje se kako strateški planovi poslovanja postoje, inače u suprotnom poduzeća ne bi dugo opstala. Međutim, informacijski sustavi su u velikoj mjeri zanemareni.

Nadalje, odgovornost vezana za informacijske sustave ipak postoji, ali opet ne u onolikoj mjeri u kolikoj je potrebna. Svega 65 % ispitanika na petnaesto pitanje odgovorilo je potvrdno, DA na postavljeno pitanje. Ta podjela odgovornosti u prvom se redu odnosi na hijerarhiju raspolaganja informacija i vođenja brige o istima.

Pitanja 16. i 17. glase:

**Da li u organizaciji u kojoj radite postoji svjesnost o mogućim rizicima upotrebe informacijskih sustava?**

**Da li postoji plan oporavka informacijskog sustava u slučaju nastanka nepovoljnog događaja?**

Ova dva pitanja odnose se na svijest zaposlenika o mogućim rizicima i planovima u slučaju neželjenih događaja. Svi ispitanici na šesnaesto pitanje odgovaraju pozitivno, 100 % odgovora DA. Dakle, svijest postoji, ali planovi i postupci u slučajevima nepovoljnih zbivanja ipak gotovo pa i ne postoje. To je vidljivo iz slijedećeg pitanja, gdje tek 60 % odgovara s DA.

Sljedeća pitanja vezana su uz *cyber* sigurnost. 18. i 19. pitanje glase:

**Da li vam je poznat pojam *cyber* sigurnosti?**

**Da li softverska oprema koju koristite sadrži programe ili aplikacije koji služe prevenciji *cyber* napada?**

Odgovorima od 80 % i 85 % s DA zaključujemo kako ipak postoji određena doza informiranosti o „suvremenim“ načinima izvora opasnosti i napada. Ispitanici posjeduju određene oblike zaštite od vanjskih i/ili unutarnjih utjecaja na svoje sustave, u oblicima programskih podrški ili aplikacija sve više dostupnih na tržištu.

Sljedeća skupina pitanja isključivo su vezana uz načine zaštite bežičnih mreža. 25., 26. i 27. pitanje glase:

**Koristite li u svom poslovanju bežičnu mrežu?**

**Koju razinu zaštite koristite kod bežične mreže?**

**Koristite li neki od navedena dva alata koja služe za sigurnosnu provjeru bežičnih mreža?**

80 % ispitanika odgovara potvrdno na pitanje koriste li u svom poslovanju bežičnu mrežu, odnosno s DA.

65 % bežičnu mrežu koju koristi u svom poslovanju zaštićuje koristeći razinu WPA2 (što se još uvijek uglavnom koristi u svim oblicima zaštite bežičnih mreža).

Kada im je postavljeno pitanje o poznavanju nekih novijih oblika zaštite, odnosno alata koji se koriste za zaštitu bežićnih mreža, oni odgovaraju negativno. 100 % ispitanika odabire odgovor *c) ništa od navedenog*. Informiranost na informatičkoj i informacijskoj razini, pomorskog sektora Republike Hrvatske nije na zavidnoj razini u odnosu na druge obalne države Europske Unije.

Od 28. pitanja pa do kraja ankete (pitanje 31.) ispitanicima je postavljen niz pitanja vezanih za provođenje politike EU-e na području zaštite informacija, kako općenito tako i isključivo za pomorski sektor.

Pitanja glase:

**Da li ste čuli za ENISA centar (European Network and Information Security Agency)?**

**Da li znate koja je njihova politika i kako se provodi?**

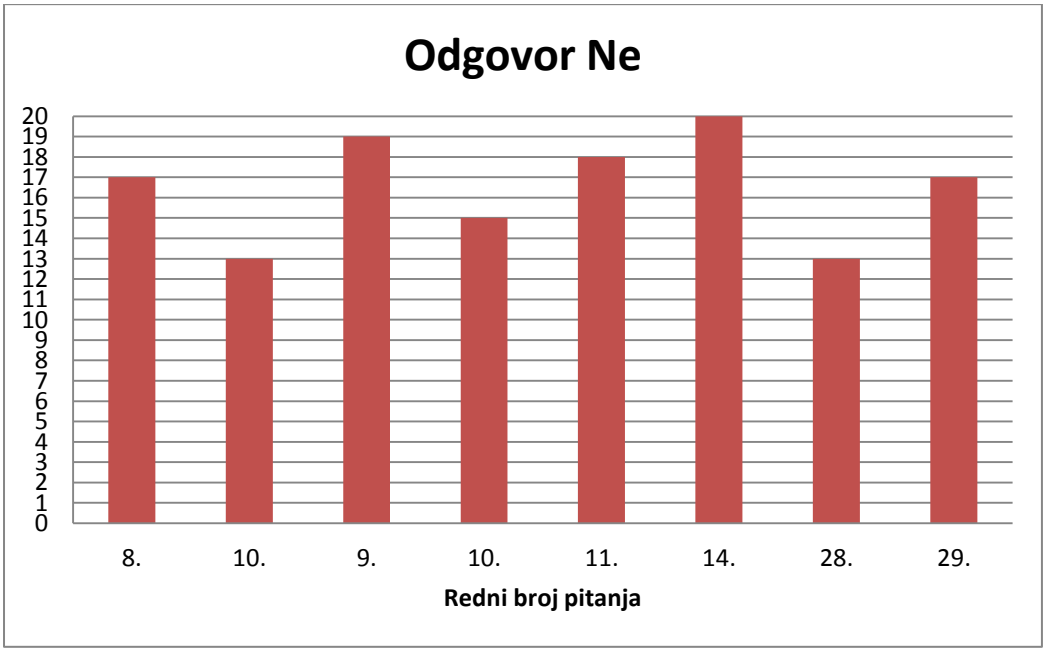
**Smatrate li pomorski sektor kritičnom infrastrukturom kada je u pitanju sigurnost informacija?**

**Da li vam je poznata platforma SafeSeaNet?**

Za ENISA centar (*European Network and Information Security Agency*) 90 % ispitanika uopće nije čulo (samo jedan ispitanik odgovorio je potvrdno), dok je svih 100 % odgovorilo NE na pitanje o njihovoj politici i na koji se način provodi.

Smatraju li pomorski sektor kritičnom infrastrukturom ispitanici odgovaraju pomalo iznenađujuće. Čak 65 % smatra kako pomorski sektor nije kritična infrastruktura. Za takav odgovor zaslužna je neinformiranost i needuciranost zaposlenika cjelokupnog pomorskog sektora Republike Hrvatske.

Također, u okviru ENISA centra postoji relativno nova platforma tzv., SafeSeaNet kojem u zadnje vrijeme teži sve više članica EU-e (naravno, obalnih država). Međutim, pomorski sektor ispitivan u ovom istraživanju odgovora s 85 % NE, odnosno njih 85 % nikada nije čulo za istoimenu platformu.




**Grafikon 4. Specifičan odgovor „NE“**

Grafikon 4. Prikazuje najspecifičniji odgovor NE, tj., odgovor koji je u najvećem postotku zastupljen. Prikazuje broj pitanja na koja je specifičan odgovor zastupljen s preko 50 % (konkretno odgovor „NE“). Pitanja se odnose na sljedeće:

**9. Da li u organizaciji u kojoj radite postoje pravila i postupci o zaštiti i čuvanju podataka od neovlaštenog korištenja?**

**11. Da li se u organizaciji u kojoj radite ikad dogodio slučaj prijevare, pronevjere, zatajenja ili bilo koji drugi oblik namjerne zloupotrebe poslovnih informacija?**

**14. Da li organizacija u kojoj radite ima strateški plan razvoja informacijskih sustava?**

**28. Da li ste čuli za ENISA centar (European Network and Information Security Agency)?**

Upravo na ova pitanja postoji preko 50 % odgovora NE, što bi značilo kako postupanja u slučaju zaštite i čuvanja podataka nisu na zavidnoj razini ili uopće ne postoje, ali i kako ne postoji svijest o mogućim zloupotrebama poslovnih informacija. Pitanje broj 11 samo je prikaz trenutnog stanja, što nikako ne znači apsolutnu i potpunu sigurnost. Posljednja dva pitanja daju naslutiti kako planovi u slučajevima potrebe ne postoje, ali i kako se kadar slabo i gotovo uopće ne educira ni informira o novostima na području informacija i njihove sigurnosti.

# 9. ZAKLJUČAK

Istraživanje koje je provedeno u svrhu pronalaženja relevantnih podataka za izradu diplomskog rada daje uvid u trenutno stanje na području informacijske sigurnosti u sektoru pomorstva. Iz rezultata, vidljivo je kako je upravo pomorski sektor izložen velikom broju prijetnji i opasnosti. Međutim, sudionici unutar sektora pomorstva još uvijek nisu dovoljno svjesni izazova koji se pred njih stavljaju, a sve u svrhu zaštite sigurnosti vlastitih informacijskih sustava.

Informacijski sustavi, kao dio osnovnog komunikacijskog kanala postali su ranjiva točka i meta nekih novih oblika napada, ali i modernog ratovanja (terorizma). Kako bi se svijest o tome proširila, potrebno je da cjelokupna zajednica (poslovni subjekti, privatni subjekti, država, međunarodna zajednica) utječe na obnavljanje znanja i stvaranje novih kako bi se neželjeni događaji mogli prevenirati ili spriječiti.

Na temelju svega navedenog, može se zaključiti kako situacija na području sigurnosti i zaštite informacijski sustava unutar pomorskih sustava, nikako nije na zavidnoj razini. Još uvijek se uvelike odskače od europskog i svjetskog prosjeka što je definitivno upozorenje za nužne promijene.

Kako bi se situacija što više poboljšala potrebno je uvesti nove načine unutar educiranja kadra zaduženog upravo za sektor informacijske sigurnosti i sigurnosti informacijskih sustava unutar pomorskih sustava, ali i stvoriti svijest o mogućim opasnostima koje nas okružuju ili su u našoj neposrednoj blizini. Prije svega, potrebno je početi promatrati pomorski sektor kao dio kritične infrastrukture preko koje, u bliskoj budućnosti mogu dolaziti prijetnje ili u najgorem slučaju napadi. Međutim, u tom trenutku više neće biti vremena za edukacije i buđenje svijesti, tada ne preostaje ništa drugo nego djelovati.

# LITERATURA


[1] Kasum, Josip *„Radioslužba za pomorce“*, Hrvatski hidrografski institut, Split, 2012.

[2] Hadjina, Nikola *„Zaštita i sigurnost informacijskih sustava“*, nastavni materijali sa zbirkom zadataka, Sveučilište u Zagrebu, Fakultet elektrotehnike i računarstva, zavod za primjenjeno računarstvo, Zagreb, 2009.

[3] CARNet, Hrvatske akademska i istraživačka mreža *„DdoS napad“*, Nacionalno središte za sigurnost računalnih mreža i sustava (CARNet CERT), Laboratorij za sustave i signale pri Zavodu za elektorničke sustave i obradu informacija Fakulteta elektortehnike i računarstva, Sveučilište u Zagrebu, 2008.

[4] CARNet, Hrvatske akademska i istraživačka mreža *„WPA2 zaštita“*, Nacionalno središte za sigurnost računalnih mreža i sustava (CARNet CERT), Laboratorij za sustave i signale pri Zavodu za elektorničke sustave i obradu informacija Fakulteta elektortehnike i računarstva, Sveučilište u Zagrebu, 2009.

[5] CARNet, Hrvatske akademska i istraživačka mreža *„Europska politika mrežne i informacijske sigurnosti“*, Nacionalno središte za sigurnost računalnih mreža i sustava (CARNet CERT), Laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradu informacija Fakulteta elektrotehnike i računarstva, Sveučilište u Zagrebu, 2005.

[6] CARNet, Hrvatske akademska i istraživačka mreža *„Upravljanje lozinkama“*, Nacionalno središte za sigurnost računalnih mreža i sustava (CARNet CERT), Laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradu informacija Fakulteta elektrotehnike i računarstva, Sveučilište u Zagrebu, 2009.

[7] CARNet, Hrvatske akademska i istraživačka mreža *„Fizička zaštita informacijskih sustava“*, Nacionalno središte za sigurnost računalnih mreža i sustava (CARNet CERT), Laboratorij za sustave i signale pri Zavodu za elektorničke sustave i obradu informacija Fakulteta elektortehnike i računarstva, Sveučilište u Zagrebu, 2010.

[8] Ministarstvo pomorstva, prometa i infrastrukture *„Pravilnik o ispravama, dokumentima i podacima o pomorskom prometu, te o njihovoj dostavi, prikupljanju i razmjeni, kao i o načinu i uvjetima izdavanja odobrenja za slobodan promet s obalom“*, Zagreb, 2013.

[9] Badurina, Egon *„Automatski identifikacijski sustav (AIS)“*, stručni rad, Rijeka, 2003.

[10] ENISA – European Network and Information Security Agency *„Analysis of Cyber Security Aspects in the maritime Sector“*, Heraklion, Grčka, 2011.

[11] Europska komisija; Komunikacija komisije europskom parlamentu i vijeću *„Bolja informiranost o stanju poboljšanom suradnjom tijela za pomorski nadzor: sljedeći koraci u okviru Zajedničkog okruženja za razmjenu informacija za pomorsko dobro“*, Bruxelles, 2014.

[12] Sviličić, Boris, Kraš, Antun *„Zaštita privatnosti računalnog sustava“*, stručni rad, Pomorski fakultet u Rijeci, 2005.

[13] http://obris.org/hrvatska/meki-napadi-na-ais-moguci-i-na-jadranu/

[14] http://www.egmdss.com/en/

[15] http://www.nato.int/docu/review/2010/Maritime_Security/Safe_Mediterranean/CR/index.htm

[16] http://www.nato.int/cps/en/natohq/topics_70759.htm?selectedLocale=en

[17] http://ec.europa.eu/transport/media/infringements/proceedings/maritime_en.htm

[18] http://www.zakon.hr/z/504/Zakon-o-sigurnosnoj-za%C5%A1titi-pomorskih-brodova-i-luka

[19] http://narodne-novine.nn.hr/clanci/sluzbeni/2013_06_79_1640.html

[20] http://ec.europa.eu/idabc/en/document/2282/5926.html

[21] http://www.emsa.europa.eu/ssn-main/ssn-how-it-works.html

[22] https://en.wikipedia.org/wiki/Wireless_security

[23] http://os2.zemris.fer.hr/ns/wireless/2004_maric/tkip.htm

[24] http://www.eskema.eu/defaultinfo.aspx?topicid=37&index=3

[25] http://www.safety4sea.com/safeseanet-upgrade-to-bring-enhanced-information-exchange/

[26] https://hr.wikipedia.org/wiki/Antivirusni_program

[27] https://hr.wikipedia.org/wiki/Sigurnosna_stijena

[28] https://mssis.volpe.dot.gov/Main/

[29] https://www.volpe.dot.gov/infrastructure-systems-and-technology/situational-awareness-and-logistics/maritime-safety-and

[30] https://de.wikipedia.org/wiki/Maritime_Rescue_Coordination_Centre

[31] https://sysportal.carnet.hr/node/342

[32] http://znatko.com/1501/sto-je-sigurnosni-protokol

# POPIS SLIKA

Slika 1. Shematski prikaz TKIP protokola [4], preuzeto 25.5.2016. ..... 17
Slika 2. Shematski prikaz autentikacije WPA2 kroz proces razmjene tajnih ključeva unutar četiri koraka [4], preuzeto 25.5.2016. ..... 18
Slika 3. AES kriptiranje kod WPA2 protokola [4], preuzeto 25.5.2016. ..... 19
Slika 4. Prikaz korištenja RADIUS mrežnog protokola [4], preuzeto 25.5.2016. ..... 20
Slika 5. Prikaz na koji način radi AIS (*Automatic Indentification System*) mreža [13], preuzeto 10.3.2016. ..... 23
Slika 6. Primjer korištenja AIS sustava u RH za putnički brod „Zadar“, 21.4.2014. godine [33], preuzeto 10.3.2016. ..... 24
Slika 7. SafeSeaNet grafičko sučelje [21], preuzeto 2.4.2016. ..... 28
Slika 8. SafeSeaNet razmjena informacija [21], preuzeto 2.4.2016. ..... 29

# POPIS TABLICA

Tablica 1. Uzorak na kojem je prevedeno istraživanj ..... 49
Tablica 2. Odgovori na sva ponuđena pitanja prema postotku ..... 50
Tablica 3. Odgovori koji su zastupljeni s 50 % i više ..... 51
Izvor: Izradila studentica prema rezultatima vlastitog istraživanja

# POPIS GRAFIKONA

Grafikon 1. Zastupljenost prema odazivu anketiranih ..... 50
Grafikon 2. Postotak svih odgovorenih pitanja ..... 51
Grafikon 3. Pitanja s 50 % i više odgovora ..... 52
Grafikon 4. Specifičan odgovor „NE“ ..... 56

Izvor: Izradila studentica prema rezultatima vlastitog istraživanja

## POPIS KRATICA

MRCC (*Maritime Rescue and Coordination Centres*)

GMDSS (*Global Maritime Distress and Safety System*)

MSSIS (*Maritime Safety and Security Information System*)

CRS (*Coast Radio Station*)

SAR (*Search and Rescue*)

Mbps (*Megabite per second*)

MRCC (*Maritime Rescue Co-ordination Centres*)

MRSC (*Maritime Rescu Sub Centre*)

MSI (*Maritime Safety Information*)

LAN (*Local Area Network*)

WAN *(Wide Area Network*)

PAN (*Personal Area Network*)

Gbps (*Giga bit per second)*

MAN (*Metropolitan Area Networks*)

## PRIMJER ANKETE

1. **Kojom se djelatnošću bavi poduzeće u kojem ste zaposleni?**

   _____

2. **Kolika je prosječna starost računalne opreme (hardvera) organizacije u kojoj radite?**

   a) manje od 1 godine

   b) od 1 do 3 godine

   c) od 3 do 5 godina

   d) od 5 do 10 godina

   e) više od 10 godina

3. **Kolika je prosječna starost računalnih programa (softvera) organizacije u kojoj radite?**

   a) manje od 1 godine

   b) od 1 do 3 godine

   c) od 3 do 5 godina

   d) od 5 do 10 godina

   e) više od 10 godina

4. **Da li organizacija u kojoj radite razmjenjuje poslovne informacije elektroničkim putem? (s dobavljačima, kupcima, zaposlenicima...)**

   DA NE

5. **Da li organizacija u kojoj radite čuva poslovne informacije na računalima?**

   DA NE

6. ***Povezano s potvrdnim odgovorom iz prethodnog pitanja***

   **Na koji način se osigurava čuvanje ili zaštita tih podataka/informacija?**

   a) kopiranjem na neizbrisiv medij

   b) kopiranjem na backup server

   c) drugo _____

**7.** ***Povezano s odgovorom iz prethodnog pitanja***

**Koliko često se to provodi?**

a) dnevno

b) tjedno

c) mjesečno

d) drugo _____

**8. Da li u organizaciji u kojoj radite postoji pravilnik o korištenju informatičke opreme i informacijskih sustava?**

DA NE

**9. Da li u organizaciji u kojoj radite postoje pravila i postupci o zaštiti i čuvanju podataka od neovlaštenog korištenja?**

DA NE

**10.** ***Povezano s odgovorom i prethodnog pitanja***

**Na koji način se čuvaju poslovne informacije?**

a) antivirusni program

b) firewall

c) kriptiranje podataka

d) digitalni potpis

e) lozinke

f) biometrija

g) zatvoreni tip mreže

h) fizička zaštita

i) drugo _____

**11. Da li se u organizaciji u kojoj radite ikad dogodio slučaj prijevare, pronevjere, zatajenja ili bilo koji drugi oblik namjerne zloupotrebe poslovnih informacija?**

DA NE

**12.** ***Povezano s potvrdnim odgovorom iz prethodnog pitanja***

**U kojem obliku?**

a) računalna prijevara

b) računalno krivotvorenje

c) oštećenje računalnih podataka ili programa

d) računalna sabotaža

e) neovlašten pristup

f) neovlašteno prisluškivanje

g) neovlaštena reprodukcija zaštićenih računalnih programa

h) neovlašteno korištenje zaštićenih računalnih programa

i) drugo _____

**13. Provjera ranjivosti IT sustava u Vašoj organizaciji provodi se:**

a) jednom mjesečno

b) polugodišnje

c) kvartalno

d) jednom godišnje

e) prema potrebi (rijetko, kada se nađe vremena za provjeru)

f) nakon svake izmjene sklopovlja i/ili programa

g) nakon promjere administratora i/ili sistem inženjera

h) ne provodi se

**14. Da li organizacija u kojoj radite ima strateški plan razvoja informacijskih sustava?** DA NE

**15. Da li u organizaciji u kojoj radite postoji podjela odgovornosti vezano za informacijske sustave?** DA NE

**16. Da li u organizaciji u kojoj radite postoji svjesnost o mogućim rizicima upotrebe informacijskih sustava?** DA NE

**17. Da li postoji plan oporavka informacijskog sustava u slučaju nastanka nepovoljnog događaja?** DA NE

**18. Da li vam je poznat pojam *cyber* sigurnosti?** DA NE

**19. Da li softverska oprema koju koristite sadrži programe ili aplikacije koji služe prevenciji *cyber* napada?** DA NE

**20. Tko provodi nadzor nad informacijskim sustavima u organizaciji u kojoj radite?**

a) interna kontrola

b) odjel interne revizije

c) odjel kontrolinga

d) posebno oformljen odjel za informacijske sustave

e) drugo_____

**21. S kojom tvrdnjom biste ocjenili sigurnost informacijskog sustava organizacije u kojoj radite?**

a) apsolutno zadovoljan/zadovoljna

b) zadovoljan/zadovoljna

c) srednje zadovoljan/zadovoljna

d) nezadovoljan/nezadovoljna

e) apsolutno nezadovoljan/nezadovoljna

f) drugo _____

**22.** ***Povezano s odgovorom iz prethodnog pitanja***

**Koji je razlog takve ocjene?**

a) nedovoljna edukacija za rad za sustavom i opremom

b) kvalitetna oprema

c) nedovoljna razumljivost sustava i opreme

d) svijest svih zaposlenih

e) novac

f) uređena sigurnosna politika

g) drugo _____

**23. Na koji način se provodi autentifikacija i autorizacija korisnika koji pristupa informacijskom sustavu i informacijama?**

a) obveznim upisivanjem korisničkog imena i lozinke

b) posjedovanjem identifikacijskih kartica

c) fizičkom karakteristikom korisnika (glas, otisak prsta...)

d) fizičkom zaštitom (zaključavanje prostorije, video nadzor)

e) drugo_____

**24. U slučaju upotrebe lozinki pri zaštiti informacija, koliko često se provodi njihova modifikacija?**

a) tjedno

b) mjesečno

c) tromjesečno

d) polugodišnje

e) godišnje

f) samo u slučaju nastanka štetnog događaja

g) nikad

h) drugo_____

**25. Koristite li u svom poslovanju bežićnu mrežu?**

DA NE

**26.** ***Povezano s potvrdnim odgovorom na prethodno pitanje***

**Koju razinu zaštite koristite kod bežićne mreže?**

a) WEP

b) WPA

c) WPA2

e) bez zaštite

**27. Koristite li neki od navedena dva alata koja služe za sigurnosnu provjeru bežićnih mreža?**

a) Kismet

b)NetStumbler

c) ništa od navedenog

**28. Da li ste čuli za ENISA centar (European Network and Information Security Agency)?**

DA NE

**29.** ***Povezano s potvrdnim odgovorom iz prethodnog pitanja***

**Da li znate koja je njihova politika i kako se provodi?**

DA NE

**30. Smatrate li pomorski sektor kritičnom infrastrukturom kada je u pitanju sigurnost informacija?**

DA NE

**31. Da li vam je poznata platforma SafeSeaNet?**

DA NE