Procjena rizika u softverskom inžinjerstvu

Pezić, Ivan

Undergraduate thesis / Završni rad

2019

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Pula / Sveučilište Jurja Dobrile u Puli**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:137:791334

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-09-03**

Repository / Repozitorij:

Digital Repository Juraj Dobrila University of Pula

Sveučilište Jurja Dobrile u Puli

Fakultet informatike

IVAN PEZIĆ

PROCJENA RIZIKA U SOFTVERSKOM INŽENJERSTVU

Završni rad

Pula, rujan 2019.

Sveučilište Jurja Dobrile u Puli

Fakultet informatike

IVAN PEZIĆ

PROCJENA RIZIKA U SOFTVERSKOM INŽENJERSTVU

Završni rad

JMBAG: 0303046260; redoviti student

Studijski smjer: Informatika

Predmet: Softversko inženjerstvo

Mentor: doc. dr. sc. Tihomir Orehovački

Pula, rujan 2019.

IZJAVA O AKADEMSKOJ ČESTITOSTI

Ja, dolje potpisani Ivan Pezić, kandidat za prvostupnika informatike ovime izjavljujem da je ovaj Završni rad rezultat isključivo mojega vlastitog rada, da se temelji na mojim istraživanjima te da se oslanja na objavljenu literaturu kao što to pokazuju korištene bilješke i bibliografija. Izjavljujem da niti jedan dio Završnog rada nije napisan na nedozvoljen način, odnosno da je prepisan iz kojega necitiranog rada, te da ikoji dio rada krši bilo čija autorska prava. Izjavljujem, također, da nijedan dio rada nije iskorišten za koji drugi rad pri bilo kojoj drugoj visokoškolskoj, znanstvenoj ili radnoj ustanovi.

Student

_____

U Puli, _____, 2019. godine

IZJAVA

o korištenju autorskog djela

Ja, Ivan Pezić dajem odobrenje Sveučilištu Jurja Dobrile u Puli, kao nositelju prava iskorištavanja, da moj završni rad pod nazivom „Procjena rizika u Softverskom inženjerstvu“ koristi na način da gore navedeno autorsko djelo, kao cjeloviti tekst trajno objavi u javnoj internetskoj bazi Sveučilišne knjižnice Sveučilišta Jurja Dobrile u Puli te kopira u javnu internetsku bazu završnih radova Nacionalne i sveučilišne knjižnice (stavljanje na raspolaganje javnosti), sve u skladu s Zakonom o autorskom pravu i drugim srodnim pravima i dobrom akademskom praksom, a radi promicanja otvorenoga, slobodnoga pristupa znanstvenim informacijama. Za korištenje autorskog djela na gore navedeni način ne potražujem naknadu.

U Puli, _____ (datum)

Potpis

_____

SADRŽAJ

1.UVOD 1
2. O PROGRAMSKOM INŽENJERSTVU 3
2.1. DEFINICIJE I OBILJEŽJA PROGRAMSKOG INŽENJERSTVA 3
2.2. SOFTVERSKI PROJEKT 4
2.3. PROGRAMSKI PROCES 7
3. O RIZICIMA 10
3.1. DEFINICIJE, VRSTE I MODELI RIZIKA 10
3.2. UPRAVLJANJE RIZICIMA 12
3.3. ANALIZA RIZIKA 15
4. RIZIK U PROGRAMSKOM INŽENJERSTVU 16
4.1. POJAM I DEFINICIJA RIZIKA U PROGRAMSKOM INŽENJERSTVU 17
4.2. UPRAVLJANJE RIZICIMA U PROGRAMSKOM INŽENJERSTVU 18
4.3. PROCJENA RIZIKA 20
4.3.1. Karakterizacija informacijskog sustava 22
4.3.2. Identificiranje prijetnji 22
4.3.3. Analiza kontrola 23
4.3.4. Određivanje vjerojatnosti 23
4.3.5. Analiza utjecaja 23
4.3.6. Preporuka kontrola 24
4.3.7.Dokumentiranje rezultata 24
4.4. PRAKTIČNO POJAŠNJENJE 24
5. ZAKLJUČAK 29
LITERATURA 31
POPIS SLIKA 33
POPIS TABLICA 34
SAŽETAK 35
SUMMARY 36

1.UVOD

Tema ovoga rada tiče se procjene rizika u softverskom inženjerstvu. U današnjici se sve češće koristi i naziv programskog inženjerstva, koji implicira značenje ovoga termina. Iz danoga naziva može se ukazati na to da je riječ o kompleksnom procesu izrade softvera ili programa (programskog rješenja). Kompleksnost u tom terminu podrazumijeva fazni tijek procesa, ali i primjenu raznih metoda, instrumenata i ostaloga.

Kao i u svakom procesu, posebno onom kompleksnijem, postoje brojne prijetnje i mogući problemi, a tada je zapravo riječ o rizicima koji se javljaju prije, tijekom i nakon njegove izvedbe. Jednako je i na primjeru osmišljavanja konkretnog programa, odnosno tijeka njegove izvedbe od inovativne ideje do komercijalizacije.

Sam proces izvedbe nekog programa, koji čini krovni proces programskog inženjerstva zahtijeva opsežna znanja i vještine, kao i iskustvo. Jednako je i po pitanju procjene rizika u ovome procesu, a s obzirom na složenost i zahtjevnost problematike, može se tvrditi kako je ispravnije govoriti o pojmu upravljanja rizicima u programskom inženjerstvu.

Cilj ovoga rada je objasniti značenje programskog inženjerstva, ukazati na specifičnosti i ulogu softvera u današnjici, kao i obraditi tijek predmetnog procesa. Time se stvara osnova za provedbu konkretnog istraživanja, koje čini središnju problematiku rada, kao i samu svrhu.

Svrha pisanja rada na ovu temu je spoznati rizike u programskom inženjerstvu, kao i specificirati pristup i značajke procjene rizika, odnosno shvatiti važnost procesa njihova upravljanja.

Rad je strukturiran kroz tri poglavlja, uvod i zaključak. Prvo poglavlje obrađuje osnovne teorijske odlike, a u svezi programskog inženjerstva kao interdisciplinarnog znanstvenog područja. U okviru njega izvode se osnovne definicije, pobliže se obrađuje softverski projekt te se razmatra proces njegove izvedbe. Sljedeće poglavlje

posvećeno je problematici rizika. U okviru njega daju se definicije, vrste i modeli rizika, pristupa se mjerenjima istih, kao i kategorizaciji te stavu prema riziku. Posljednje poglavlje rada specificira središnju tematiku, odnosno obrađuje rizike u programskom inženjerstvu. Osim definicija, ono daje pregled razloga neuspjeha te razmatra proces upravljanja rizicima u programskom inženjerstvu.

2. O PROGRAMSKOM INŽENJERSTVU

Softversko ili programsko inženjerstvo u domaćoj i inozemnoj literaturi, znanstvenim krugovima, ali i javnosti definira se na brojne načine. Iako je riječ o relativno novom znanstvenom području, kao i samo terminu, činjenica je da o ovoj temi postoji opsežna literatura, što potvrđuje interes brojnih dionika za njezinim izučavanjem. Tome treba pridodati i intenzivni razvoj programskog inženjerstva, od prvotnih razdoblja pojave pa sve do danas, a nastavak ovoga trenda izvjestan je i u budućnosti.

Smatra se kako je programsko inženjerstvo jedna od aktualnijih tema u suvremeno doba, a što se potvrđuje činjenicom da je riječ o podržavajućem procesu današnjeg poslovanja, ali i svakodnevnog života globalnog društva. Naime, današnje poslovanje i način života uvelike se razlikuju od onog nekadašnjeg, a što je najvećim dijelom uzrokovano napretkom tehnologije, koja danas zadire u sve sfere života. Njezino učinkovito i efikasno funkcioniranje u domeni je ovog znanstvenog područja i procesa, što dodatno potvrđuje njegov značaj i ulogu.

Sukladno navedenome, u ovome poglavlju razrađuje se osnovna teorijska pozadina u svezi predmetnog pojma, ali i povezanih termina. Time se daje opsežniji uvod u sami rad, odnosno ističu se definicije i obilježja programskog inženjerstva, softverskog projekta i procesa njegove izvedbe.

2.1. DEFINICIJE I OBILJEŽJA PROGRAMSKOG INŽENJERSTVA

Među brojnim inozemnim i domaćim stručnim definicijama programskog inženjerstva, u ovome poglavlju izdvajaju se tek neke od njih. One su rezultat rada i istraživanja uglavnom znanstvenika i stručnjaka iz ovoga područja, to jest iz područja informatike, a misli se na sljedeće:

- Softversko inženjerstvo je znanstvena i stručna disciplina koja se bavi svim aspektima proizvodnje softvera (Manger i Mauher, 2010);
- Inženjerstvo je znanstvena disciplina koja se bavi metodologijama koje se koriste kod učinkovite izgradnje velikih i kompleksnih sustava (Galinac, 2018);

- Softversko inženjerstvo definira se i kao primjena sustavnog, disciplinarnog, kvantificiranog pristupa razvoju, izvođenju i održavanju programskog proizvoda (IEEE, 2018).

Prema navedenim definicijama daje se zaključiti kako je načelno riječ o primjeni inženjerstva na programski proizvod ili softver, točnije inženjerskom pristupu njegova razvoja. Počeci razvoja ove znanstvene discipline razmatraju se od 70-ih godina prošloga stoljeća na dalje. Točnije, 1968. i 1969. godine organizirane su konferencije pod pokroviteljstvom NATO-a, na kojima se po prvi puta spominje i javno promovira ovaj termin (Galinac, 2018). Od tada do danas on doživljava rapidan razvoj, koji teče usporedno s ekonomskim, socijalnim i inim potrebama i promjenama na međunarodnoj razini.

U današnjici se, za objašnjavanje obilježja i važnosti programskog inženjerstva, često koristi definicija istoga koja navodi kako je riječ o skupu metodologija, aktivnosti, alata i modela za razvoj uspješnih softvera uz što niže troškove samoga procesa. Vidljivo je, kako je za cjelovito poznavanje i razumijevanje ovoga pojma, discipline ili znanstvenog područja, presudno poznavanje značenja i specifičnosti programskog proizvoda.

Vrlo je važno još istaknuti kako načelno programsko inženjerstvo i programiranje nisu istovjetni pojmovi, kao što se često prakticira tvrditi u javnosti. Programiranje je samo jedan od dijelova programskog inženjerstva. Prema tome, važno je istaknuti kako programsko inženjerstvo uz programiranje objedinjuje i matematički, psihološki i menadžerski pristup (Galinac, 2018).

Posljedično, može se zaključiti kako računalni programski inženjeri primjenjuju principe i tehnike računalnih znanosti, inženjerstva i matematičkih analiza na dizajn, razvoj, testiranje i evaluaciju softvera te sustava koji računalima omogućuju obavljanje svojih mnogobrojnih aplikacija (Try Engineering, 2018).

Programski inženjeri su uključeni u projektiranje i razvoj mnogih vrsta softvera, uključujući softver za operacijske sustave i distribuciju mreže, te softver za kompajlere. Kod programiranja ili kodiranja, programski inženjeri upućuju računalo

redak po red, kako izvršiti željenu funkciju (Try Engineering, 2018). Oni moraju imati snažne vještine programiranja, ali često su više zabrinuti za razvoj algoritama i analizu te rješavanje problema programiranja nego stvarno kodiranja.

Tipično programski inženjeri, koji rade u aplikacijama ili razvoju sustava, najprije analiziraju potrebe korisnika. Zatim dizajniraju, konstruiraju, testiraju i održavaju softverske aplikacijske programe ili sustave kako bi zadovoljili te potrebe.

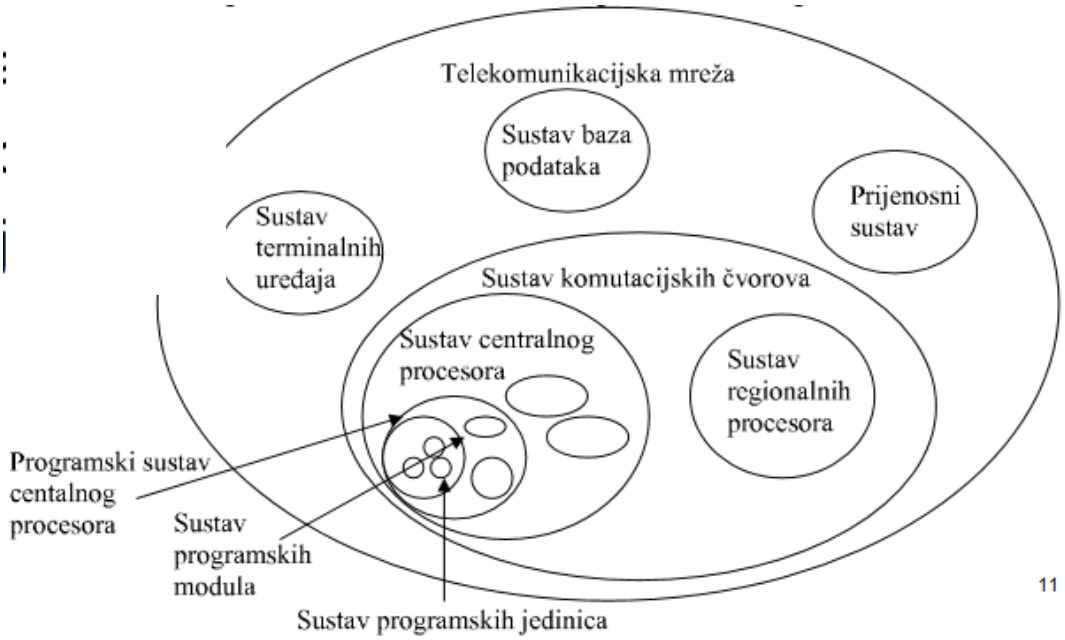
2.2. SOFTVERSKI PROJEKT

Softver ili softverski projekt (proizvod) nije isto što i program. Softverski proizvod je skup računalnih programa i pripadajuće dokumentacije koji se integrirano isporučuju krajnjem korisniku za zadovoljenje nekih osobnih potreba i želja (Galinac, 2018).

Također, riječ je o skupu računalnih programa i pripadajuće dokumentacije, koji je osmišljen i razvijen u svrhu prodaje ili komercijalizacije i to za specifičnog korisnika ili općenite korisnike na tržištu. Neovisno o vrsti, postoje neka konkretna obilježja programskog proizvoda, a misli se na (Galinac, 2018):

- Apstraktnost;
- Kompleksnost;
- Fleksibilnost;
- Teška mjerljivost svojstava.

S obzirom da pojam sustav predstavlja skup elemenata, softverski se sustav ili proizvod može prikazati na sljedeći način.



Slika 1.: Softverski proizvod ili sustav

Izvor: Galinac (2018)

Vidljivo je kako je riječ o iznimno kompleksnom produktu, a u današnjici postoje razne vrste istih, ovisno o korisnicima, potrebama i ostalim obilježjima. Jedna od općih klasifikacija ovih sustava, prema hijerarhiji i veličini, daje se u nastavku.

Slika 2.: Vrste softvera-hijerarhijska podjela

Izvor: Znanje (2018)

Neovisno o vrsti softvera te ostalim obilježjima, u današnje vrijeme presudno je da isti bude kvalitetan, funkcionalan, a sve više i korisnicima prilagođen. Svaki programski sustav ima za cilj osigurati sljedeće (Manger i Mauher, 2010):

- Mogućnost održavanja;

- Pouzdanost i sigurnost;
- Učinkovitost;
- Upotrebljivost.

Posebnu pažnju ovim elementima, kao i nizu ostalih obilježja te specifičnosti pridaje programski proces, odnosno proces izrade programskog sustava. Analizirajući isti, u nastavku poglavlja, zaokružuje se osnovna teorijska podloga u svezi ove problematike, te se obrađuju temeljni termini.

2.3. PROGRAMSKI PROCES

Programski proces sljedeći je ključni element, pojam ili termin u okviru ove problematike. On je nositelj svih aktivnosti ove prirode, to jest na istome se tijekom njegove provedbe, analiziraju svi relevantni pojmovi i aktivnosti. Iz prethodnog teksta daje se ukazati na značenje i obilježja ovoga termina, a najjednostavnije je reći da je riječ o procesu izvedbe programskog proizvoda, to jest njegova razvoja. U okviru programskog inženjerstva, kada se govori o razvoju programskog proizvoda, zapravo je riječ o njegovu životnom ciklusu, koji se sastoji od nekoliko faza.

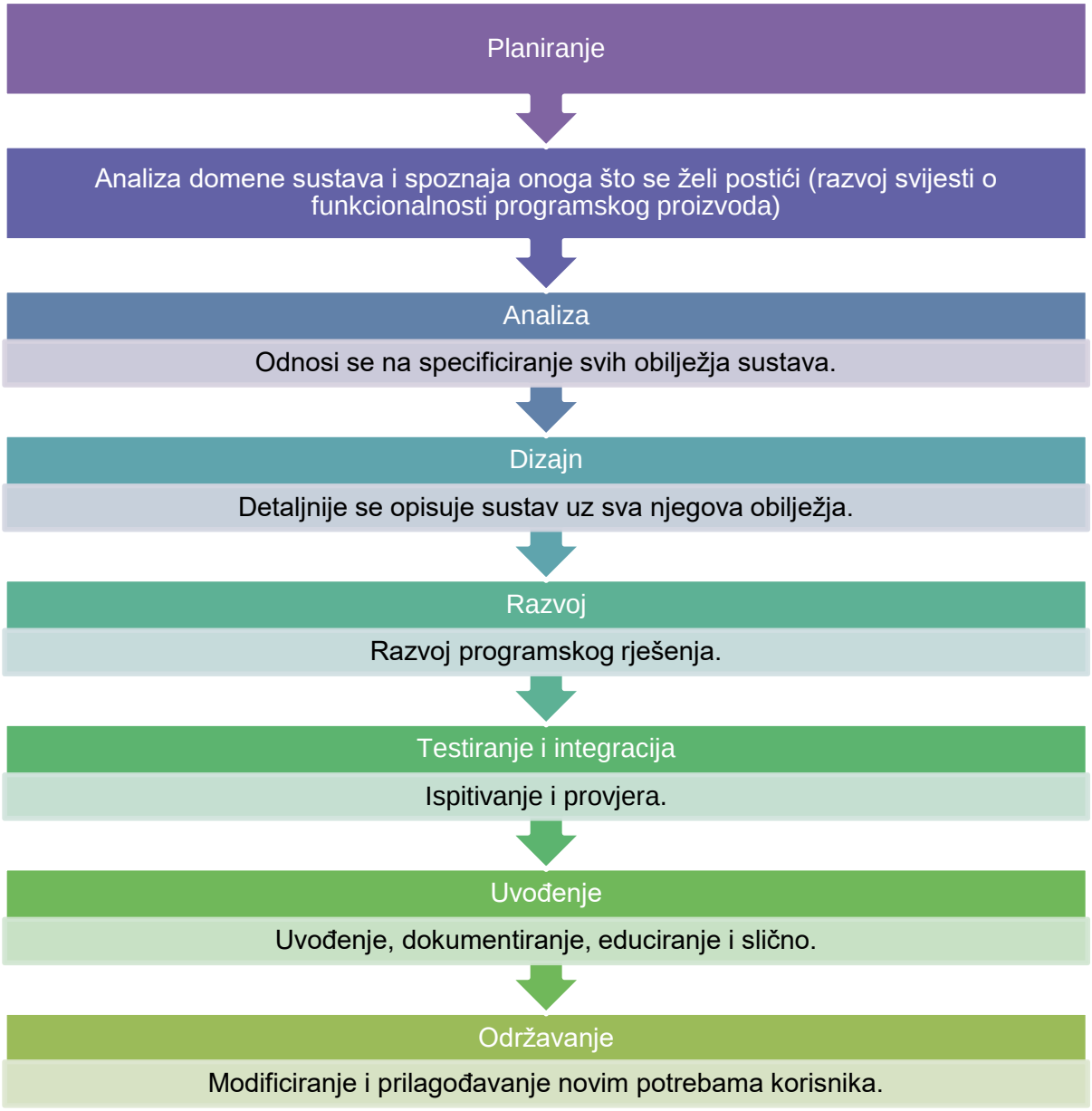
Programski proces podrazumijeva korištenje metodologije, niza metoda te alata u navedene svrhe. S obzirom na postojanje raznih metodologija, modela, instrumenata i alata, te ostalih obilježja, riječ je o vrlo kompleksnom procesu. Njegove osnovne aktivnosti ili faze mogu se razmatrati na sljedeći način.

Slika 3.: Programski proces

Izvor: Izrada autora prema: Uršulin Trstenjak et al. (2014)

Ovaj se fazni proces može razmatrati i na drugačiji način, pri čemu se identificira veći ili manji broj faza. Neovisno o načinu gledanja, važno je istaknuti kako su sve faze međusobno povezane i kao takve uvjetovane pa se pri njegovoj provedbi teži kvalitetnoj izvedbi svake od njih, kako bi i konačni rezultat bio takav.

Razrada ovoga procesa uz pojašnjenje svake od navedenih faza slijedi u nastavku.



Slika 4.: Životni ciklus programskog proizvoda

Izvor: Izrada autora prema: Matić et al. (2016, str. 7)

Za potrebe izvedbe ovoga procesa, kao što je i istaknuto, koriste se razne metodologije. Pri tome se razlikuju one tradicionalne ili klasične, sekvencijske koje se nadograđuju na tradicionalne i agilne metode kao suvremeni aspekti i pristupi razvoja programskog proizvoda. Pored toga, moguće je govoriti o nizu instrumenata, alata, tehnika i aktivnosti, što dodatno otežava izvedbu ovoga procesa. Treba istaknuti kako svaka od metodologija nudi konkretne prednosti i nedostatke pa je o odabiru optimalne važno cjelovito promišljati.

3. O RIZICIMA

Rizici se mogu pojmiti na nekoliko načina, no neovisno o aspektu njihova definiranja i razmatranja, riječ je o pojmu, koji ne mora nužno uvijek imati negativne konotacije. Načelno je riječ o mogućim problemima ili opasnostima u okviru neke aktivnosti ili čitavog procesa, no ponekad izloženost riziku, u konačnici, može donijeti znatno bolje rezultate i uspjeh.

Rizici se mogu podijeliti na nekoliko skupina, a posebno je važno istaknuti teško i lako mjerljive rizike. Činjenica je kako je s lako mjerljivim rizicima lakše i jednostavnije upravljati, odnosno postoje veće mogućnosti za njihovo izbjegavanje i minimiziranje, te obrnuto.

U ovome dijelu rada, definiraju se rizici, određuju neke od vrsta i modela rizika, te se razmatra mjerenje ili kvantificiranje rizika, uz osvrt na kategorizaciju i stav prema riziku.

3.1. DEFINICIJE, VRSTE I MODELI RIZIKA

Rizici i rizično poslovanje predstavljaju opsežno područje o kojem je moguće raspravljati na diferencirani način. Može se reći da oni predstavljaju dio svakodnevnice poslovanja i razvoja proizvoda, subjekata, organizacija, djelatnosti i redom dalje. Riječ je o jednom od sastavnih dijelova heterogene okoline.

Već je prethodno istaknuto kako rizici načelno ne moraju uvijek donositi probleme i gubitke, pa se njihovo percipiranje treba proširiti i u drugom smjeru. Naime, u suvremeno doba se nastoji ukazati na sljedeće mogućnosti pregleda rizika (Udovičić i Kadlec, 2013):

- Raspon koji obuhvaća rizike, ali i prilike;
- Dobitci i gubitci koji obuhvaćaju pozitivne i negativne rezultate;
- Vjerojatnost nastavka i posljedice.

Prema tome, ispravno je tvrditi kako rizik predstavlja neizvjestan ishod nekog događaja, pothvata i sličnog, odnosno situaciju u kojoj ne postoji sigurna percepcija onoga što slijedi i što će se kao takvo dogoditi (Srića, 2011).

Rizici se naziru u mnogim segmentima, a često se proučavaju u domeni poslovnog odlučivanja. Pri tome, a u okviru ove problematike, moguće je govoriti o odlučivanju u svezi razvoja novog programskog proizvoda, gašenja ili modificiranja postojećeg te redom dalje.

Kada se govori o rizicima generalno, moguće je identificirati nekoliko njihovih vrsta. Neka od najčešćih podjela rizika je ona koja razlikuje poslovni i financijski rizik.

Slika 5.: Vrste rizika

Izvor: Izrada autora prema: Udovičić i Kadlec (2013, str. 50.-60.)

Iz danog prikaza moguće je ukazati kako se poslovni rizici pojavljuju u kontekstu gotovinskog tijeka, dok su oni financijski, kao što i naziv ukazuje, vezani uz način financiranja neke odluke, aktivnosti ili pothvata.

3.2. UPRAVLJANJE RIZICIMA

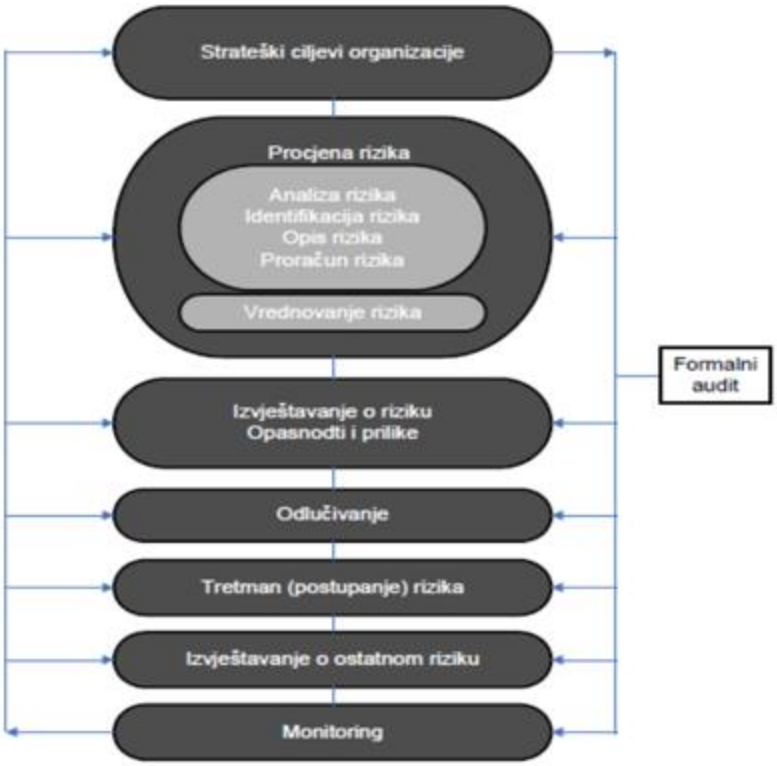
U okviru procesa upravljanja rizicima, odvijaju se sve radnje i aktivnosti u svezi njih. Stručno se ovaj pothvat i svojevrsni proces naziva menadžmentom rizika (engl. *risk management*), a predstavlja proces mjerenja, procjene rizika i razvoja strategija za kontrolu rizika (Udovičić i Kadlec, 2013).

U znanosti se često menadžment rizika raščlanjuje na manje dijelove, odnosno sastavne elemente pa je moguće govoriti o (Software testing help, 2018):

- Tradicionalnom sustavu upravljanja rizikom;
- Financijskom menadžmentu rizika;
- Tradicionalni menadžment rizika
- Menadžmentu rizika u pojedinim sektorima ili djelatnostima i redom dalje.

U kontekstu toga identificira se i menadžment rizika u programskom inženjerstvu. S obzirom da rizici predstavljaju jedinicu nesigurnosti, vrlo je važno kontinuirano ih istraživati, procjenjivati, mjeriti, a time i kontrolirati. To su osnovne aktivnosti procesa upravljanja rizicima, neovisno o području, djelatnosti ili sektoru u kojem se provode. Mjerenje rizika vrlo je značajno za ovaj proces, pa se često tvrdi kako je moguće upravljati jedino onim rizicima koje je moguće kvantificirati na cjelovit način.

Generalno, proces upravljanja rizikom može se prikazati na nekoliko načina, a pri tome se identificiraju različite faze ovoga procesa. Jedan od mogućih prikaza daje se u nastavku.



Slika 6.: Proces upravljanja rizikom

Izvor: Udovičić i Kadlec (2013, str. 50.-60.)

Upravljanje rizikom odvija se, kao što je i vidljivo na nekoliko različitih načina, no svrha ovoga procesa je izbjegavanje, smanjivanje, preuzimanje, te pomicanje rizika. Moguće je čak tvrditi kako je svrha i iskorištavanje rizika u pozitivnom kontekstu, to jest u smislu prepoznavanja prilika koje iz njih proizlaze. Ta uvjerenja treba primjenjivati na svim razinama, a time i na području programskog inženjerstva.

U sam proces integrirane su različite skupine dionika, a često se ističe kako je riječ o integraciji svih onih subjekata koji su povezani na izravan ili neizravan način. Generalno misli se na sljedeće (Udovičić i Kadlec, 2013):

- Direktor projekta (eng. *project director*);
- Voditelj odjela rizika (eng. *risk manger*);
- Potencijalni nositelj rizika (eng. *risk owner*);
- Nositelj aktivnosti (eng. *risk action owner*).

Iz danih značajki potvrđuje se kompleksnost ovoga procesa, no svakako treba istaknuti, kako među brojnim funkcijama posebnu pažnju plijeni kontrola rizika. Ona

je usko vezana i zavisna o svim ostalim funkcijama, posebice mjerenju i procjeni rizika.

Kako bi izvedba ovoga procesa bila moguća, a ujedno i kvalitetna, važno je provoditi kontinuirana istraživanja okoline. To za cilj ima, između ostaloga, reduciranje nesigurnosti i rizika, kao i osiguranje stabilnih i optimalnih uvjeta za provedbu odluke, procesa i sličnoga. Reduciranje i upravljanje rizikom jest proces s glavnim ciljem očuvanja učinkovitosti djelovanja. Pri tome, kvalitetno organiziran proces upravljanja rizikom mora pažljivo i stručno identificirati i analizirati rizik, a ovaj proces nosi pet ključnih točaka ili faza (Srića, 2011):

- Utvrditi sve relevantne izvore rizika;
- Procijeniti učestalost i težinu mogućih gubitaka;
- Izabrati ili razviti metodu kontrole rizika;
- Primijeniti odabrane metode upravljanja rizikom;
- Nadgledati djelotvornost i održivost odabranih metoda upravljanja rizikom.

Zaključno se ističe kako upravljanje rizikom biva utemeljeno na analizi rizika. Ona daje osnovu, odnosno definira plan djelovanja, u svrhu izbjegavanja ili minimiziranja negativnih posljedica istoga, kao i maksimiziranja onih pozitivnih. Može se istaknuti kako ovaj proces u svakom području i na primjeru svih poslovnih subjekata ima izniman značaj jer doprinosi mnogočemu. Načelno je moguće tvrditi kako doprinosi sigurnijem, efikasnijem i učinkovitijem poslovanju, ali i razvoju, neovisno o objektu istraživanja.

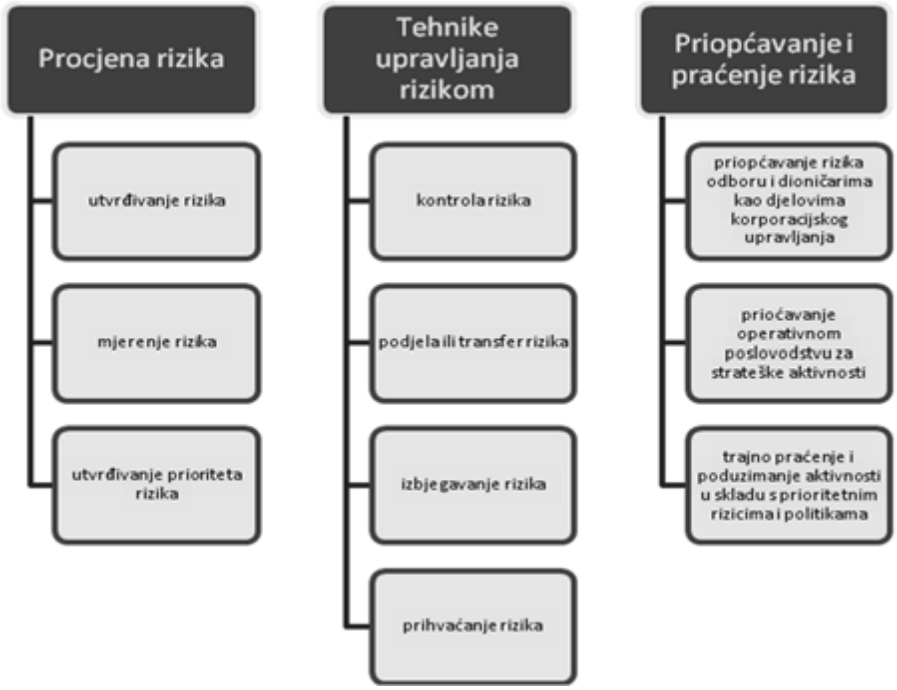
Generalne koristi samoga procesa upravljanja rizikom mogu se razmatrati kroz stvaranje okvira za buduće aktivnosti, unapređenje odlučivanja i planiranja, učinkovitije korištenje resursa i smanjenje nestabilnosti u poslovanju uz optimizaciju poslovnih uvjeta i prilika. S obzirom da analiza rizika predstavlja osnovu ili izvorište ovoga procesa, u nastavku slijedi detaljnije o njoj.

3.3. ANALIZA RIZIKA

Analiza rizika nezaobilazno je područje pri svakom istraživanju problematike ove prirode. U kontekstu iste analizira se i značenje procjene rizika, što načelno zadire u središnju problematiku ovoga rada.

Sam pojam analize rizika definira se kao „skup metoda i postupaka koji omogućuju potpunije razumijevanje problema u situacijama strateškog odlučivanja i pomažu da se pronađe zadovoljavajuća strategija prema unaprijed postavljenom kriteriju izbora (Udovičić i Kadlec, 2013, str. 54.).“ Strukturiranje i modeliranje pri tome biva u službi identificiranja ili prepoznavanja rizika, što je početni korak u procesu njegova upravljanja.

Nakon identificiranja rizika, važno je kvantificirati njegovu veličinu, to jest pristupiti njegovu mjerenju, a na temelju toga izvršiti razdiobu ključnih varijabli, utjecaja i očekivanih rezultata, što dovodi do optimalne strategije upravljanja rizicima. Sam proces analize rizika, kao središnji proces upravljanja istima, može se prikazati na sljedeći način.



Slika 7.: Analiza rizika

Izvor: Udovičić i Kadlec (2013., str. 50.-60.)

Evidentno je kako je analiza rizika sačinjena od tri temeljna područja ili elementa. Misli se pri tome na procjenu rizika, upravljanje rizicima i izvještavanje o istima. Svaka od ovih faza sačinjena je od nekoliko jednostavnijih, a sve bivaju međusobno uvjetovane i u tom kontekstu povezane. Sukladno navedenome, procjenu rizika sačinjava identificiranje istih, mjerenje ili kvantificiranje, odnosno procjena rizika. Narednu fazu čine kontrola rizika, segmentiranje ili podjela, izbjegavanje rizika te njihovo spremno prihvaćanje. Konačnu fazu, koja zaokružuje ovaj proces, čine priopćavanje rizika svim dionicima i sudionicima procesa, te trajno praćenje istih i djelovanje sukladno aktualnim politikama, ciljevima, potrebama i redom dalje.

Kada se govori o procesu upravljanja rizicima u programskom inženjerstvu, istaknute činjenice i značajke ovoga procesa i analize rizika izravno se impliciraju na predmetno znanstveno područje. Prema tome, sam proces načelno se odvija u istome smjeru i prema istim principima, koristi se u iste svrhe, ali se prilagođava ili modificira specifičnostima aktivnosti i potrebama. Detaljnije o tome slijedi u narednom poglavlju rada.

4. RIZIK U PROGRAMSKOM INŽENJERSTVU

U prethodnim poglavljima obrađena je problematika programskog inženjerstva, softvera ili programskog proizvoda, rizika i ostaloga. Smatra se kako je na taj način dana cjelovita osnova za povezivanje temeljnih problema, identificiranje uzročno-posljedičnih veza.

Rizik u programskom inženjerstvu svakodnevna je pojava. Riječ je o neizvjesnosti ovoga djelovanja, koje je rezultat niza utjecaja iz okoline, nepredvidivih trendova i izazova te redom dalje. Načelno nije riječ samo o neizvjesnosti u kontekstu prijetnje opasnosti i problema, već je riječ i o potencijalnim prilikama za maksimizaciju uspjeha. Smatra se kako su ovi rizici posebno istaknuti u današnje vrijeme, što je rezultat kompleksnosti današnjeg poslovanja, okoline u kojoj se odvija te dinamičnih i intenzivnih promjena koje nastaju i razvijaju se na međunarodnoj razini.

U ovome poglavlju sistematiziraju se stečena znanja i percepcije temeljnih pojmova, te se predmetni rad zaokružuje u smislenu cjelinu. Točnije, obrađuje se problematika rizika u programskom inženjerstvu, a poseban naglasak postavlja se na razloge neuspjeha, te upravljanje rizicima u ovome području.

4.1. POJAM I DEFINICIJA RIZIKA U PROGRAMSKOM INŽENJERSTVU

Rizici u programskom inženjerstvu nešto su specifičniji od generalnog pristupa njihovu upravljanju, analizi i procjeni. O ovoj temi počinje se intenzivnije raspravljati 80-ih godina prošloga stoljeća, kada dolazi do intenzivnijeg korištenja formalnih metoda za istraživanje, upravljanje i kontrolu rizicima, a od strane vodećih multinacionalnih kompanija. Već u to vrijeme dolazi i do razvoja svijesti kako je riječ o izazovnom, financijski iscrpnom i vremenski dužem procesu. Od tada do danas kontinuirano se unapređuju metode i tehnike u ovu svrhu, a danas zakonske obveze i regulativni okviri brojnih organizacija nastoje dati podršku organizacijama i subjektima u ovome procesu (Uremović, 2009).

Nastavno na prethodno, upravljanje rizicima u programskom inženjerstvu može se generalizirati i na taj način odrediti kao identifikacija, procjena i određivanja prioritetnih rizika, a nakon kojih slijedi koordinirana i ekonomična uporaba sredstava kako bi se smanjila, nadzirala i bolje kontrolirala vjerojatnost i/ili utjecaj neželjenih događaja, a s druge strane maksimizirale koristi i prilike (Uremović, 2009). Kao što je i prethodno istaknuto, danas se javljaju brojne vrste ovih rizika, a realna situacija ili okolišno stanje mogu se prikazati na sljedeći način.

Slika8.: Vrste IT rizika

Izvor: CIS (2003)

Vidljivo je kako na životni ciklus programskog proizvoda utječu brojni čimbenici iz okruženja, a koji se razmatraju kao zasebne vrste rizika. Ovime se potvrđuje kako je riječ o vrlo dinamičnom i neizvjesnom okruženju, točnije o skupu rizika koje je teško identificirati, pratiti i kao takve kvantificirati.

4.2. UPRAVLJANJE RIZICIMA U PROGRAMSKOM INŽENJERSTVU

Danas se u svijetu koriste razne metodologije, instrumenti i alati koji služe upravljanju rizika u programskom inženjerstvu. Njihova brojnost ukazuje ujedno i na kompleksnost ove problematike te potvrđuje početne hipoteze rada. Pri tome se misli na upravljanje rizicima različitih obilježja i prirode, a misli se na IT rizike, rizike informacijske sigurnosti i generalno poslovne rizike.

Specifičnost upravljanja rizicima u programskom inženjerstvu očituje se u tome što se cjelokupni proces uglavnom svodi na dvije glavne ili vodeće faze, a to su (Spremić, 2009):

- Procjena rizika;
- Obrada rizika.

U svrhu provedbe ovih faza koriste se brojne verzije razvijenih metodologija, a neke od njih prikazuju se u nastavku. Važno je pri tome istaknuti da se one diferenciraju s obzirom na osnovna obilježja, cijenu, ali i primjenjivost.

	Zemlja porijekla	**Cijena**	**Primjenjivost na vrstu organizacije**	**Mogućnost certificiranja**
CRAMM	Velika Britanija	N/A	velike	Ne
BS 7799-3:2006	Velika Britanija	Cca 80 funti	Sve	U sklopu ISO 27001
ISO/IEC 27001:2008	Velika Britanija	Cca 90 funti	Sve	U sklopu ISO 27001
IT-Grundshutz	Njemačka	Besplatno	Sve	Ne
Mehari 2007	Francuska	Besplatno	Sve	Ne
Octave	SAD	Besplatno	Srednje i male	Ne
SP 800-30 (NIST)	SAD	besplatno	Sve	Ne

Tablica 1.: Metodologije za upravljanje rizicima u programskom inženjerstvu

Izvor: Izrada autora prema: Uremović (2009)

Nakon identificiranja nekih od postojećih metodologija koje se koriste u predmetne svrhe, treba istaknuti kako ujedno postoji čitavi splet softverskih alata koji služe ubrzavanju postupaka u okviru ovoga procesa. Oni se pri tome koriste za potrebe procjene i obrade rizika u programskom inženjerstvu. Svrha istih, pored navedenoga, jest osigurati sveobuhvatnost pri definiranju prijetnji i ranjivosti, a ujedno omogućiti jednostavnije i lakše mjerenje odnosno kvantificiranje rizika, koristeći se pri tome matematičkim izrazima i formulama. Sve to u konačnici rezultira stvaranjem izvještaja koji se dostavljaju menadžerima i ostalim dionicima.

Pri upravljanju rizicima postoje dva različita pristupa, preventivni i korektivni. Osnovna razlika među njima očituje se u vremenu njihove primjene ili provedbe, u odnosu na pojavnost rizičnog događaja. Naime, preventivni pristup fokus postavlja na prevenciju rizika i planiranje. On se temelji na izbjegavanju i ublažavanju rizika, a

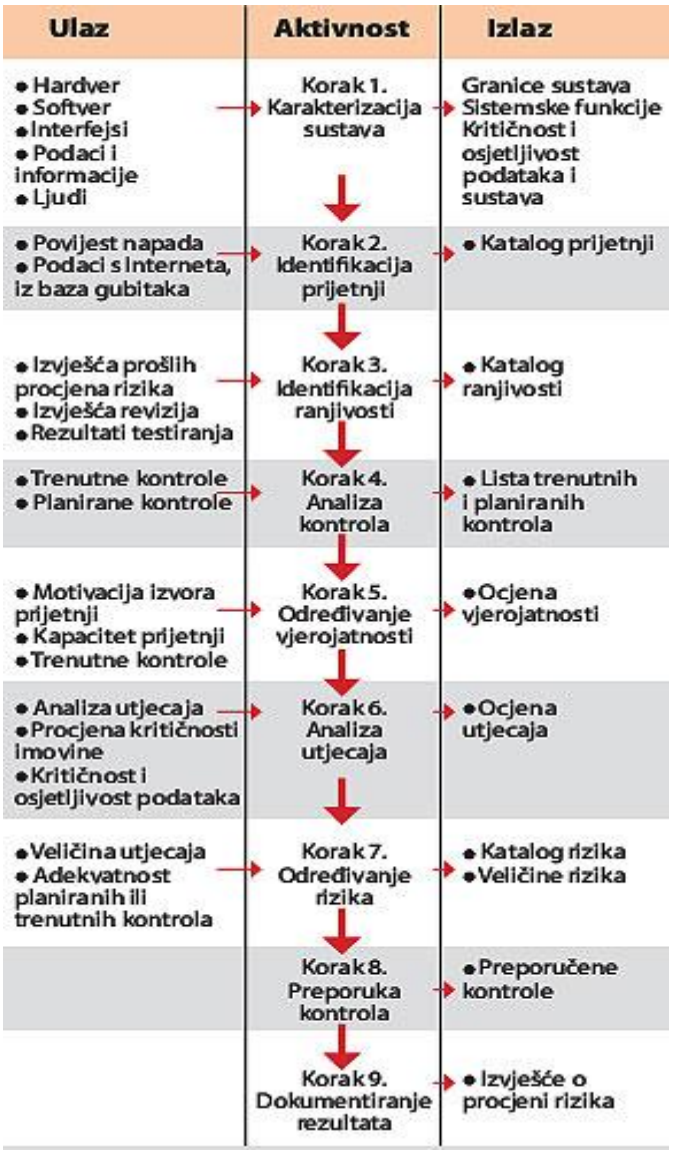
podrazumijeva izradu plana i preventivnih mjera. S druge strane, korektivni pristup provodi se nakon pojave rizika, a fokus postavlja na oporavak od istoga. On se temelji na provedbi plana oporavka od rizika (Buntak et al., 2014).

Kod preventivnog pristupa izbjegavanje rizika podrazumijeva promjenu koncepta, zahtjeva, specifikacije ili načina rada. U okviru ovoga pristupa provode se konkretni koraci koji se odnose na definiranje minimalno prihvatljivih rezultata, definiranje očekivanja, izbjegavanje nesigurne tehnologije, korištenje standarda i provjerenih metoda te oslanjanje na rad drugih (Buntak et al., 2014).

Na primjeru korektivnog pristupa kontrola rizika zasniva se na ublažavanju i otklanjanju negativnih učinaka koje je rizik uzrokovao. Ovaj pristup zahtijeva dobru komunikaciju i vidljivost rizika, korištenje znanja i vještina specijalista, snažnu podršku vodstva, kontinuiranu uključenost korisnika i jasne prioritete u odlučivanju (Buntak et al., 2014).

4.3. PROCJENA RIZIKA

Procjena rizika u programskom inženjerstvu vrlo je izazovan proces, ali istovremeno i vrlo koristan pothvat, o čijoj kvaliteti izvedbe ovise mnoge buduće aktivnosti i radnje. Pored toga, smatra se ispravnim tvrditi kako kvalitetno procijenjeni rizici, te poduzete radnje za minimiziranje njihovih negativnih učinaka i maksimiziranje onih pozitivnih, generiraju kvalitetu programskog proizvoda, ali i zadovoljstvo te povjerenje korisnika. Kako bi bilo jasnije što ovaj proces zaista predstavlja u praksi, u nastavku se daje njegov prikaz.



Slika 9.: Proces procjene rizika u programskom inženjerstvu

Izvor: Uremović (2009)

Sukladno navedenome, procjenu rizika u programskom inženjerstvu treba spoznati kao prvi ili vodeći proces upravljanja rizikom, koji se koristi u razne svrhe. Pri tome se prvenstveno misli na određivanje opsega potencijalnih prijetnji i rizika koji prate neki informacijski sustav kroz njegov životni ciklus. Također, izniman doprinos predmetnog procesa očituje se i u identificiranju optimalne kontrole za smanjenje ili ublažavanje negativnih rizika, te suprotno.

4.3.1. Karakterizacija informacijskog sustava

U okviru prvog koraka ovoga procesa, definira se sam cilj pothvata ili nekoliko njih. Točnije, riječ je o određivanju granica informacijskog sustava, zajedno s ostalim uređajima i informacijama. Od tuda potječe i sami naziv faze, a ona služi, između ostaloga, za utvrđivanje osnovnih informacija u svezi definiranja rizika.

U okviru nje prikupljaju se podaci o sustavu, a misli se na (CIS, 2018):

- Hardver:
- Softver;
- Sučelje sustava;
- Podatke i informacije;
- Osoblje koje koristi sustav;
- Namjenu sustava;
- Kritičnost sustava i podataka;
- Osjetljivost sustava i podataka.

Prikupljanje podataka vrlo je zahtjevan posao, a zasniva se na korištenju tehnika poput upitnika, intervjua s dionicima, analize postojeće dokumentacije ili upotrebu automatskih skenirajućih alata.

4.3.2. Identificiranje prijetnji

Ovo je ujedno sljedeća faza u procesu procjene rizika. Kod identificiranja prijetnji vrši se njihovo prepoznavanje, specificiranje i razrada vjerojatnosti uz analizu ranjivosti sustava. Naime, kod procjene prijetnje razmatraju se svi potencijalni izvori iste, koji se dijele na (CIS, 2018):

- Tehničke izvore – kvarovi opreme;
- Ljudske izvore – nestručnost osoblja, neodgovornost, zlonamjernost i slično.

Ova faza ima za cilj formiranje liste prijetnji koja je prilagođena aktualnoj organizaciji ili situaciji. Ova faza se često razmatra integrirano s fazom procjene ranjivosti

sustava s obzirom na njihovu usku povezanost, a što je već i istaknuto. Produkt te faze je lista ranjivosti sustava.

4.3.3. Analiza kontrola

Kao što i sam naziv ukazuje, ova faza posvećena je kontroli, to jest razmatranju onih kontrola koje se planiraju ili primjenjuju u organizaciji, a u svrhu izbjegavanja i minimiziranja prijetnji. Pri tome, govori se o nekoliko mogućih kontrola. Sigurnosne kontrole obuhvaćaju tehničke i netehničke metode, odnosno zaštitni alati ugrađeni u računalni hardver, softver ili fireware (npr. mehanizmi za kontrolu pristupa, mehanizmi za identifikaciju i autentikaciju, enkripcijske metode, softver za otkrivanje upada) te kontrole upravljanja i radne kontrole poput sigurnosnih politika, zaštitnih procedura i slično. Nadalje, tehničke se kontrole mogu dijeliti na preventivne i aktivne. Preventivne su one koje sprečavaju pokušaje prekršaja sigurnosne politike i uključuju kontrolu pristupa, enkripciju i autentikaciju, dok aktivne kontrole upozoravaju na prekršaje sigurnosne politike i sadrže takve kontrole kao što su nadzorna praćenja (audit trails), metode otkrivanja upada i kontrolne sume (CIS, 2018).

4.3.4. Određivanje vjerojatnosti

Za određivanje vjerojatnosti važno je razmotriti neke ključne elemente poput motivacije, prirode ranjivosti, postojanja i učinkovitosti postojećih kontrola te mogućih korekcija.

Osim navedenoga, vrlo je važno odrediti štetni utjecaj, kao rezultat iskorištavanja ranjivosti, odnosno učinka prijetnje. Kako bi isto bilo moguće, važno je prikupiti informacije o svrsi, kritičnosti i osjetljivosti sustava.

4.3.5. Analiza utjecaja

Analiza utjecaja vrši se, između ostaloga, uvidom u postojeću dokumentaciju organizacije, a misli se na pregled raznih izvještaja. Provedbom predmetne analize

zapravo se pristupa klasifikaciji nivoa utjecaja, kvantificiranje utjecaja i opisivanju njihovih kvalitativnih značajki. Svrha predmetnog koraka ili faze jest procijeniti razinu rizika za neki informacijski sustav te na osnovu toga planirati ostale faze i potrebite akcije, a misli se na preporuku kontrole.

4.3.6. Preporuka kontrola

Ova faza proizlazi iz svih prethodnih aktivnosti predmetnog procesa. Optimalna kontrola željeno je stanje istoga, a ona se definira s obzirom na niz čimbenika poput zakonodavstva, organizacijske politike, utjecaja na rad, sigurnosti i pouzdanosti te redom dalje (Uremović, 2009). Sama faza može se odrediti kao da daje smjernice za proces ublažavanja rizika, za vrijeme kojeg se preporučene proceduralne i tehničke sigurnosne kontrole procjenjuju, klasificiraju i primjenjuju (CIS, 2018).

4.3.7.Dokumentiranje rezultata

Dokumentiranje rezultata zapravo se odnosi na pisanje izvješća o ovome procesu, koji predstavlja svojevrsno istraživanje. Dobiveni izvještaj proširuje postojeću bazu podataka, a time se koristi sadašnjim i tekućim potrebama, kao i onim budućim. Ovom se fazom okončava predmetni proces u tom vremenu, no njegov kraj podrazumijeva povratak na prvu fazu, s obzirom na obilježja procesa procjene rizika, o čemu je prethodno bilo riječ.

4.4. PRAKTIČNO POJAŠNJENJE

Kako bi se procjena rizika uspješno izvela u praksi, u okviru prve faze ovoga procesa definira se sustav kojim će se rizici promatrati, odnosno identificirati i objasniti. U okviru ove faze, u znanosti se često spominje termin registra obavijesne imovine (engl. *asset register*), koji predstavlja registar ili popis osobnih računala, poslužitelja i aplikacijskog softvera, no i poslovnih procesa, računalnih i komunikacijskih usluga, aplikacijskih i sistemskih softvera, računalne i komunikacijske opreme, medija, izvora napajanja, klima uređaja, vanjskih partnera, djelatnika organizacije i ostaloga (Uremović, 2009).

Kod organizacija koja prvi puta pristupaju praćenjima, odnosno upravljanju rizicima, važno je provesti karakterizaciju ovoga sustava. Nakon poznavanja sustava i obavijesne imovine unutar sustava, moguće je identificirati sve one prijetnje, kao i ranjivost, a što u suštini predstavlja svojevrsne rizike.

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

Tablica 2.: Primjeri rizika
Izvor: Uremović (2009)

Važno je istaknuti kako je upravljanje rizicima jedan od najizazovnijih procesa u ovome području, ali i šire. Često se on razmatra kao živući proces koji nema granice. Ono što je esencijalno u kontekstu ove problematike jest spoznati kako se rizici kontinuirano javljaju i vrlo intenzivno razvijaju. Upravo zbog toga sustav upravljanja rizicima u programskom inženjerstvo treba se implementirati kao svakodnevni operativni organizacijski proces, a izvori se mogu pronaći u postojećim bazama podataka u svezi projektnih rizika, testiranja softverskih proizvoda, ranjivosti na internetu i sličnome.

Tek nakon što se definiraju moguće prijetnje kojima je izložena imovina, prikupe podaci o kontrolama, moguće je izvršiti procjenu rizika. Za te potrebe koriste se razne formule i pristupi, a jedan od najjednostavnijih i najprimjenjivanijih je umnožak osnovnih varijabli, odnosno imovine, prijetnje i ranjivosti (CIS, 2018). Kako bi isto bilo provedivo, u praksi se ovim varijablama dodjeljuju vrijednosti koje su definirane sljedećom kvantitativnom skalom.

Vrijednost imovine	Razina prijetnje								
	Mala			Srednja			Velika		
	Razina ranjivosti								
	M	S	V	M	S	V	M	S	V
0	0	1	2	1	2	3	2	3	4
1	1	2	3	2	3	4	3	4	5
2	2	3	4	3	4	5	4	5	6
3	3	4	5	4	5	6	5	6	7
4	4	5	6	5	6	7	6	7	8

Tablica 3.: Kvantitativna skala vrijednosti imovine, prijetnje i ranjivosti
Izvor: Uremović (2009)

Sukladno navedenome, procjena rizika, u smislu njegova kvantificiranja vršiti će se na način da se pomnože vrijednost ostvarivanja prijetnji s utjecajem na imovinu. Konačni rezultati takvog kvantificiranja predstavljaju procjenu rizika.

		Utjecaj		
Vjerojatnost ostvarivanja prijetnje	Vrlo visok (100)	Umjereno veliki (60)	Srednji do mali (30)	Vrlo mali (10)
Vrlo velika (1)	Vrlo visok (100)	Vrlo visok (60)	Visok (30)	Srednji (10)
Umjereno velika (0,6)	Vrlo visok (60)	Visok (36)	Srednji (18)	Nizak (6)
Srednja do mala (0,3)	Visok (30)	Srednji (18)	Nizak (9)	Nizak (3)
Vrlo mala (0,1)	Srednji (10)	Nizak (6)	Nizak (3)	Nizak (1)

Tablica 4.: Rezultati procjene rizika
Izvor: Uremović (2009)

Prema danoj matrici moguće je s jednostavnošću izvršiti procjenu rizika, neovisno o kojem je problemu riječ. Istu je moguće primjenjivati u svakodnevnom poslovanju, a na taj način doprinijeti izbjegavanju i minimalizaciji štetnih rizika, te suprotno.

Nakon procjene rizika, nastupa faza njihove obrade. Zapravo se pristupa razmatranju djelovanja u svezi kontrole rizika. Moguće strategije su minimiziranje rizika, otklanjanje rizika, izbjegavanje rizika te redom dalje. Načelno je riječ o nadolazećoj kompleksnoj fazi, koja upotpunjuju prethodnu, a integrirano čine proces upravljanja rizika u programskom inženjerstvu.

Načelno postoji nekoliko kategorija rizika u programskom inženjerstvu, koje određuju niz mogućih vrsta u praksi. Misli se na loš raspored (npr. vrijeme), financijske rizike (npr. nedovoljan budžet, premašivanje troškova i slično), operacijske rizike (npr. nepostojanje komunikacije unutar tima, nedostatak adekvatnog treninga i izvora planiranja te slično), tehničke rizike (npr. konstantno mijenjanje opreme) i programske rizike (npr. promjena zakonskih pravila i odredbi, razvoj tržišta i slično). Sve su to rizici koji kontinuirano prijete ovome procesu u praksi (Cast Software, 2018)

Kako bi predmetna problematika bila jasnija, moguće je dati nekoliko praktičnih primjera rizika i njihova upravljanja u programskom inženjerstvu. Pri tome, moguće je

govoriti o generičkim rizicima, koji imaju vjerojatnost pojave u svim vrstama projekata, te o specifičnim rizicima. Dva ogledna primjera generičkih rizika na nekom projektu mogu biti prekoračenje troškova projekta i nedostatak resursa.

Kod identificiranja ovih i ostalih rizika važno je integrirano djelovanje svih sudionika projekta. Oni na temelju opsežnih istraživanja prvenstveno identificiraju rizik i nastoje ga kvantificirati i opisati. Moguće je preventivno djelovati na ove rizike, to jest nastojati ih izbjeći ili korektivno, odnosno umanjiti posljedice ovih rizika.

Na primjeru rizika prekoračenja budžeta neke od strategija mogu biti strategija prihvaćanja gubitaka, strategija prijenosa odgovornosti na ostale dionike, na primjer dobavljače resursa ili strategija promjene cijene konačnog proizvoda uz dodjelu dodane vrijednosti, ukoliko je moguće.

Kod rizika nedostatka resursa također se predlaže strategija prihvaćanja i ublažavanja negativnih učinaka (npr. kašnjenje, veći troškovi i slično) putem nabave potrebitih resursa. Navedene uzroke i posljedice potrebno je adekvatno arhivirati i koristiti se podacima za buduće pothvate, kako bi se preventivno djelovalo na taj rizik u budućnosti.

5. ZAKLJUČAK

Može se reći da je programsko inženjerstvo kompleksno znanstveno područje, koje u današnjici daje izravnu podršku svim djelatnostima i sektorima. U tom kontekstu, ono predstavlja funkcionalni dio suvremene ekonomije, ali i globalnog društva.

Poistovjećivanje programskog inženjerstva s programiranjem nije ispravno, s obzirom da je programiranje tek dio ovoga područja pa ga je kao takvog važno i pojmiti. Često se ističe kako je to i ključni segment istoga s obzirom da se fokusira na ključni proces, odnosno razvoj softverskog proizvoda. Riječ je o složenom procesu koji se odvija u nekoliko faza, integrira brojne dionike, a biva suočen s kontinuiranim rizicima.

Iako se u literaturi i znanosti rizik često razmatra u negativnom kontekstu, to nije sasvim točno, a ovu tvrdnju moguće je potvrditi i na primjeru programskog inženjerstva. Naime, rizici predstavljaju neizvjesna stanja, a ona mogu biti negativna u smislu problema i prijetnji, ali i pozitivna u kontekstu maksimiziranja prilika i mogućnosti. Kako bi konačni ishod, uslijed njihova djelovanja, bio uspješan, važno je izvršiti kvalitetnu procjenu rizika.

Identificiranje rizika i njihovo mjerenje preduvjet su za uspješnu procjenu rizika. Načelno je riječ o vrlo složenoj situaciji, s obzirom da je rizike generalno teško mjeriti, a posebice u području programskog inženjerstva, uslijed kompleksnosti procesa, složenosti i dinamičnosti okoline, nepredvidivosti situacija i redom dalje.

U današnje se vrijeme primjenjuju različiti pristupi, metode i tehnike procjene rizika, a takav trend očekuje se i u budućnosti. Za programere, inženjere, menadžere i ostale dionike riječ je o esencijalnom procesu, to jest pothvatu, o čijoj kvaliteti izvedbe ovisi cjelokupni proces upravljanja rizicima, a naposljetku i proces razvoja softverskog proizvoda.

Vidljivo je kako je riječ o zasebnom faznom procesu, koji se sastoji od niza koraka i radnji, a predstavlja osnovu za spoznaju realnog stanja, prijetnji informatičkom

sustavu, ranjivosti istoga te redom dalje. Svrha samoga procesa, osim navedenoga, jest utvrditi i optimalnu kontrolu koja će osigurati stabilnost, sigurnost i efikasnost nekog sustava, a time doprinijeti konačnom zadovoljstvu korisnika, ali i ostalih dionika.

LITERATURA

Knjige:

1. Manger, R., Mauher, M. (2010.) Programsko inženjerstvo – priručnik. Zagreb: Algebra d.o.o.
2. Matić, M. et al. (2016.) Razvoj i primjena informacijskih sustava. Zagreb: Tehničko veleučilište u Zagrebu.
3. Sikavica P. et al. (2008.): Suvremeni menadžment vještine, sustavi i izazovi. Zagreb: Školska knjiga
4. Srića V. (2011.): Menadžment rizika. Šibenik: Veleučilište u Šibeniku

Članci:

1. Udovičić, A. et al. (2013.) Analiza rizika upravljanja poduzećem. Praktični menadžment. Vol. IV. Br. I. str. 50.-60.
2. Uršulin Trstenjak, N. et al. (2014.) Implementacija sustava i aplikacija softvera za monitoring sustava sigurnosti hrane u djelatnosti ugostiteljstva. Tehnički glasnik. Vol. 8. No. 2. Str. 166.-170.

Internet izvori:

1. Casts software (2018.) Risk Management in Software Development and Software Engineering Projects. Dostupno na: https://www.castsoftware.com/research-labs/risk-management-in-software-development-and-software-engineering-projects (06.09.2018.)
2. CIS (2018.) Osnove upravljanja rizikom. Dostupno na: https://www.cis.hr/files/Celuska-Osnove_upravljanja_rizikom.pdf (27.07.2018.)
3. Galinac, T. (2018.) Uvod u programsko inženjerstvo. Dostupno na: http://www.riteh.uniri.hr/zav_katd_sluz/zr/nastava/proginz/materijali/Uvod_u_programsko_inzenjerstvo.pdf (25.07.2018.)
4. IEEE (2018.) Publications. Dostupno na: https://www.ieee.org/publications/index.html (25.07.2018.)

5. Software testing help (2018.) Types of Risks in Software Projects. Dostupno na: https://www.softwaretestinghelp.com/types-of-risks-in-software-projects/ (06.09.2018.)
6. Spremić, M. (2009.) Informatički rizici. Dostupno na: http://www.icti.svijetosiguranja.hr/userfile *(27.07.2018.)*
7. Try Engineering (2018.) What does a Computer Software Engineer do? Could you give me a description of the field?. Dostupno na: http://tryengineering.org/ask-expert/what-does-computer-software-engineer-do-could-you-give-me-description-field (06.09.2018.)
8. Uremović, D. (2009.) Kako upravljati IT rizicima. Dostupno na: http://www.infotrend.hr/clanak/2009/6/kako-upravljati-it-rizicima,37,767.html (27.07.2018.).
9. Znanje (2018.) Osnove računara. Dostupno na: http://www.znanje.org/abc/tutorials/computer_basic/01/060_software.htm (25.07.2018.).

POPIS SLIKA

Slika 1. Programski proizvod ili sustav 6
Slika 2. Vrste softvera – hijerarhijska podjela 6
Slika 3. Programski proces 8
Slika 4. Životni ciklus programskog proizvoda 9
Slika 5. Vrste rizika 11
Slika 6. Proces upravljanja rizikom 13
Slika 7. Analiza rizika 15
Slika 8. Vrste IT rizika 18
Slika 9. Proces procjene rizika u programskom inženjerstvu 21

POPIS TABLICA

Tablica 1. Metodologije za upravljanje rizicima u programskom inženjerstvu 19
Tablica 2. Primjeri rizika 25
Tablica 3. Kvantitativna skala vrijednosti imovine, prijetnje i ranjivosti 26
Tablica 4. Rezultati procjene rizika 27

SAŽETAK

Programsko inženjerstvo široko je znanstveno područje koje se između ostaloga odnosi na programiranje, ali i menadžment u informatici. Menadžment implicira upravljačke funkcije, pa je, između ostaloga, orijentiran i na upravljanje rizicima u programskom inženjerstvu. Riječ je o esencijalnom procesu koji generira krajnju kvalitetu poslovanja, ali i zadovoljstvo dionika.

Rizici se načelno razmatraju u negativnom kontekstu, no to nije sasvim ispravno. Često oni mogu biti pozitivnog karaktera, a tada predstavljaju mogućnost i priliku. Upravljanje takvim rizicima ima za cilj maksimiziranje koristi pa je poznavanje istih vrlo značajno i korisno.

Procjena rizika u programskom inženjerstvu prva je faza procesa upravljanja rizicima. Ona se odnosi uglavnom na identificiranje, kvantificiranje i opisivanje rizika, ali i na predlaganje kontrole te izradu dokumentacije. Osim što služi sadašnjim potrebama, koristi se i za buduće potrebe.

Ključne riječi: programsko inženjerstvo, menadžment, rizik, procjena rizika.

SUMMARY

Software engineering is a wide scientific field that, among the other things, is related to programming and IT management. Management implies board of management functions and, due that, is oriented to risk management in software engineering. It is an essential process that generates the ultimate quality of business, but also the satisfaction of all stakeholders.

Risks are generally considered in a negative context, but this is not entirely correct. Often they can have a positive character. In that case they present a possibility and an opportunity. Managing such risks aims to maximize the benefits and knowing it is very important and useful.

Risk assessment in software engineering is the first phase of the risk management process. It mainly refers to identifying, quantifying and describing risks, but also to suggesting control and document making. Apart from serving the present needs, it is also used for future needs.

Key words: software engineering, management, risk, risk assessment.