UDC: 37.018.43:004.7 Info M: str. 50-56

PRIMENA PDCA METODOLOGIJE U RAZVOJU BEZBEDNOSNOG MODULA U E-OBRAZOVANJU
APPLICATION OF PDCA METHODOLOGY FOR DEVELOPMENT OF SECURITY MODULE IN E-LEARNING

Marjan Milošević, Fakultet tehničkih nauka u Čačku, Univerzitet u Kragujevcu
marjan.milosevic@ftn.kg.ac.rs

REZIME: U radu je prikazan razvoj bezbednosnog modula integrisanog u okruženju za e-obrazovanje. Primenjena je popularna PDCA metodologija. Opisani su elementi razvoja po odgovarajućim fazama cikličnog procesa i prikazan primer implementacije u okruženju Moodle. Kroz razvoj modula formiran je model bezbednosti informacija u obrazovanju, dok je u završnoj fazi izvršena evaluacija u realnom okruženju sa studentima. Pokazano je da je PDCA metodologija efikasan sistematičan pristup u razvoju ne samo sistema za upravljanje bezbednošću (što je preporučeno standardom ISO 27001:2005), već i manjih podsistema, kao što je bezbednosni modul.
KLJUČNE REČI: bezbednost informacija, bezbednosni modul, e-obrazovanje, Moodle, PDCA
ABSTRACT: Paper presents development of a security module integrated in e-learning environment. The popular PDCA methodology was used. Elements of development are described according to the cyclic process phases and an example of implementation in LMS Moodle is shown. Throughout the module development a model of information security in e-learning is formed and in the final phase an evaluation was conducted with students involved. PDCA showed up to be an efficient approach not only for development of information security management systems (that is recommended by ISO 27001:2005 standard), but also for smaller subsystems, such as security module.
KEY WORDS: information security, security module, e-learning, Moodle, PDCA

1. UVOD

Popularnost e-obrazovanja beleži poseban rast pojavom masovnih otvorenih onlajn kurseva (MOOC) i inicijativa korišćenja otvorenih obrazovnih resursa (OER) [1]. Obrazovne ustanove različitog formata uključuju u svoje programe obrazovanja različite varijante elektronskog, onlajn održavanja nastave, bilo kroz varijantu kompletnog e-obrazovanja, bilo kroz kombinovanu, tzv. *blended learning* varijantu. Različite ustanove biraju različite oblike okruženja za e-obrazovanje, pa tako izbor rešenja varira od klasičnih statičkih veb-sajtova, do kompletnih okruženja za e-obrazovanje. Ostvarivanje kompletnih nastavnih aktivnosti koje odgovaraju tradicionalnoj nastavi, što podrazumeva raznovrsne vidove komunikacije i provere znanja, iziskuje kompleksno okruženje, koje podržava praćenje aktivnosti korisnika, predaju zadataka, rad sa testovima, grupnu i pojedinačnu komunikaciju. Ovakva okruženja poznata su kao sistemi za upravljanje učenjem (*LMS – learning management system*), a u nastavku teksta će se referisati kao okruženja za e-obrazovanje (ili samo okruženja). Pojedine varijante poseduju i autorske alate pomoću kojih nastavnici mogu kreirati sve što je potrebno za nastavu u samom softveru.

Primena okruženja za e-obrazovanje dovela je do promene paradigme obrazovanja i svakodnevne nastavne prakse. Umesto postavljanja obaveštenja na oglasnu tablu, koriste se forumi. Aktivnost na nastavi uključuje i aktivnost u okruženju. Ispitne sveske i skripte menjaju se elektronskim testovima i multimedijalnim materijalima itd. Ukratko: značajan deo po nastavu kritičnih aktivnosti sve više se odvija u elektronskoj formi korišćenjem nekog okruženja za e-obrazovanje (BlackBoard, Moodle, Sakai…). Ovakav trend bi trebalo da bude propraćen intenzivnijim interesovanjem za pitanja bezbednosti informacija, međutim u praksi to nije u potpunosti ostvareno [2].

U ovom radu se predlaže rešenje u vidu bezbednosnog modula. Ovaj modul bi bio integrisan u okruženju za e-obrazovanje, na taj način olakšavajući administraciju i komunikaciju sa korisnicima. Takođe, jedna od ideja je da se alati koje sama okruženja već poseduju, iskoriste od strane modula za ostvarenje bezbednosnih ciljeva.

Von Solms u radu intrigantnog naslova “10 smrtnih grehova u upravljanju bezbednošću informacija” definiše kao “4. greh”: “Neuviđanje da plan bezbednosti informacija mora biti zasnovan na analizi rizika” [3]. Paušalno tretiranje pretnji i rizika može dovesti do toga da se na malo verovatne rizike troše značajni resursi, dok se verovatniji rizici zanemaruju. Ovaj postulat se može primeniti i kod bezbednosti u e-obrazovanju. Za ostvarenje ideje projektovanja bezbednosnog modula potrebno je izabrati određenu metodologiju. Osim same metodologije razvoja softvera, neophodan je još jedan “sloj”, u kojem bi se prvo definisali sami bezbednosni zahtevi i formirali odgovarajući modeli, koji bi kasnije bili ulaz za razvoj samog softverskog rešenja.

“Proces, a ne proizvod” [4]. Ova rečenica poznata je i kao “Šajnerova mantra” zbog čestog ponavljanja i možda na najbolji način ilustruje beskonačnu cikličnu prirodu bezbednosti informacija. Kontinualni razvoj tehnologija i novih pretnji podrazumeva stalni rad na unapređenju mehanizama zaštite uz određenu dozu repetitivnosti, tako da nije moguće definisati bezbednost kao konačan proizvod. Ovakvo ciklično svojstvo nije karakteristično samo za bezbednost informacija, već i za različite poslovne procese. U tom smislu razvijeni su i modeli kojima se opisuje neprekidan kružni tok aktivnosti, kao i odgovarajuće metodologije kojima se pokušava unaprediti funkcionisanje u određenom domenu. Među najpoznatijim je PDCA, znana još i kao Demingov krug [5].

Faze PDCA metodologije su: Planiranje (P - Plan), Implementacija (D – Do), Provera (C- Check) i Ispitivanje/Poboljšavanje (A – Act). Standardi serije ISO 27000 u prethodnoj verziji su favorizovali PDCA kao pristup u implementaciji bezbednosnog informacionog sistema [6], dok je u novim verzijama predviđeno da se mogu koristiti i druge metode kontinualnog razvoja [7].

PDCA enkapsulira više elemenata konceptualizacije i razvoja modula. Modul u svom konačnom obliku, odnosno u implementiranom stanju, predstavlja softver. U tom smislu, potrebno je razviti ga kroz neku od opšteprihvaćenih metodologija razvoja softvera. PDCA je nivo iznad. PDCA enkapsulira sam razvoj softvera kao deo faze PDCA.

Faze razvoja i pripadajućih aktivnosti su sledeće:

Planiranje (Plan):

Definisati procese koji su od značaja za formiranje modela bezbednosti e-obrazovanja. Definisati ciljeve zaštite i zaštitnih mehanizama (kontrola) uzimajući u obzir ciljeve sistema i zahteve kvaliteta vezane za bezbednost. Izvršiti analizu rizika. Formirati odgovarajuću arhitekturu. Odrediti prioritete rizika i ingerencije samog modula unutar arhitekture, odnosno unutar sistema za e-učenje.

Implementacija (Do):

Implementirati izabrane zaštitne mehanizme. Potrebno je prevesti arhitekturu, odnosno njene delove u odgovarajući modul, razviti softver i implementirati njegove funkcije. Potrebno je opredeliti se za odgovarajuću metodologiju razvoja softvera, koja odgovara nameni.

Provera (Check): Izvršiti praćenje rada modula, njegov uticaj na prihvaćenost i poverenje kod korisnika. Potrebno je evidentirati i dokumentovati eventualne greške (bagove) i sakupiti povratne informacije od korisnika.

Poboljšavanje (Act): Definisati korektivne mere na osnovu povratnih informacija od korisnika, odnosno od mehanizama za praćenje rada modula, kao i na osnovu procedura za evaluaciju bezbednosti.

U nastavku su definisane razvojne aktivnosti po fazama PDCA, kao i njihova realizacija i "zatvaranje" kruga kroz evaluaciju u realnom okruženju i predloge unapređenja.

2. PLANIRANJE (FAZA P)

Na bezbednost utiče niz parametara i pravilno modelovanje je od dragocenog značaja za uspostavljanje odgovarajućih mehanizama zaštite.

U fazi planiranja neophodno je:

- Identifikovati okvire sistema, relevantne procese, dobra (assets) i tehnologiju
- Definisati politiku bezbednosti informacija
- Definisati pristup ispitivanju rizika
- Identifikovati rizike
- Analizirati i proceniti rizike
- Identifikovati i proceniti opcije za tretiranje rizika
- Ustanoviti ciljeve kontrola i kontrole za tretiranje rizika

U nastavku će biti dat kratak pregled ove faze.

E-učenje je distribuirana multidisciplinarna delatnost. Samim tim postoji izvesna složenost u definisanju domena i određivanju faktora kada je reč o bezbednosti.

Specifičnosti upravo diktiraju didaktički zahtevi koji se postavljaju pred e-obrazovanje.

- Dostupnost učenja sa bilo kog mesta.
- Mogućnost kolaborativnog rada..
- Uključivanje spoljnih resursa

Druge specifičnosti e-obrazovanja koje zahtevaju posebnu pažnju su:

- Elektronska provera znanja.
- Dodatna prava pristupa i nadgledanja aktivnosti učenika

Jedan od vitalnih faktora koji figuriše u bezbednosti je upravo korisnik. Pojedini autori su čak decidirani da je korisnik "najslabija karika" u bezbednosti [8], [9]. Korisnici pristupaju okruženju za e-učenje koristeći svoju klijentsku platformu. Svaki korisnik se identifikuje koristeći određen mehanizam autentifikacije i mapira u određenu kategoriju korisnika sa resursima kojima može pristupati.

U e-obrazovanju mogu se definisati različite kategorije korisnika, sa specifičnim pravima. Uobičajene osnovne klase korisnika su: administrator, nastavnik, učenik i gost. Sa strane modula koji se projektuje potrebno je pratiti ponašanje korisnika sa ulogama učenika i nastavnika, dok bi korisnik sa ulogom administrator dobijao odgovarajuće informacije i konfigurisao akcije samog modula.

Svaki korisnik poseduje određene lične podatke, koji čine njegov profil. Pored statičkih ličnih podataka (npr. i-mejl adresa, broj telefona), učenici mogu imati i druge podatke, od kojih su neki dinamični i prate njihovo učenje: na kojim su kursevima upisani, rezultate testova, lične fajlove itd. Dakle, postoje podaci profila i podaci procesa učenja. Takođe, mogu se pratiti pristup i aktivnosti svakog korisnika u okruženju. Ovaj segment je značajan za planiranje samog modula i kasniju realizaciju.

Kursevi predstavljaju sklop određenih sadržaja i aktivnosti strukturiranih u jednu celinu. Kurs se može sastojati iz raznovrsnih resursa, koji mogu uključivati sadržaje specifične za samu platformu, odnosno standardizovane pakete i druge spoljne resurse. Sadržaji koji se koriste u nastavi mogu podlegati autorskim pravima.

Osnovni bezbednosni ciljevi

Svaki proces ima određene definisane ciljeve koji su prioritetni i uslovljavaju pravilno funkcionisanje. Kod e-obrazovanja, mogu se definisati sledeći ciljevi procesa:

- Kontinuitet procesa učenja. Odnosi se na dostupnost resursa svim legitimnim korisnicima koji imaju Internet-konekciju.
- Omogućavanje što šireg dijapazona komunikacionih metoda i oblika učenja.

- Praćenje aktivnosti učenika i njegovog napretka.
- Očuvanje privatnosti ličnih informacija u skladu sa važećim regulativama.
- Očuvanje autentičnosti i privatnosti informacija o učenju, odnosno napretku.
- Sprovođenje provere znanja onlajn.
- Očuvanje autorskih prava resursa.

Polazeći od osnovnih principa bezbednosti: CIA, dalje se mogu bliže definisati bezbednosni ciljevi.

Posmatrajući e-obrazovanje i njegove ciljeve, mogu se definisati sledeći ciljevi vezani za poverljivost:

- Ograničenje pristupa resursima kursa. Samo ovlašćenim (autentifikovanim i autorizovanim) korisnicima može se dozvoliti pristup informacijama samog kursa: materijalima, aktivnostima itd.
- Ograničenje pristupa ličnim podacima. Pristup podacima učenika moguć je samo prema definisanim pravima u određenom kontekstu.
- Tajnost podataka za prijavu, uključujući i sredstva za autentifikaciju u bilo kom obliku. Isključivo autorizovani korisnici mogu učestvovati u e-obrazovanju obavezno pod svojim identitetom.

Integritet (celovitost):

- Pravo izmene informacija bilo kog oblika imaju jedino autorizovani korisnici. To se odnosi na resurse za učenje, lične podatke, parametre samog okruženja itd.
- Celovitost rezultata i ocena je od kritičnog značaja.

Raspoloživost:

- Podrazumeva dostupnost servisa e-učenja uz zadovoljavajuće performanse. Performanse mogu zavisiti od bezbednosti, ali su i pitanje planiranja i optimizacije okruženja, odnosno njegove skalabilnosti.

Autentifikacija i autorizacija

Kroz proces autentifikacije proverava se identitet korisnika, zatim se autorizuje, tj. odobrava se (ili ne) pristup servisima i određuje koji oblik pristupa postoji. Autentifikacija se može vršiti na osnovu onoga što korisnika zna (npr. lozinka), onoga što ima (identifikaciona kartica) ili onoga što jeste (biometrijske metode: sken rožnjače, otiska prstiju).

E-obrazovanje je specifično po tome što učenik, kao i član bilo koje druge kategorije korisnika, može biti lociran na bilo kom mestu, odnosno pristupati sa bilo koje platforme. Iako su izgrađena određena rešenja koja podrazumevaju nadgledanje korisnika [10], ona nisu ozbiljnije zaživela u praksi i ono što preostaje kao opcija se uglavnom svodi na dobro poznati sistem autentifikacije korišćenjem korisničkog imena i lozinke.

Autentifikacija može biti integrisana sa drugim sistemima kroz primenu jedinstvenog pristupa *(SSO - Single Sign On):* isti izvor podataka koristi se za autentifikaciju za različite sisteme. To dalje onda znači da politika lozinki može biti diktirana nezavisno od samog okruženja za e-učenje. Iako se sa jedne strane preporučuje SSO, a takve zahteve postavljaju i pojedine šeme obezbeđenja kvalitet [11] , postoje i analize koje pokazuju loše strane ovog pristupa [12].

Politika lozinki je jedan od bitnih elemenata koji se mora definisati i sastavni je deo bezbednosne politike. Poseban je izazov definisati politiku koja će sa jedne strane omogućavati korišćenje jakih lozinki, a sa druge strane biti poštovana u smislu upotrebljivosti, pamtljivosti, strategija beleženja i sl. Na rizike koje donosi ovaj pristup potrebno je posebno obratiti pažnju pri izgradnji modula.

Interoperabilnost

Okruženje za e-obrazovanje u užem smislu nije izolovana celina. Pored toga što je integrisan u informacioni sistem ustanove, postoji i interoperabilnost na nivou drugih sistema, odnosno na nivou nastavnih materijala. Na primer. povezivanje sa spoljnim storage servisima, kao što je GoogleDrive ili sa e-portfolio sistemima, kao što je Mahara. Paradigma e-obrazovanja usko je povezana sa fleksibilnošću i u tom smislu potrebno je omogućiti protok podataka između dva sistema, što donosi nove potencijalne rizike.

Bezbednost okruženja za e-obrazovanje

Okruženje je središnji deo infrastrukture za e-učenje i uglavnom je realizovan u vidu veb-aplikacije. Bezbednost okruženja može se analizirati sa aspekta slojevitosti koja se podrazumeva kod aplikacije ovog tipa, što podrazumeva bezbednost na nivou hardvera, softvera, pratećih servisa itd. Istraživanja iz ove tematike bilo je u više navrata i mogu se pogledati npr. u [13].

Predviđa se da modul predstavljen u ovom radu deluje na krajnjem, aplikativnom sloju, u ravni samog okruženja za e-obrazovanje. U tom smislu domen delovanja domena ne uključuje kompletnu infrastrukturu (operativni sistem, mrežu).

Bezbednosna politika i uslovi korišćenja sistema

Važno je da bezbednosna politika bude ustanovljena i dobro dokumentovana [14], ali i što bolje raširena među korisnicima. Istraživanje stanja u e-obrazovanju u Srbiji pokazalo je da najčešće uopšte ne postoji bezbednosna politika, niti kao poseban dokument, niti kao deo politike korišćenja sajta na primer [15].

Kako sugeriše ISO 27002, politika treba da bude definisana na nivou institucije, a onda slede politike na nižim nivoima, kojima se detaljnije definišu potrebe i otvara prostor za uspostavljanje odgovarajućih kontrola. Poseban skup regulativa odnosi se na politiku krajnjeg korisnika. U standardu se navodi (na str. 9) [16]:

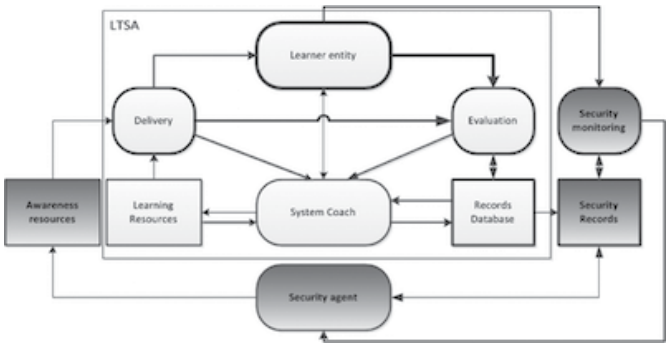
"Ove politike treba da budu saopštene zaposlenima i odgovarajućim eksternim stranama u obliku koji je odgovarajući, prihvatljiv i razumljiv čitaocu, npr. u kontekstu „upoznavanja sa bezbednošću informacija, programa obrazovanja i obuke"

Modul treba da bude usklađen sa bezbednosnom politikom, a korisnici upoznati sa njenim elementima koji se tiču prava i obaveza samih korisnika. U tom smislu neophodno je diseminirati informacije o pravima pristupa i dobroj praksi među korisnicima, što se može definisati kao još jedan zadatak modula.

Odnos modula i arhitekture sistema obrazovne tehnologije

Kako bi modul bio integrisan u procese e-obrazovanja, precizirano je njegovo mesto u standardnoj arhitekturi sistema za obrazovnu tehnologiju (LTSA - Learning Technology System Architecture) [17]. Ova arhitektura daje generički prikaz procesa u obrazovanju, primenjiv u faktički bilo kom edukativnom scenariju, od tradicionalne nastave do e-obrazovanje.

Modifikacija ove arhitekture formirana je kao seLTSA – security enhanced LTSA [18]. seLTSA predstavlja nadgradnju LTSA, pri čemu dodatni sloj upravo jeste bezbednosni modul. U najužem smislu, bezbednosni modul je agent koji orkestrira radom nadgrađenih elemenata (slika 1).



Slika 1 - *seLTSA arhitektura*

S obzirom na značaj praćenja informacija o korisniku, izvršena je nadgradnja standardnog profila korisnika (IMS LIP) [19] dodavanjem polja kojim se omogućava beleženje informacija o ponašanju relevantnom za bezbednost [18].

Analiza rizika

Ključan element u razvoju bilo kakvog bezbednosnog sistema, modula ili mehanizma zaštite je analiza rizika. U tabeli 1 dat je isečak analize rizika koji odgovaraju okruženju za e-obrazovanje.

Tabela 1 - *Izvod iz tabele analize rizika*

Pretnja	Rizik	Zaštitni mehanizam
Korisnik postavlja zaražen fajl	Drugi korisnici preuzimaju fajl i zaražavaju svoje računare. Integritet sistema je narušen, pojavljuju se reklame itd.	Korisnik se obaveštava o riziku, bezbednosni kapacitet (vrednost u profilu) opada, administrator dobija dodatne informacije
Korisnik se ne odjavljuje sa sistema nakon korišćenja	Dolazi do neautorizovanog pristupa drugih osoba	Korisniku se smanjuje vrednost loginadmin korisnikovog profila, na osnovu koje se prezentuju odgovarajuće informacije o bezbednosnoj kulturi. Korisnik dobija posebne savete o potrebi odjave.
Korisnik šalje veliki broj privatnih poruka	Drugi korisnici dobijaju spam	Korisnik je informisan o bezbednosnoj politici, smanjen je njegov bezbednosni kapacitet (vrednost u profilu) i proverava se korisnikov nivo svesti o bezbednosti - na osnovu čega se eventualno vrši restrikcija prava pristupa
Pristup podacima profila nije kontrolisan	Korisnik dobija neželjenu poštu ili čak biva uznemiravan na druge načine (skajp, telefon)	Korisnik može da samostalno definiše nivo privatnosti. Dodatno je informisan o tome kako da upravlja privatnošću.

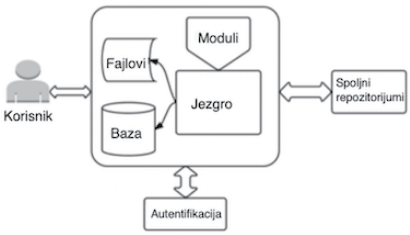
3. IMPLEMENTACIJA (FAZA DO)

U drugoj fazi PDCA razvoja modula vrši se upravo razvoj softvera. Pošto su u prethodnoj fazi definisani okviri procesa, analizirani rizici i kreirana arhitektura, sledi razvoj samog softverskog elementa.

Koncept modula do ovog trenutka je generički i dalji razvoj se može izvesti na izabranoj platformi i u različitim tipovima okruženja. Od ove tačke definiše se u kojem tačno okruženju se dalje razvija modul. Zbog svoje prirode otvorenog koda, dostupnosti obimne dokumentacije i podrške zajednice, izabran je Moodle [20]. Takođe, sa aspekta evaluacija Moodle je najpovoljniji izbor, jer se već koristi u autorovoj matičnoj instituciji.

Aspekti integracije

Da bi se realizovao modul, neophodno je izvršiti analizu arhitekture Moodle-a. Na slici 2 data je osnovna šema komponenti Moodle-a.



Slika 2 - *Komponente Moodle-a*

U središtu sistema je jezgro. Jezgro sadrži ključne elemente oko kojih su izgrađene sve ostale funkcionalnosti, na primer biblioteke funkcija za grafički prikaz, rad sa bazom, upravljanje događajima itd. Izmene jezgra su koordinisane od strane Moodle razvojnog tima. Bilo kakve samostalne izmene dalje mogu dovesti do problema sa ažuriranjem sistema novim verzijama, jer se pri svakoj nadgradnji menja i jezgro.

Širok spektar funkcionalnosti može biti realizovan kroz module, koji se u terminologiji Moodle-a nazivaju i plaginovi *(plugins)*. Kompletna lista dostupnih vrsta modula data je na zvaničnom sajtu [21]. Određeni plaginovi su već deo jezgra, dok ostali mogu da se naknadno dodaju. Pojedini plaginovi koji se pokažu kao veoma korisni, vremenom mogu postati deo jezgra i tada se isporučuju sa osnovnom instalacijom.

Događaji su pojave koje sadrže određene informacije o različitim aktivnostima. Na primer, napisana poruka na forumu, kreiranje novog korisnika, detekcija malicioznog softvera itd. Mehanizmom događaja prenose se informacije između različitih delova sistema, kroz model proizvođač/pretplatnik (producer/subscriber). Događaji su definisani kao izdvojeni elementi koji se zatim aktiviraju u određenim segmentima aplikacije, a zatim se vrši pozivanje funkcija (hendlera) koje su pretplaćene na događaje. Ovakav pristup omogućava veoma jednostavno asinhrono povezivanje modula sa jezgrom i pretplatu na postojeće događaje, kao i kreiranje novih događaja. U verzijama 2.7 i novijim administrator može da se pretplati na bilo koji događaj i dobije obaveštenja ukoliko se pojavi češće od zadatog broja puta.

Bezbednost je uvek suprotstavljena korisničkom iskustvu i pronalaženje balansa je izazov koji je konstantan predmet istraživanja. Agent koji se realizuje u ovom radu sam po sebi nije bezbednosni mehanizam u konvencionalnom smislu. Krajnji korisnik u stvari nema direktne interakcije sa agentom u smislu da koristi određene bezbednosne kontrole, podešava ga itd. Takođe, agent ne štiti direktno i proaktivno u maniru u kojem to radi antivirusni softver, na primer. Osnovna uloga agenta jeste da prati ponašanje korisnika i samog korisnika (i administratora) obaveštava o akcijama koje su poželjne ili ne, o načinima za unapređenje bezbednosne svesti, kao i da mu pomogne da koristi pojedine, već postojeće bezbednosne kontrole. Činjenica da korisnik uglavnom ne upravlja ponašanjem agenta ne znači da agent ne bi mogao da naruši kvalitet upotrebljivosti (usability) osnovnog sistema. Upravo u tome je osnovni izazov dizajna ovakvog agenta. Takođe, elementi komunikacije koje agent ima sa administratorom sistema dodaju dimenziju pasivnog IDS-a (sistema za detekciju upada): administrator je obavešten o određenim incidentima ili promenama koje bi mogle biti značajne za sistem i na njemu je da dalje preduzme određene mere.

Na slici 3 prikazana su tri osnovna aspekta delovanja modula.

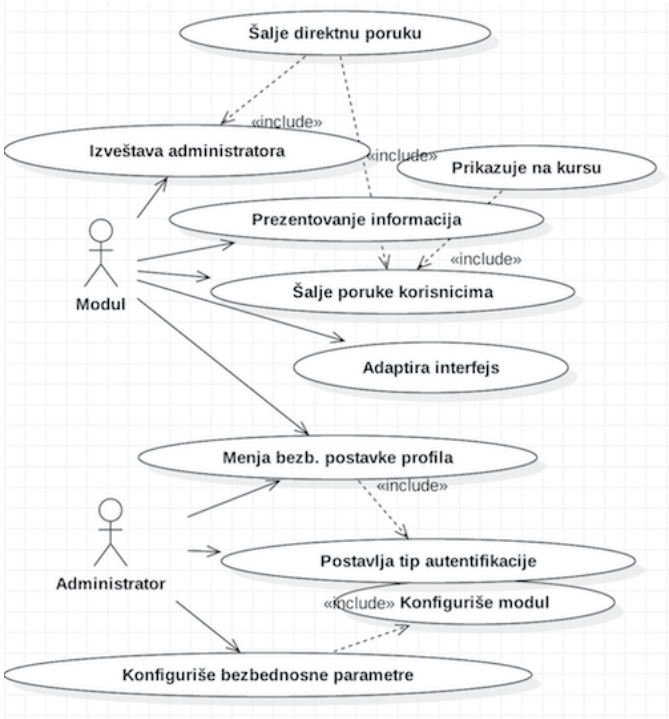
Slika 3 - *Aspekti delovanja modula*

Za potrebe što efikasnijeg i kvalitetnijeg projektovanja softvera, ustanovljene su različite metodologije razvoja [22]. Izbor konkretne metodologije zavisi od samog softvera, odnosno zahteva klijenta, kompleksnosti i vremenskih rokova.

Za razvoj softvera izabran je pristup brze izrade prototipa. U prilog ovom izboru idu sledeći argumenti:

- Ulazni parametri nisu fiksni, tj. zahtevi nisu kompletno poznati na početku razvoja, već se mogu pojaviti i dodatni zahtevi
- Postoji određen stepen interaktivnosti korisnika i modula
- Potrebno je što pre doći do povratnih informacija, koje bi doprinele doradi modula, ali i koje bi bile pokazatelj o tome kakav je širi uticaj samog modula

Na slici 4 prikazan je jedan dijagram slučajeva korišćenja.



Slika 4 - *Slučaj korišćenja "Upravljanje bezbednošću"*

Za pisanje koda i implementaciju korišćeni su NetBeans [23], Windows 7 i XAMPP paket [24], kao i Moodle 2.9.

4. FAZA PROVERE (FAZA CHECK)

Naredna faza PDCA ciklusa jeste *Check* faza - faza provere. U ovoj fazi izvršeno je testiranje modula, kao i provera njegovog uticaja na poverenje i prihvatanje tehnologija.

Za potrebe istraživanja korišćena je platforma navedena u prethodnom poglavlju. Sajtu je omogućen pristup preko adrese Laboratorije za informacione tehnologije na Fakultetu tehničkih nauka u Čačku (itlab.ftn.kg.ac.rs:8000/moodle).

Registracija je otvorena, a testni kurs je zaštićen lozinkom, kojom je regulisan upis.

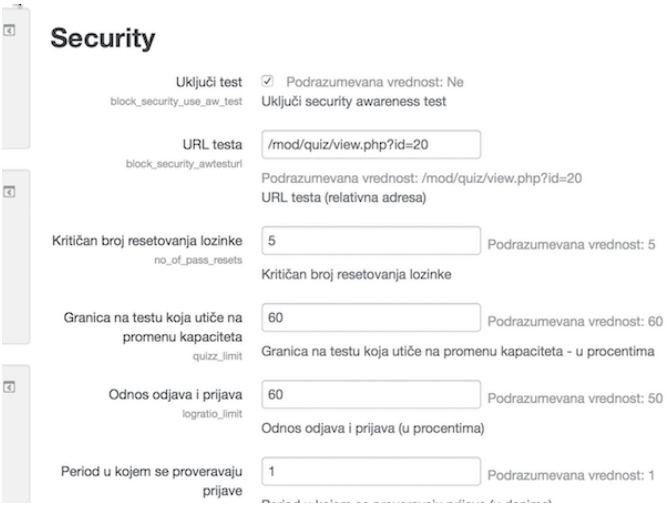
Istraživanje je trajalo od 20. novembra 2015. do 31. januara 2016. Na Moodle sistemu sa implementiranim modulom postavljen je kurs "Tehnologije i alati za ocenjivanje" i upisano 35 polaznika. Formirane su 4 nastavne teme sa različitim oblicima sadržaja. Svake sedmice otvarana je po jedna nova tema, čime se održavala dinamika. Nastavni sadržaji su izabrani tako da ne budu previše teški i da svojom zanimljivošću motivišu polaznike da posećuju kurs.

Polaznicima nije predočeno šta se tačno ispituje sa ciljem da se ne utiče na njihov način korišćenja sajta i kursa, kako bi se na kraju dobili što validniji podaci za analizu. Sve vreme trajanja kursa, polaznici su od nastavnika (autora) dobijali zadatke i informacije kao na klasičnom sistemu, bez naglašavanja značaja bezbednosti. Nije bilo sugerisanja o načinu korišćenja sajta, o tome da li treba rešavati test vezan za bezbednost itd. Da bi se proverilo kako sam modul utiče na poverenje u sistem i prihvaćenost e-učenja, učinjen je maksimalan napor da se ostvari realno okruženje, u kojem bi modul samostalno prezentovao određene informacije na kursu, slao poruke i obavljao svoje aktivnosti bez upliva i dodatnih objašnjavanja od strane administratora ili drugih lica. (Na svaki zahtev za korisničku podršku je odgovoreno, međutim nije ni na koji način dodatno skretana pažnja na bezbednosne kontrole, niti indukovana potražnja za podrškom - ambijent je maksimalno približen realnom sistemu.)

Po završenom kursu, polaznici su popunili dva upitnika. Cilj upitnika bio je ispitivanje: da li i kako modul utiče na prihvaćenost sistema za e-učenje i koliko utiče na poverenje korisnika (polaznika) u e-obrazovanje. Upitnici su formirani na osnovu modela predstavljenih u samom radu, konkretno: [25] и [26] за poverenje, a za prihvatanje modifikovani TAM [27], [28]. Upitnici su realizovani kroz modul Questionnaire u samom okruženju.

Rezultati uticaja modula na poverenje dati su u [29]. Uticaj modula na prihvaćenost tehnologija je delimično potvrđen.

Prilikom korišćenja sajta i samog kursa, korisnici su imali mogućnost da rešavaju test kojim se proverava bezbednosna svest. Ovaj test nije obavezan, već se pojavljuje povremeno u okviru bloka, kao opcija. Administrator konfiguriše test unosom URL-a u svom konfiguracionom panelu (slika 5)



Slika 5 - *Konfiguracija modula*

Ukoliko korisnik odluči da rešava test, to će uticati na njegov kapacitet, tj. ažuriraće se bezbednosni profil. Test se može rešavati neograničen broj puta, uz zadatu minimalnu pauzu između više pokušaja. Test su rešavala 23 korisnika i pri tom je ostvaren prosečan uspeh 7,73 (od 10). Ukupan broj pokušaja je 34. To pokazuje da su korisnici bili zaintersovani da poboljšaju svoj uspeh - samostalno inicirajući ponovne pokušaje rešavanja.

Korisnici su izneli različite pozitivne utiske vezane za sam sajt i kurs, međutim nije bilo posebnih naznaka da su studenti prepoznali da je sam sajt (okruženje) bezbedniji od sajta koji inače koriste za e-učenje.

Pojedini korisnici imali su problem sa autentifikacijom, koji je direktno prouzrokovan radom modula. Problem je nastao tako što je njihov tip autentifikacije promenjen na 2-faktorski, uz slanje odgovarajuće informacije kako se prijaviti uz token. Međutim, pošto je predviđeno da se token generiše sa Android uređaja, korisnici koji imaju neki drugi sistem, ostali su uskraćeni za tu informaciju. Na kraju su samostalno otkrili kako se i preko PC-a može generisati token. Ovaj slučaj je još jedan indikator o potrebi olakšavanja pristupa bezbednosnim kontrolama.

5. FAZA POBOLJŠAVANJA (ACT)

Kroz prethodne faze modul je izgrađen i testiran. U poslednjoj fazi (uslovno rečeno, jer ciklična struktura PDCA predviđa ponavljanje faza), sumiraju se opažanja i formulišu predlozi za unapređenje, koji se kasnije implementiraju u narednom ciklusu.

Tehnička relizacija samog modula mora biti predmet revizije: počevši od implementacije novih funkcije, pa do olakšavanja pristupu bezbednosnim kontrolama. Predviđa se ponovna analiza rizika i obuhvatanje novih relevantnih pretnji. Sa novim verzijama okruženja i uvođenjem novih elemenata u funkcionisanju (na primer dodatnih metoda autentifikacije

Analiza rada modula dovela je do sledećih predloga za unapređenje:

- Implementacija novih mogućnosti *(features)* u modulu, uključujući bolju podršku za različite klijentske platforme

- Integracija svih funkcija bezbednosti (postojećih i novih metoda) radi upravljanja kroz jedan administrativni modul koji bi mogao da generiše i odgovarajuće izveštaje.
- Primena naprednih metoda obrade podataka (rudarenje podataka, mašinsko učenje) i metoda veštačke inteligencije za rad modula.
- Uvođenje novih elemenata učenja zasnovanog na igri u svrhu unapređenja bezbednosti korisnika i testiranje uspešnosti ovakvog pristupa.

6. ZAKLJUČAK

Kroz rad je pokazano da se PDCA može uspešno primeniti u razvoju modula za bezbednost u e-obrazovanju. Faza planiranja je univerzalna i nije vezana ni za jedan poseban sistem. U kasnijim fazama vrše se razvoj i testiranje samog softvera, koji je neposredno vezan za konkretno izabrano okruženje.

Modul je pokazao značajan uticaj na poverenje, dok je kod prihvatanja tehnologija uticaj nedovoljno potvrđen. Na osnovu rezultata testiranja modula u praksi, kao i na osnovu istraživanja uticaja na poverenje i prihvatanje tehnologija i povratnih informacija korisnika, dobijeni su ulazni parametri za naredni krug ciklusa. To podrazumeva potencijalne promene same arhitekture, reviziju analize rizika, implementaciju novih fukcija modula itd.

U radu je potvrđena opravdanost primene metode u razvoju bezbednosnih elemenata različite granulacije i u specifičnom kontekstu. U ovom slučaju reč je o integralnom delu okruženja za e-obrazovanje, međutim elementi razvoja pokazani u radu imaju potencijal korišćenja i u drugim predmetnim sistemima u kojima je potreban sistematičan pristup bezbednosti.

LITERATURA

[1] J. L. Hilton III, C. Graham, P. Rich, i D. Wiley, „Using online technologies to extend a classroom to learners at a distance“, *Distance Education*, sv. 31, izd. 1, str. 77–92, 2010.

[2] Y. Chen i W. He, „Security risks and protection in online learning: A survey“, *The International Review of Research in Open and Distributed Learning*, sv. 14, izd. 5. 31-lis-2013.

[3] B. von Solms i R. von Solms, „The 10 deadly sins of information security management“, *Computers & Security*, sv. 23, izd. 5, str. 371–376, srp. 2004.

[4] B. Schneier, *Secrets & Lies Digital Security in a Networked World*. New Jersey: John Wiley & Sons, 2000.

[5] P. Arveson, „The Deming Cycle“, *Balances Scorecard Institute*, 1998. [Na internetu]. Dostupno na: http://balancedscorecard.org/Resources/Articles-White-Papers/The-Deming-Cycle.

[6] ISO, „INTERNATIONAL STANDARD ISO / IEC techniques — Information security“, sv. 2010. 2010.

[7] „Moving from ISO/IEC 27001:2005 to ISO/IEC 27001:2013“. BSI UK.

[8] S. Lineberry, „The Human Element: The Weakest Link in Information Security“, *Journal of Accountancy*, sv. 204, str. 44–49, 2007.

[9] R. Woerner, „Fixing the weakest link in your security chain : People“, *Security Magazine*, izd. December, str. 60–62, 2012.

[10] S. Ribarić, B. Dalbelo Bašić, Z. Kalafatić, T. Hrkać, i I. Fratrić, „System for Biometric Authorization of Internet Users Based on Fusion of Face and Palmprint Features“, 2005. [Na internetu]. Dostupno na: http://www.zemris.fer.hr/projects/Biometrics/english/results.shtml. [Pristupano: 12-nov-2014].

[11] EFQUEL, „UNIQUE Information Package“, 2011. [Na internetu]. Dostupno na: https://www.efmd.org/projects-test?download=6:06-unique-guidelines-2011. [Pristupano: 01-jan-2013].

[12] A. Armando, R. Carbone, L. Compagna, J. Cuéllar, G. Pellegrino, i A. Sorniotti, „An authentication flaw in browser-based Single Sign-On protocols: Impact and remediations“, *Computers & Security*, sv. 33, str. 41–58, mart 2013.

[13] D. Costinela-Luminita, „Information security in E-learning Platforms“, *Procedia - Social and Behavioral Sciences*, sv. 15, str. 2689–2693, 2011.

[14] M. E. Whitman, „Security Policy: From Design to Maintenance“, *Advances in Management Information Systems*, sv. 11, str. 123–151, 2008.

[15] M. Milosevic, R. Krneta, i D. Milosevic, „Security and Privacy in On-Line Learning: Case Study from Serbia“, *Metalurgia International*, sv. 18, izd. 3, str. 85–88.

[16] ISO, „SRPS ISO/IEC 27002:2015“. Институт за стандардизацију Србије, 2015.

[17] IEEE, „IEEE Standards IEEE Standard for Learning TEchnology - Learning TEchnology Systems Architecture (LTSA)“, *IEEE Standards*, sv. 9, izd. December. IEEE, str. 5–8, 2003.

[18] M. Milošević i D. Milošević, „Defining the e-learner's security profile: Towards awareness improvement“, *Sadhana*, sv. 41, izd. 3, str. 317–326, 2016.

[19] L. E. Anido-Rifón, M. J. Fernández-Iglesias, M. Caeiro-Rodríguez, J. M. Santos-Gago, M. Llamas-Nistal, L. Álvarez Sabucedo, i R. Míguez Pérez, „Standardization in computer-based education“, *Computer Standards and Interfaces*, sv. 36, izd. 3, str. 604–625, 2014.

[20] M. Dougiamas, „Moodle“, 2011. [Na internetu]. Dostupno na: https://download.moodle.org/releases/legacy/. [Pristupano: 01-jan-2015].

[21] M. Dougiamas, „Moodle Plugin Types“, 2015. [Na internetu]. Dostupno na: https://docs.moodle.org/dev/Plugin_types. [Pristupano: 01-jan-2015].

[22] B. K. Jayaswal i P. C. Patton, *Design for Trustworthy Software: Tools, Techniques, and Methodology of Developing Robust Software*. Upper Saddle River, NJ, USA: Prentice Hall PTR, 2006.

[23] „NetBeans“, 2015. [Na internetu]. Dostupno na: https://netbeans.org.

[24] K. Seidler i K. Vogelgesang, „XAMPP“, 2016. [Na internetu]. Dostupno na: https://www.apachefriends.org/index.html.

[25] B. Y. D. Wang, „Building Trust in E-Learning“, *Athens Journal of Education*, izd. February, str. 9–18, 2014.

[26] E. Costante i J. Den Hartog, „On-line Trust Perception : What Really Matters“, u *Socio-Technical Aspects in Security and Trust (STAST), 2011 1st Workshop on*, 2011, str. 52–59.

[27] M. Lallmahamood, „An Examination of Individual ' s Perceived Security and Privacy of the Internet in Malaysia and the Influence of This on Their Intention to Use E-Commerce : Using An Extension of the Technology Acceptance Model“, *Journal of Internet Banking and Commerce*, sv. 12, izd. 3, str. 1–26, 2007.

[28] B.-C. Lee, J.-O. Yoon, i I. Lee, „Learners' acceptance of e-learning in South Korea: Theories and results“, *Computers & Education*, sv. 53, izd. 4, str. 1320–1329, 2009.

[29] M. Milošević i D. Milošević, „Enhancing trust in e-learning through security mechanisms improvement“, u *The seventh International Conference on eLearning*, 2016, str. 148–150.

Marjan Milošević, asistent na Fakultetu tehničkih nauka u Čačku
Kontakt: marjan.milosevic@ftn.kg.ac.rs
Oblasti interesovanja: e-obrazovanje, bezbednost informacija, računarske mreže, interakcija čovek-računar