Универзитет у Крагујевцу
Факултет техничких наука у Чачку

Мр Марјан Милошевић

РАЗВОЈ И ИМПЛЕМЕНТАЦИЈА БЕЗБЕДНОСНОГ МОДУЛА И ЊЕГОВ УТИЦАЈ НА КВАЛИТЕТ Е-ОБРАЗОВАЊА

Докторска дисертација

Чачак, 2016.

I Аутор	
Име и презиме:	Мр Марјан Милошевић, проф. тех. и инф.
Датум и место рођења:	13.10.1979. Горњи Милановац
Наслов магистарске тезе:	Моделовање рачунарског адаптивног теста према персоналним карактеристикама испитаника
Датум и место одбране тезе:	8.10.2008, Технички факултет Чачак
Област магистарске тезе:	Информационе технологије и системи
Садашње запослење:	Асистент на Факултету техничких наука у Чачку
II Докторска дисертација	
Наслов:	Развој и имплементација безбедносног модула и његов утицај на квалитет е-образовања
Број страница:	152
Број слика:	51
Број библиографских података:	145
Установа и место где је рад израђен:	Факултет техничких наука у Чачку, Универзитет у Крагујевцу
Научна област (УДК):	004.41:37.018.43.](043.3)
Ментор:	Др Данијела Милошевић, ванр. проф., Факултет техничких наука у Чачку
III Оцена и одбрана	
Датум пријаве теме:	24.04.2013.
Број одлуке и датум прихватања докторске дисертације:	332/14, 12.06.2013.
Комисија за оцену подобности теме и кандидата:	
1. Др Данијела Милошевић, ванредни професор, Факултет техничких наука у Чачку, Универзитет у Крагујевцу, научна област: Информационе технологије и системи 2. Др Живадин Мицић, редовни професор, Факултет техничких наука у Чачку, Универзитет у Крагујевцу, научна област: Информационе технологије и системи 3. Др Радојка Крнета, ванредни професор, Факултет техничких наука у Чачку, научна област: Рачунарска техника 4. Др Дејан Симић, редовни професор, Факултет организационих наука, Универзитет у Београду, научна област: информациони системи и технологије 5. Др Борислав Ђорђевић, доцент, Факултет техничких наука у Чачку, Универзитет у Крагујевцу, научна област: Рачунарска техника	
Комисија за оцену и одбрану докторске дисертације:	
1. Др Радојка Крнета, ванредни професор, Факултет техничких наука у Чачку, научна област: Рачунарска техника 2. Др Дејан Симић, редовни професор, Факултет организационих наука, Универзитет у Београду, научна област: Информациони системи и технологије 3. Др Владе Урошевић, редовни професор, Факултет техничких наука у Чачку, Универзитет у Крагујевцу, научна област: Примењене рачунарске науке и информатика	
Датум одбране дисертације:	

Предговор

Докторат је пре свега резултат ауторовог дугогодишњег интересовања и практичног и теоријског рада у области е-образовања. Данас су многе научне дисциплине испреплетане и тако је и е-образовање у ствари амалгам различитих научних дисциплина. Мултидисциплинарност је једна од основних одлика овог рада.

У истраживању је значајну улогу одиграло ауторово богато искуство у администрацији и пројектовању система за е-учење, као и наставном ангажовању на електронским курсевима. Аутор је био (и даље је) учесник бројних пројеката који се управо баве е-образовањем и одређеним специфичним облицима примена модерних технологија у настави (Темпус пројекти DL@Web, NeReLa, Incoming, затим национални пројекат Интелис, пројекти WUS-а итд.), чиме је добио додатне могућности за дубље проучавање феномена е-образовања и практичних аспеката примене информационих технологија у настави.

Докторат је сазревао више година и током израде су захваћени веома разноврсни аспекти е-образовања и употребљене различите технике за добијање потребних научних резултата. Спровођене су анкете, прикупљани подаци о е-образовању у Србији директним приступом, систематизовани су бројни стандарди који дотичу тематику самог е-образовања и безбедности информација и формирани нови модели. Од непроцењивог значаја је чињеница да је аутор имао приступ реалном систему за е-учење са великим бројем корисника, на којем је могао да спроводи потребне анкете, односно тестира модул.

Аутор верује и нада се да ће овај докторат својим теоријским и практичним резултатима уградити једну значајну циглу у зидине модерног, технолошки подржаног образовања, пре свега на матичном факултету, али и шире, у Србији, као и да ће пружити материјал истраживачима у овој области да даље проучавају тромеђу е-образовање/безбедност информација/квалитет.

Аутор се неизмерно захваљује својој породици на подршци и храбрењу у оним кључним моментима када се ”ломио резултат” дисертације и када је то било најпотребније.

Аутор се најсрдачније захваљује свом ментору, проф. Данијели Милошевић, која му је пружила драгоцену помоћ у напредовању кроз каткад наизглед непроходне врлети научно-истраживачког рада.

На крају, аутор се захваљује и члановима комисије, који су својим сугестијама допринели да докторат добије на квалитету и поприми коначни, заокружен облик.

У Чачку, маја 2016
Аутор

Резиме

Развој и имплементација безбедносног модула и његов утицај на квалитет е-образовања

Електронско образовање постало је саставни део модерног друштва знања. С обзиром на то да се највећим делом ослања на информационе технологије, поставља се питање какав утицај има безбедност информација на квалитет е-образовања и како се може унапредити безбедност корисника у окружењима за е-учење.

У докторату је приказан развој безбедносног модула. Овај модул креиран је са задатком да делује као интегрисани део окружења за е-учење: да прати корисникове активности, примењује мере заштите и дисеминира елементе безбедносне политике. Дати су опис имплементације, као и тока и резултата истраживања утицаја модула на конструкте који су повезани са квалитетом е-образовања: поверење у систем за е-учење и прихваћеност технологија.

Сам процес развоја заснован је на стандардима из области безбедности информација (ISO) и е-образовања (IEEE, IMS), а као улазни параметри узети су и критеријуми за обезбеђење квалитета. Целокупан развој, као и имплементација и евалуација модула спроведени су кроз PDCA циклус. Током пројектовања модула развијен је и холистички модел безбедности у е-учењу, надграђена је стандардна архитектура за е-учење и адаптиран модел ученика. Фокус модула је на кориснику, па је стога IMS модел ученика (IMS LIP) допуњен структуром која има за задатак да евидентира безбедносне параметре учениковог понашања. Овај допуњени модел саставни је део надграђене LTSA архитектуре, назване seLTSA, која за задатак има да пружи оквире за унапређење безбедности процеса е-образовања. Кључни део надградње је управо модул, eLearnion, који оркестрира безбедношћу. У сврху евалуације модула и провере хипотеза, модификовани су постојећи модели поверења и прихватања технологија.

Модул је реализован као додатак Moodle-а, окружења за учење отвореног кода, применом методе брзог развоја прототипа (rapid prototyping). Због захтева појединих функција за дубљом интеграцијом у само окружење, било је неопходно извршити и одређене измене језгра Moodle-а. Модул је имплементиран и тестиран у склопу е-курса на који су уписани ученици (студенти). Курс је трајао три месеца, након чега су ученици анкетирани.

Показано је да је применом стандарда из области безбедности информација могуће креирати модул који својим активностима доприноси испуњењу критеријума за обезбеђење квалитета. Потврђено је да је безбедност један од најутицајнијих фактора поверења корисника у систем за е-учење. Делимично је потврђено да су безбедносни елементи, формулисани кроз безбедносни модул, значајни за прихватање технологија.

кључне речи: е-образовање, безбедност информација, LTSA, Moodle, безбедносни модул

Abstract

Development and implementation of security module and its influence on quality of e-education

Electronic education has become an integral part of modern knowledge society. Having in mind that it mostly depends on information technology, a question is yielded on how the information security influences e-education quality and in what way the user security may be improved in learning environments.

The development of security module is shown in thesis. Module is created in order to act as integral part of the e-learning environment: to monitor user's activities, apply security measures and disseminate elements of information security policy. Description of implementation is given as well as flow and results of research of module's influence on construct coupled with quality such as trust in learning environment and technology acceptance.

The development process is based on standards in area of information security (ISO) and learning technologies (IEEE, IMS) and the e-learning quality criteria are taken as input. During the module design, a holistic model of security in e-learning was developed. Additionally, the standard e-learning architecture was upgraded and the standard learner model was adapted. Module is focused on user, therefore the IMS learner model (IMS LIP) is supplemented with structure with task of keeping security parameters of learner's behavior. This supplemented model is building block of upgraded LTSA architecture, called seLTSA, with goal of providing framework for security improvement of e-education processes. Key part of this upgrade is the very module, called eLearnion, which orchestrate with security. In favor of module evaluation and hypothesis check, the existing trust and technology acceptance models are modified.

Module is made as plugin for Moodle, open source learning environment, using the rapid prototype method. Because some function required deeper integration in the very environment, certain modification of Moodle code was needed. Modul is implemented and tested inside an e-course with students enrolled. Course lasted three months and learners were surveyed afterward.

It is shown that it is possible to create module whose activities contribute to fulfillment of quality assurance criteria by using information security standard. It is confirmed that security is very important factor of user trust in e-learning system. It is partly confirmed that security elements, formulated through security module, are significant for technology acceptance.

keywords: e-learning, e-education, information security, LTSA, Moodle, security module

Садржај

1. УВОД

1.1 Мотиви за рад

Модерно друштво је друштво знања. Тржишна економија поставља пред појединца императив сталног усавршавања, односно целоживотног учења. У таквим оквирима модерне технологије играју виталну улогу у савременом образовном процесу. Створене су и нове образовне парадигме: е-учење, мобилно учење, свеприсутно учење („ubiquitous learning“) [1] и др.

Корисници имају потребу за максималном флексибилношћу: приступом ресурсима и континуалној комуникацији, 24/7, у свом ритму и по свом временском распореду, са својих уређаја.

Ослањање на информатичке технологије отвара питања безбедности. Сваки прекид у раду, губитак података, нарушавање приватности или пад перформанси директно утичу на квалитет учења, али и компромитују саму образовну институцију, односно пружаоца услуга образовања. Стога је од нарочитог значаја заштитити систем и смањити вероватноћу отказа и нарушавања безбедности.

Обезбеђење квалитета у е-учењу је природан наставак третирања питања квалитета у образовању уопште. Захваљујући специфичностима овог вида наставе/учења развијене су посебне процедуре и шеме за обезбеђење квалитета на различитим нивоима: на нивоу установе, на нивоу студијског програма, појединачног курса или образовног софтвера. Пошто је квалитет е-учења повезан са безбедношћу, ове шеме кроз своје критеријуме третирају и питања безбедности.

Независно од намене информационог система који се користи, постоје опште безбедносне препоруке и стандарди који су дефинисани посебним документима. Међународна организација за стандардизацију ISO је кроз свој сет стандарда ISO 27000 дала препоруке (best practice) за управљање безбедношћу информација [2].

Упркос убрзаном порасту популарности е-учења, јасној потреби за третирањем питања безбедности, као и постојању одговарајућих регулатива и препорука, безбедности у е-учењу се не посвећује довољно пажње [3]. У том смислу, постојање модела који би покрио различите организационе и техничке аспекте безбедности, може бити од значајне помоћи у креирању конкретних механизама и употребљивих модуса безбедности. Од имплементације оваквог модела очекује се да позитивно утиче на квалитет образовања.

Ауторова основна мотивација је креирање употребљивих оквира за унапређење е-учења проактивним третирањем питања безбедности и формирање корисниковог доживљаја е-учења као равноправног облика е-пословања. Такође, у мотиве се може убројити и истраживање нових модела, помоћу којих се ближе могу објаснити односи на релацији човек-информациона технологија.

1.2 Предмет и циљ дисертације

Предмет дисертације је пројектовање и имплементација безбедносног модула у е-образовању, који својим проактивним деловањем унапређује безбедност система за е-образовање, а посебно корисника е-учења.

За дефинисање предмета дисертације кључна су следећа питања:

- Од каквог је значаја безбедност информација у е-образовању?
- Да ли је могуће креирати модел који би приказао е-образовање кроз безбедносне аспекте?
- На који начин постојећи стандарди третирају питање безбедности информација у е-образовању?
- Да ли је могуће побољшати позицију корисника у окружењима за е-учење са аспекта безбедности?
- Постоји ли релација између квалитета е-образовања и безбедности информација?
- Какви су захтеви по питању приватности података у системима е-образовања?
- Да ли ситуација у Србији показује одређене специфичности по питању е-образовања и односа са безбедношћу података?

Дефинисани су следећи основни циљеви дисертације:

- утврђивање утицаја безбедности информација на е-образовање
- концептуализација и пројектовање модела безбедности и приватности у е-учењу
- пројектовање, имплементација и евалуација безбедносног модула, као интегралне компоненте система за електронско учење
- систематизација постојеће стандардизације (IMS, IEEE, ISO) и усаглашавање модела са стандардима
- развој пратећих полиса, докумената и процедура
- интеграција са шемама за обезбеђење квалитета е-учења
- имплементација софтверског модула применом савремених технологија и алата
- имплементација безбедносног модула и интеграција у систем за е-учење

- евалуација интегрисаног система

На безбедност утиче низ параметара и правилно моделовање је од драгоценог значаја за успостављање одговарајућих механизама заштите. Један од циљева рада је управо формирање модела безбедности у е-образовању који би обухватио све релевантне факторе који чине сам систем и утичу на безбедност података и самог процеса образовања.

Један од виталних фактора који фигуришу у безбедности је управо корисник. Поједини аутори су чак децидирани да је корисник ”најслабија карика" у безбедности [4], [5]. Стога је идеја истражити на који начин се позиција корисника може ојачати у погледу безбедности, на који начин се може унапредити његов профил, како се питање безбедности уклапа у постојеће стандарде и на који начин се одражава на квалитет е-учења.

Имплементација модела представља наредни корак у којем се врши пресликавање модела у реални систем креирањем одговарајућих процедура, докумената и софтверских елемената који чине модул: интегрални део инфраструктуре за е-образовање посвећен управо безбедности.

1.3 Очекивани резултати

Предвиђена је реализација безбедносног модула, који представља интегрални део система за управљање учењем.

Остали резултати су:

- систематизован преглед елемената који утичу на безбедност и приватност у е-образовању
- систематизација стандарда који се баве безбедношћу и приватношћу и е-образовању
- предлози за унапређење безбедносних стандарда и процедура у е-образовању
- развијена унапређена, безбедносно оријентисана архитектура е-учења, заснована на стандардима е-учења
- развијен безбедносни модел корисника е-учења
- интегрисани систем за е-учење са имплементираним безбедносним модулом
- дефинисана политика коришћења система за е-учење

Научне хипотезе

- H1 Модул безбедности се може успешно развити применом стандардизоване методологије управљања безбедношћу и стандарда у е-образовању
- H2 Пројектовани модул безбедности и приватности у е-образовању директно утиче на обезбеђење квалитета е-образовања.
- H3 Безбедносни модул позитивно утиче на поверење корисника у систем за е-учење.
- H4 Безбедносни модул позитивно утиче на степен прихватања е-образовања.

Методе истраживања

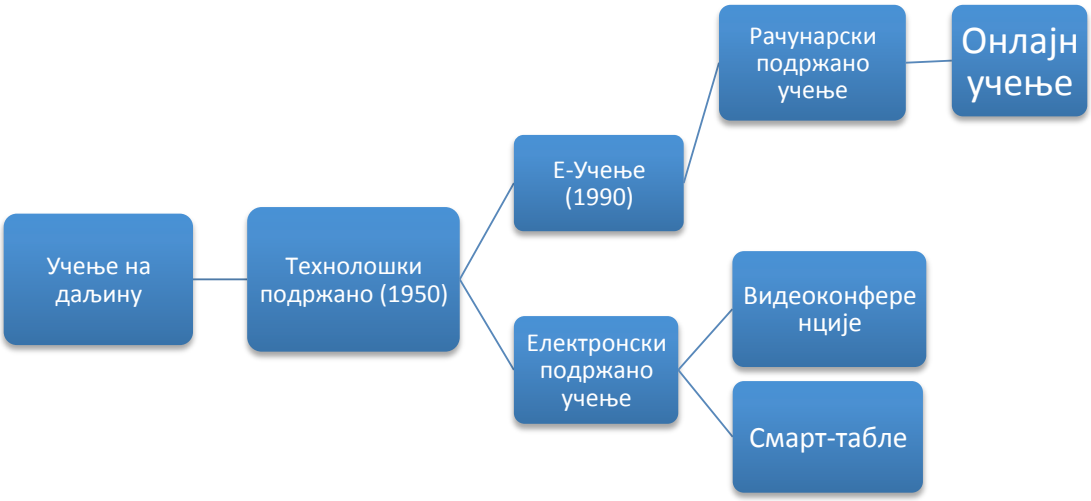
- У првом делу рада коришћене су методе компилације, дедуктивне и емпиријске методе. Коришћена је и метода студије случаја *(case study)*.
- У централном делу рада коришћена је метода моделирања.
- Током имплементације коришћене су методе практичног рада.
- На крају рада, у сегменту евалуације су коришћени: метода упитника и статистичке методе.

1.4 Основни појмови

У наставку су дате основне информације о кључним појмовима који се користе кроз рад. С обзиром на то да је област е-учења у развоју, те да је терминологија неусаглашена у оригиналном облику, односно у верзијама превода, значајно је посебно одвојити сегмент који се бави управо разјашњавањем појединих појмова и њихових значења. У области безбедности такође постоји низ термина, чија ће стандардизована значења бити представљена.

1.4.1 Образовни појмови

Учење на даљину је модел који поседује дугу историју и обухвата разноврсне технике комуникације између наставника и ученика. Е-учење се издвојило као посебна грана средином 90-их година 20-ог века, као модел који се ослања на електронску технологију.[6] - Слика 1.



Слика 1 - Таксономија е-учења

Данас постоји више дефиниција појма е-учење. Оксфордски речник дефинише е-учење као "учење спроведено преко електронских медијума, обично интернета" [7].

Е-учење (e-learning) је дакле појам којим се дефинише широк спектар примена информационо-комуникационих технологија (ИКТ) у учењу и настави. Развојем интернета и све већим ослањањем других технологија е-учења на интернет, односно смањивањем удела алтернативних техника (едукативни CD, оф-лајн софтвери), све чешће се ставља знак једнакости између е-учења и он-лајн учења, тј. учења коришћењем интернета. И у овом раду ће се надаље под е-учењем подразумевати образовне технологије и наставне методе које укључују коришћење интернета, тј. е-учење се поистовећује са онлајн (on line) учењем.

Е-образовање у овом раду подразумева формално образовање засновано на е-учењу у било ком облику (комбиновано или комплетно е-учење).

Даље од саме организације програма предмета, односно курса, зависи да ли ће настава бити у потпуности спровођена он-лајн (тзв. *pure on-line*, комплетно е-учење) или ће бити заступљена комбинација традиционалних метода и е-учења (тзв. хибридни, комбиновани - *blended* режим).

1.4.2 Појмови из области безбедности информација

Међународни комитет ITU-T описује безбедност на следећи начин [8]:

Термин безбедност („security“) се користи у смислу минимизације рањивости имовине и ресурса. Имовина је било шта што има вредност. Рањивост је било која слабост која се може искористити у циљу нарушавања система и информација које садржи. Претња је потенцијално нарушавање безбедности.

Фундаменти безбедности се огледају у тзв. CIA тројству (Confidentiality (поверљивост), Integrity (целовитост) и Availability (доступност)). Основни задатак безбедности је очување ова три својства. Поред тога, безбедност се бави и аутентификацијом, непорицањем, поузданошћу итд.

ISO на следећи начин дефинише основне појмове [9]:

- Поверљивост подразумева да одређени ресурс није доступан неауторизованим појединцима, ентитетима или процесима.
- Приватност је блиско повезана са поверљивошћу и подразумева очување тајности личних информација.
- Интегритет подразумева очување тачности и комплетности ресурса
- Доступност подразумева могућност приступа и употребљивост на захтев ауторизованог ентитета.
- Ризик (information security risk) је могућност да дата претња искористи рањивост имовине и тиме нанесе штету организацији. Одређује се као комбинација очекивања догађаја и његових последица.
- Процена ризика (risk estimation) је поступак додељивања вредности вероватноћама и последицама ризика.
- Површина напада (attack surface) представља скуп рањивости неког система.

Microsoft је за потребе моделовања претњи развио методологију познату под акронимом STRIDE [10]. У питању је скраћеница од речи којима се описују типови нарушавања безбедносних циљева:

- Spoofing identity (лажирање идентитета) - Нпр. коришћење туђег корисничког имена/лозинке
- Tampering with Data (измена података) - Промена записа у бази података, измена IP пакета који се преносе Интеретом итд.
- Repudiation (порицање) - Корисник пориче да је извршио одређену операцију, а не постоји праћење догађаја, којим би се то спречило.
- Information disclosure (откривање информација) - Омогућен приступ и евентуално објављивање информацијама које би требало да су тајне.
- Denial of Service (ускраћивање услуге) - Нарушавање доступности сервиса његовим успоравањем или потпуним онемогућавањем.

- Elevation of Privilege (повећање права) - Лице или програм стиче привилегије које регуларно не би добило, са циљем извршавања операција које захтевају виша права.

1.5 Специфичности е-образовања

Ако се погледају технологије присутне у традиционалној настави и оне код е-учења, постоје бројне сличности. И у традиционалној настави све присутнији су модерни технолошки подржани елементи: користе се рачунари и едукативни програми, ресурси са интернета и специјална наставна средства (паметне табле, пројектори). Поставља се питање у чему тачно леже специфичности е-учења у односу на модерну традиционалну наставу.

Пре свега, традиционална настава је непосредна настава. То значи да су ученици и наставници, дакле сви учесници у наставном процесу, физички присутни на истом простору у исто време. То такође значи да је опрема која се користи под контролом образовне установе. Други аспект је критичност информатичких ресурса који су у употреби. Код традиционалне наставе преовладавају традиционални облици и методе и критични елементи као што је нпр. праћење напредовања ученика, покривени су традиционалним методама. На пример, тестирање се углавном врши у традиционалној форми папир и оловка, активност на настави се прати и оцењује на самом часу итд.

Код е-учења информационо-комуникациона инфраструктура игра кључну, критичну улогу. Инфраструктура за подршку е-учењу представља све оне информационо-комуникационе ресурсе који се користе у настави/учењу. Део тих ресурса обично је у власништву установе, док су други делови под контролом самог ученика, односно трећих страна. На пример, систем за управљање учењем, са пратећим сервером и помоћним сервисима се налази у самој установи, рачунари са којих се приступа ресурсима (са одговарајућим програмима и приступом интернету) припадају самим ученицима, а додатни ресурси који се користе посебно или су повезани са системом за управљање, налазе се на интернету и у власништву су различитих фирми или појединаца.

Захваљујући дистрибуираној природи е-учења, одговорност према самом процесу учења је такође дистрибуирана међу учесницима процеса. Установа је дужна да обезбеди ресурсе на ”серверској страни”, што значи платформу и пратећи хардвер. Установа може имати и клијентске рачунаре, оне са којих се приступа садржајима, али генерално је тај ”клијентски део” под ингеренцијом самих учесника у настави. Нарочито када се узме у обзир шароликост мобилних уређаја и тренд који говори о популарности мобилног учења [11].

1.6 Предности е-образовања

Могућности које пружа е-образовање су бројне [12]:

- флексибилно учење (по сопственом темпу, са произвољне локације)
- интензивна комуникација (коришћењем он-лајн алата могуће је остварити веома квалитетну комуникацију у којој сваки учесник може лако добити свој простор, неретко једноставније него у непосредној настави)
- аутоматизација различитих активности (оцењивање тестова, генерисање портфолија)
- поновно коришћење (reusability) и дељење једном креираних ресурса
- аутоматска детекција плагијаризма
- интеграција са другим електронским системима (портфолио-платформа, информациони систем установе)

У зависности од начина интеракције актера међусобно и са наставним ресурсима, може се говорити о синхроном или асинхроном учењу [13].

Основна карактеристика синхроног учења је рад у реалном времену. Овакав вид подразумева комуникацију путем инстант порука, Интернет састанака, као и наставу путем видео-линка. Предности оваквог приступа су: постојање повратне информације, и висок степен интеракције са свим учесницима у наставном процесу. Претходно поменути модел дистрибуиране учионице базира се на синхроном учењу - учесници фактички у реалном времену комуницирају (држе се предавања, дискусије, приказују експерименти). Недостаци оваквог приступа су: високи хардверски захтеви, ограниченост на задате термине наставе (консултације, радионице, предавања, лабораторијске вежбе), као и диктирање темпа учења од стране наставника.

Код асинхроног учења, учесници не комуницирају у реалном времену, већ се користе методе комуникације код којих постоји кашњење: електронска пошта, форуми и дискусионе групе, а материјали за учење су припремљени унапред (нпр. снимак предавања). Предност овог приступа је крајња независност ученика - он може бирати којим темпом и којим редоследом ће учити. Недостатак је управо изолованост ученика - изостанак интеракције и повратне информације у реалном времену. Постоје закључци да је оптимално асинхроно учење подржати синхроним учењем, односно одговарајућим алатима [14].

За потребе реализације е-образовања образовна институција је у обавези да формира, администрира и одржава одговарајућу инфраструктуру, чиме се обезбеђује: доступност материјала за учење, синхрона и асинхрона комуникација између свих актера укључених у процес учења и наставе, праћење напретка студената и спровођење осталих активности од значаја за успех учења

на даљину. Потребно је да инфраструктура прати модерне техничке стандарде, да буде модуларна, флексибилна и скалабилна и усклађена са потребама циљне групе корисника.

Е-образовање је присутно у облику комплетног спровођења наставе он-лајн (pure online) и као компонента интегрисана у традиционалну наставу, у виду тзв. комбинованог учења (blended learning) [15]. На тај начин учесници у настави за одређене активности могу користити он-лајн ресурсе (на пример за проверу знања, комуникацију путем форума и сл.), док се већи део наставе ослања на традиционалне методе и спроводи у установи.

Постоје многобројни примери универзитета који наставу спроводе искључиво он-лајн. Најпознатији је Отворени универзитет (Open University), који је у школској 2011/2012 години нудио 342 модула основних студија и 141 постдипломски модул, са преко 240 хиљада уписаних студената [16].

Електронско учење подразумева коришћење било којег он-лајн алата. На пример, употреба Гугл докумената (GoogleDocs) за колаборативни рад на писању есеја је такође е-учење. Или нпр. коришћње Скајпа (Skype) за разговор у реалном времену. Уколико је реч о потпуном моделу е-учења (pure e-learning), од значаја је пратити активности ученика у централизованом маниру. У том случају у пракси се најчешће прибегава коришћењу окружења за учење (Learning Environment). Реч је о софтверу који учесницима у настави пружа амбијент за учење/наставу у смислу ресурса и различитих активности, пре свега оријентисаних ка међусобној комуникацији.

Окружење може покривати велико подручје опција: од регистрације нових корисника, испоруке садржаја, обезбеђења ефикасне комуникације и сарадње, безбедносних прописа па све до аутоматизоване провере презентованих знања.

Термин близак *Окружењу за е-учење* (а често се користи и као синоним) је *систем за управљање е-учењем* (Learning Management System). У раду ће ова два термина бити коришћена као појмови истог значења.

Данас постоје многи услужни системи који омогућавају постављање образовног садржаја, чиме се на једноставан начин може изводити процес електронског учења. То многе образовне институције и чине, тиме готово у потпуности елиминишући потребу за физичким простором за окупљање учесника у процесу наставе/учења.

Постоје различите варијанте система за управљање учењем, зависно од тога да ли се користе готови садржаји или се они креирају у самом окружењу. Такође,

на располагању су плаћене, комерцијалне верзије, али и верзије отвореног кода, које корисницима пружају могућности побољшања и доградње.

1.7 Трендови у е-образовању

Е-учењу свакако предстоји експанзија, али не треба занемарити неопходност консолидације у периоду који следи после ”бума” е-учења [17]. У том смислу потребно је размишљати и деловати ка што прецизнијем дефинисању услова и начина у којима се е-образовање одржава.

На конкретном примеру: захваљујући сопственим средствима, а нарочито захваљујући бројним европским пројектима, велики број високошколских установа у Србији опремљен је ИТ ресурсима. Године 2013. број корисника широкопојасног Интернета премашио је 1,5 милиона [18]. Када се на то дода и константно повећање броја корисника 3g Интернета, добија се преглед који говори о значајној заступљености ”клијентских услова” за е-учење. Закључује се да информационо-комуникациони ресурси постоје. Међутим, то је само потребан услов за квалитетно е-образовање. Искуство и истраживања показују да је унапређење потребно у широком опсегу питања [19].

Системи за е-учење бележе велики број информација о понашању корисника. На основу тих информација могуће је анализом доћи до карактеристика корисника, њихових преференција и различитих закључака о самом материјалу и наставним активностима, који се не могу добити директним посматрањем. Област која се бави овим аспектом позната је као *Learning Analytics* и постоји изражен тренд истраживања у овој области, као и развоја алата који могу да искористе велике количине података генерисане кроз процесе е-учења [20], [21].

Значајни напори су извршени у смеру креирања динамичких, аутоматизованих окружења за е-учење. У таквим окружењима сценарио учења се динамички прилагођава кориснику [22]. Може се очекивати даљи развој интелигентних агената који ће помагати корисницима и адаптирати садржаје према њиховим личним карактеристикама и преференцама.

Мобилно учење (м-учење) постаје незаобилазан сегмент е-учења [23]. Начини на које се врши адаптација садржаја и то како сама адаптација утиче на процес учења предмет је текућих истраживања [24].

Проширена стварност (Augmented Reality) је приказ стварности у реалном времену при чему су одређени делови замењени рачунарски генерисаним информацијама, тако комбинујући стварне и виртуалне светове [25]. Примена у образовању један је од значајних потенцијала е-образовања, нарочито када је реч о колаборативном учењу [26].

Е-образовање неретко је на мети критика, конкретно: е-образовне методе наставе, али и организационо-технички елементи. У последње спада управо ослоњеност на технологију, која са собом повлачи и питања безбедности података који се користе у е-образовању, а који су у потпуности засновани на информационим технологијама. Многе од критика е-едукатори третирају као митове [27]. Без обзира на то колико су одређене критике оправдане, постоји потреба да се инфраструктурни елементи уреде, што подразумева процедуре, документацију, односно одговарајућу софтверску подршку.

1.8 Изазови е-образовања

Поред бројних предности које доноси е-учење, овај вид едукације суочава се са бројним изазовима [28], [29] као што су: споро прихватање нове технологије, проблеми са навигацијом кроз садржаје, потреба за додатном едукацијом, мотивисаност за учење, одржавање инфраструктуре, безбедност информација и друго.

Значајна препрека у даљем развоју е-образовања је недостатак законских регулатива којима би се разноврсни аспекти и новине које е-учење доноси на пољу формалног образовања дефинисали. На тај начин би установама било олакшано формирање студијских програма, пројектовање одговарајуће подршке и реализација наставног програма. Пројекат DL@Web [30] је током своје реализације изнедрио низ докумената којима се предвиђају нове регулативе на пољу студија на даљину [31]. Званично, Комисија за проверу квалитета и акредитацију (КАПК) усмерава на своја упутства [32]. Анализе су указале на потребу за даље унапређење и детаљније дефинисање ових препорука [33]. И даље остаје отворено питање реализације свих формираних предлога и уврштавање у званичне регулативе високог нивоа.

Међу битним изазовима су управо безбедност података и заштита приватности корисника. Сама природа е-учења отвара низ питања која захтевају адекватне механизме за решавање: безбедност платформе, безбедност комуникације, заштита од нежељених порука, контрола приватности података итд. Решавање ових питања не може се извести једнократно, већ захтева континуирано ангажовање.

Безбедност није само питање технологије, већ и организације, односно људских фактора и потребно јој је приступати систематично, на нивоу управљања институцијом. Вон Солмс таксативно наводи тзв. „десет смртних грехова“, односно десет основних пропуста у перцепцији безбедности [34]. Ови постулати гласе:

1. Неувиђање да је за безбедност одговоран менаџмент
2. Неувиђање да је безбедност пословно питање, а не техничко питање
3. Неувиђање да је безбедност мултидисциплинарна дисциплина и да не постоји јединствено готово решење („сребрни метак“)
4. Неувиђање да план безбедности мора бити заснован на идентификацији ризика
5. Занемаривање примене најбоље међународне праксе у управљању безбедношћу
6. Неразумевање да је постојање корпоративне политике безбедности есенцијално питање
7. Неувиђање да је одговарајућа структура која управља безбедношћу кључна
8. Неувиђање неопходности за обезбеђење поштовања правила и праћења безбедносних параметара
9. Неразумевање кључног значаја свести корисника о безбедности информација (security awareness)
10. Неподржавање менаџера безбедности одговарајућом инфраструктуром, алатима и помоћним механизмима за правилно спровођење својих дужности

Ако би требало сублимирати наведене ставке и претходну дискусију у један сажети приказ, могло би се констатовати следеће:

Безбедност информација мора се и код е-образовања поставити као питање пословне важности, које захтева подршку одговарајућом инфраструктуром, документацијом и корисничком подршком.

1.9 Структура рада

Рад је конципиран из следећих поглавља:

- Друго поглавље се бави прегледом литературе: радова из часописа и са конференција, као и књига са тематиком е-учења у контексту безбедности. Преглед треба да пружи увид у досадашња истраживања и послужи као основа за усмеравање рада и формирања модела.
- Треће поглавље се бави квалитетом у е-учењу. У овом поглављу се анализирају различити модели квалитета е-учења и место безбедности информација у тим моделима, уз посебан акценат на обезбеђењу квалитета и шемама за обезбеђење. Циљ поглавља је да прикаже место безбедности информација у контексту квалитета и издвоји одговарајуће елементе које касније треба размотрити при формирању модела и пројектовању самог модула.

- Четврто поглавље обрађује појмове поверења и прихватања технологије у контексту система за е-учење. Сврха поглавља је приказ модела поверења и прихватања и дефинисање значаја ова два појма у контексту е-учења, као и њихов однос са безбедношћу информација.
- Пето поглавље посвећено је анализи стандарда различитих нивоа, који могу бити корисни при пројектовању модула. Реч је о општим безбедносним стандардима, као и о стандардима везаним за е-учење. Циљ поглавља је систематизација самих стандарда у овом контексту и дефинисање стандардизоване подршке при пројектовању и имплементацији самог модула.
- Шесто поглавље је фактички студија случаја: у каквом је стању безбедност у е-учењу у Србији. Путем анкета и непосредним испитивањем добијени су разноврсни подаци о томе како су имплементирани системи за е-учење у Србији и како се понашају корисници система - у контексту безбедности информација. Преглед и анализе дати у овом поглављу имају за циљ да пруже потребне улазне параметре за формирање модела безбедности.
- Седмо поглавље бави се проширењем модела корисника (е-ученика), ради компатибилности са потребама унапређења безбедносне позиције крајњег корисника. Основа проширења је стандард IMS LIP.
- Осмо поглавље је посвећено формирању модела безбедности у е-образовању. За те потребе прво су анализирани постојећи општи модели, а онда је формиран модел који укључује проширени модел корисника и стандардизовану LTSA архитектуру.
- Девето поглавље бави се пројектовањем модула као софтверског агента и његовом интеграцијом у LMS Moodle.
- Десето поглавље је посвећено евалуацији и истраживању утицаја модула на поверење и прихватање технологија.
- У једанаестом поглављу дата су закључна разматрања и представљене идеје за будући рад.

2. Безбедност информација у е-образовању: преглед стања у подручју истраживања

Е-образовању, иако све важнијем облику едукације, ни издалека није посвећено толико пажње у истраживањима када је реч о безбедности података, као што је случај у другим е-делатностима (е-управа, е-банкарство). Такав статус се делом може објаснити проценама да је е-образовање нижег приоритета, него на пример електронско пословање, те да је критичност информација такође мања.

Истраживања која разматрају значај безбедности информација у системима за е-учење су мултидисциплинарног карактера и могу се пронаћи у публикацијама из различитих научних области: рачунарства, образовања, менаџмента.

У наставку је дат преглед истраживања која су у последњих десетак година обрађивала мултидисциплинарни конструкт безбедности у е-учењу.

У оквиру постојећих истраживања обрађени су првенствено безбедносни модели који се тичу појединих сегмената везаних за системе е-учења, односно општији безбедносни модели који су примењени на е-учење. У том смислу радови се грубо могу класификовати у две групе: опште, који разматрају безбедност и приватност у е-учењу генерално и у склопу посебних модела и специфичне, који разматрају посебне методе заштите.

Weippl у својој књизи опширно обрађује проблематику безбедности и приватности у е-учењу [35], које на самом почетку карактерише као специфичан вид е-пословања. Аутор прво даје приказ безбедности из аспекта различитих учесника у процесу е-образовања: аутора материјала, наставника, администратора, менаџера и студената, а надаље обрађује техничке и социолошке факторе који су укључени у безбедност и приватност. Почетне секције књиге организоване су као водич за кориснике, док се у наставку дају конкретни напредни, технички детаљи заштите. Анализа ризика се помиње, али се не спроводи. Такође, није пружен осврт на квалитет, односно однос безбедности и квалитета, нити на стандардизацију.

Рад *Privacy and Security in E-Learning*, који је део извештаја канадског националног пројекта задуженог за е-образовање, представља тематику обрађену из организационог угла, са становишта постојећих општих и специфичних стандарда и могућностима њихове имплементације [36]. Дати су и конкретни предлози примене појединих алата у циљу обезбеђења приватности личних података и остваривања поверења (методама тзв. trust management-а). Посебна пажња посвећена је криптографским методама, примењеним на различите нивое заштите: тунеловање целокупног саобраћаја, шифровање

чуваних дневника активности и поменутог trust-management-а применом асиметричних алгоритама.

У раду *Information security in E-learning Platforms* аутор је дао кратак преглед основних безбедносних претпоставки са гледишта постулата безбедности: поверљивости, интегритета и доступности [37]. Дат је и кратак приказ проблематике једног од најпознатијих система за е-учење, Moodle, кроз призму појединих критичних пропуста у систему. Закључено је да постоји низ безбедносних поставки које је неопходно конфигурисати на самој платформи и ускладити са пратећом инфраструктуром, да би се чак минимално постигли безбедносни циљеви.

У раду *A secure model for building e-learning systems* аутор предлаже архитектуру софтверске платформе за е-учење, која почива на бежичној мрежној инфраструктури [38]. Окосница рада се заснива на предлогу софтверских алата и криптографских техника које је потребно ангажовати у циљу безбедног рада читаве инфраструктуре.[38] Закључено је да конвенционалне методе заштите могу бити успешно искомбиноване у циљу реализације безбедносних циљева у е-учењу.

Примена класичних методологија класификације претњи може се остварити и на нивоу система за управљања учењем, нпр. помоћу STRIDE [39]. Анализа је извршена на нивоу платформе за е-учење.

У раду *Security in the online e-learning environment*, аутори су истраживали социолошке аспекте приватности у он-лајн окружењу [40]. Основни закључци односе се на препознавање потребе за провером идентитета учесника и праћење активности као важних фактора који корисницима уливају поверење у систем. Истражено је понашање корисника на примеру колаборативног рада на вики-странама. Код вики-страна се лако може догодити да неко уништи претходни рад, те је ауторима идеја била да истраже како се корисници понашају у случају када им активности нису условљене поседовањем налога.

У раду *Privacy provision in e-learning standardized systems: status and improvements*, аутори су разматрали стање стандарда који се баве приватношћу у е-учењу и предожили модел којим се приватност унапређује, а корисници добијају већу контролу над њом [41]. Нагласак истраживања је на што детаљнијој и флексибилнијој могућности управљања сопственим поставкама приватности и обимом информација које се дају на располагање систему за учење или трећим лицима. Формирани модел (ELENA) пројектован је као спој два постојећа стандарда е-образовања који се односе на безбедност: IMS и IEEE, омогућавајући кориснику (ученику) да специфицира ниво поверљивости за

сваки елемент. У случају да корисник то није у стању да учини (нпр. нема довољно знања о томе), систем ће доделити вредности аутоматски. Аутори наглашавају да, упркос унапређењу постојећих стандардизованих варијанти које се односе на приватност информација, технологија сама није у стању да реши проблеме приватности, већ је неопходно искомбиновати је са законским регулативама, узимајући у обзир захтеве тржишта.

У раду *Towards Secure e-Learning Applications: a Multiagent Platform* представљен је приступ изградњи безбедног система за е-учење применом мултиагената кроз тзв. FIPA спецификацију, уз разраду различитих студија коришћења система [42]. Основни циљ је увођење безбедносних механизама у сам модел платформе за е-учење, а нарочито у процесе аутентификације и ауторизације. Аутори су рашчланили безбедносне захтеве на две класе: оне који се тичу саме инфраструктуре (са освртом на мултиагенте) и оне који се тичу е-учења, односно специфичних сценарија учења.

Безбедност у мобилном учењу обрађена је у раду *Security and Privacy Preservation for Mobile E-Learning via Digital Identity Attributes* [43]. Пројектован је петослојни модел, код којег је први слој заједнички и обухвата полисе и фундаменталне предуслове за реализацију процеса у е-образовању, а остали слојеви су хијерерхијски постављени. На петом слоју је посебно обрађена проблематика мобилног учења и тестирања уз нарочит осврт на специфичне методе аутентификације и ауторизације.

У појединим радовима посебан осврт је начињен ка осветљавању поимања безбедности у он-лајн окружењу од стране студената. Тедре и Чачаџе су развили упитник у којем су по том питању анализирали ставове студената у Танзанији, при чему су вршили анализе по различитим параметрима: полу, урбаности порекла итд [44]. Закључено је да ученици генерално не воде довољно рачуна о заштити података, нарочито личних, што се може решити едукацијом, али само до одређене мере.

Милошевић и други су проучавали ставове студената према безбедности и приватности е-образовања на Техничком факултету у Чачку [45]. Резултати указују на изражену потребу за едукацијом студената на пољу безбедности, али и на непостојање политике која би помогла у успостављању поверења на нивоу институције.

Нарочито интригантан аспект е-образовања је е-провера знања и овом проблематиком су се истраживачи посебно бавили. Marais и други су у раду обрадили разноврсне факторе који утичу на безбедност е-тестова: од аутентификације, до негирања идентитета и поверљивости садржаја теста [46] .

Исти аутори су се бавили и детаљнијом разрадом механизама за спречавање вишеструке предаје теста.

Gil и други су пројектовали посебан систем за биометријску идентификацију студената у е-тестирању [47]. Предвиђено је да ова функционалност буде имплементирана кроз додатак за Moodle систем.

Chiranji и други су пројектовали посебан систем за мониторинг током тестирања, којим се испитаников рачунар контролише по посебно задатом алгоритму, који прати поступак тестирања [48].

У својој докторској дисертацији *Eibl* је обухватно анализирао ризике у системима за е-учење коришћењем Fault Analysis Tree методологије [49]. Ова методологија представља систематичан дедуктиван приступ анализи претњи, при којем се одређени ризик квалитативно препознаје и поставља као почетни елемент стабла резоновања. Методологија се показала као посебно значајна за широк скуп претњи присутних у окружењима за е-учење.

Неопходност озбиљнијег обраћања пажње на корелацију између употребљивости система (usability) и безбедности посебно је истакнута у [50] и ова опсервација се може посебно искористити за унапређење безбедности и код система за е-учење. Аутори су као основна два проблема из области безбедности издвојили аутентификацију и заштиту приватности. Наглашено је да се пренебрегавањем тежине коришћења безбедносних механизама, што је често присутно код модерних окружења за е-учење, изазива контраефекат: корисници, не желећи да троше време на стицање предзнања и на примену самих метода, избегавају коришћење е-учења уопште, односно премошћавају саме механизме, нпр. уписују лозинке на видним местима и сл. Такође, изражена је потреба за што доступнијим системом помоћи. Као општи закључак наведено је да су безбедносни механизми круцијални, али да их је неопходно развијати за кориснике и са корисницима, јер једино на тај начин ће они бити правилно искоришћени.

Питање поверења (trust) у окружењима за е-учење разматрали су аутори у [51]. Аутори су разматрали систем у којем корисници одржавају псеудоанонимност. У таквом систему потребно је успоставити специфичне механизме за одржавање поверења корисника. У том смислу, аутори предлажу и модел у којем се користе тзв. парцијални идентитети: прилагођен приказ информација профила у различитим контекстима. Такође, као кључан елемент у одржању поверења наведена је репутација корисника, која се стиче одређеним активностима (понашањем).

Borcea и остали су се интензивно бавили питањем парцијалног идентитета [52]. У систему који су пројектовали постоји посебан клијент за е-учење који се бави формирањем одговарајућег профила у зависности од контекста, односно активности коју врши корисник. Циљ система је и одржавање анонимности корисника уз могућност праћења одређених статистичких параметара на страни сервера.

Конкретан пример из консултантског угла дат је у [53]. Аутори су на основу озбиљних последица које је изазвао напад на систем за учење једног универзитета дошли до закључака да је развој безбедносне политике и процедура од изузетног значаја за регулисање процеса у е-образовању.

Поверење у е-учење истражено је у релативно скромном обиму. *Wang* даје преглед неких кључних елемената и постојање безбедносних механизама се показало као важан фактор за учвршћивање поверења у е-учење [54].

Дискусија о безбедносним елементима потребним у једном окружењу за е-учење довела је истраживаче до закључка да је управљање безбедношћу информација (ISM - Information Security Management) једини начин да се безбедност на одговарајући начин инкорпорира у системе за е-учење [55]. У том смислу су дати и обриси оквира (framework) управљања. Основни закључак је да је неопходан холистички приступ и да је укључивање самих корисника кључно за успех управљања безбедношћу.

Прихваћеност технологија е-образовања није посебно разматрано у корелацији са безбедношћу у литератури доступној аутору. Са друге стране, може се пронаћи већи број радова који изучавају факторе који утичу на прихваћеност, као и радова који сумирају различите теорије [56].

Анализом литературе добијена су полазишта за развој модела:

- **Изискује се шири приступ безбедности, што подразумева формирање оквира за управљање безбедношћу.**
- **Потребно је унапредити безбедносне механизме са којима је корисник у директном контакту.**
- **Неопходан је развој политике и процедура којима се регулише безбедносни аспект е-образовања. Процедуре морају бити добро дисеминиране међу корисницима.**

Установљено је да у постојећим истраживањима није развијан модул којим би се холистички третирала безбедност у е-учењу и однос са квалитетом и поверењем корисника, као ни интегрални приступ безбедности, ни коришћење безбедносних стандарда у оквиру окружења за е-образовање, тако да је потврђен потенцијални допринос дисертације.

3. Обезбеђење квалитета у е-образовању

Пораст доступности образовних технологија и прихваћености е-учења од стране институција и привреде, довео је до омасовљења овог вида образовања. Убрзани развој није испраћен квалитетом, па се лако може догодити да увођење технологије уназади одређене образовне елементе, уколико се недовољно пажње посвети институционалној политици, квалитету садржаја и самих процеса наставе [57].

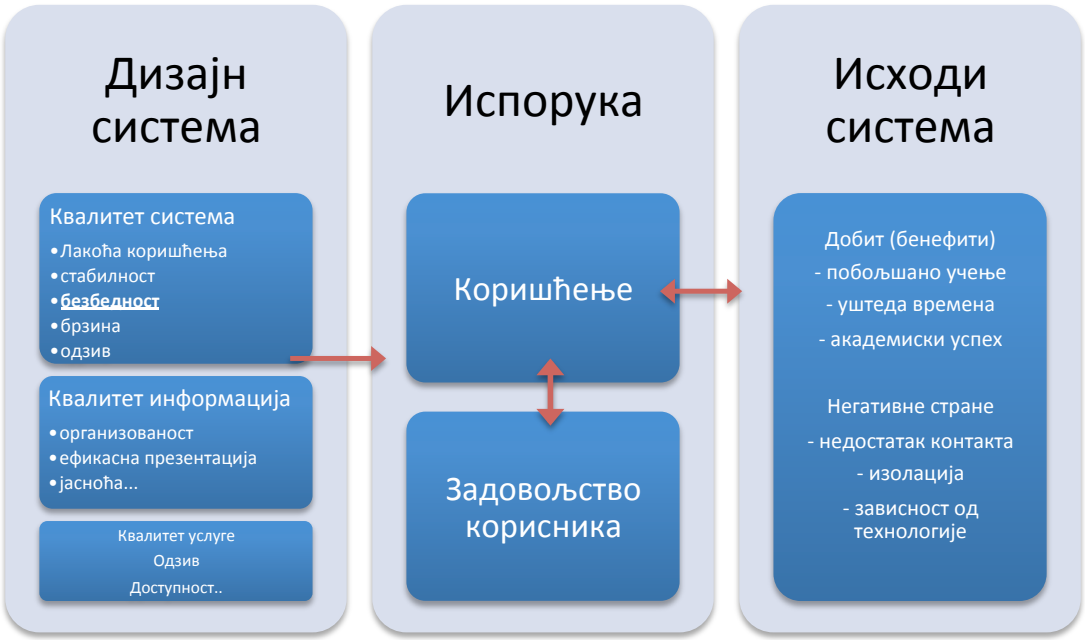
Тренд популаризације е-учења резултовао је стварањем мноштва различитих приступа питању квалитета у е-образовању. С обзиром на полазну различитост схватања самог термина квалитет [58], као и на различите погледа на квалитет од стране различитих заинтересованих страна, креирање јединственог оквир за квалитет остаје изазов [59].

На самом почетку, потребно је дефинисати појам ”обезбеђење квалитета”. Обезбеђење квалитета (QA - Quality Assurance) јесте скуп проактивних, превентивних мера. ISO 9000 у ставу 3.2.10 дефинише обезбеђење квалитета као ”део управљања квалитетом фокусиран на пружање уверења да ће захтеви за квалитетом бити испуњени” [60].

Питањем обезбеђења квалитета баве се национална тела и специјализоване агенције. И шеме обезбеђења квалитета креиране од стране различитих асоцијација, као и стандарди и препоруке, одређену пажњу посвећују безбедности информација. У наставку ће бити дат преглед најрелевантнијих модела и шема обезбеђења квалитета и анализирани одговарајући сегменти који се баве безбедношћу, са циљем формирања полазишта за модел безбедности.

3.1 Модели квалитета у е-образовању

Е-образовање представља мултидисциплинарни конструкт, па је самим тим и дефинисање параметара квалитета и њиховог садејства сложено. На слици 2 приказан је један приступ, у којем се дефинишу заједно и технолошки и педагошки скупови фактора [61]. Овај модел дефинише три скупа елемената: системски дизајн, испоруку и исходе (резултате). ”Безбедност” се налази у подгрупацији ”квалитет система”, док се у посебном ентитету налази коришћење (use) и задовољство корисника. Може се закључити да безбедност утиче на квалитет једне компоненте, ”квалитета система” и да је утицај на задовољство корисника посредно.

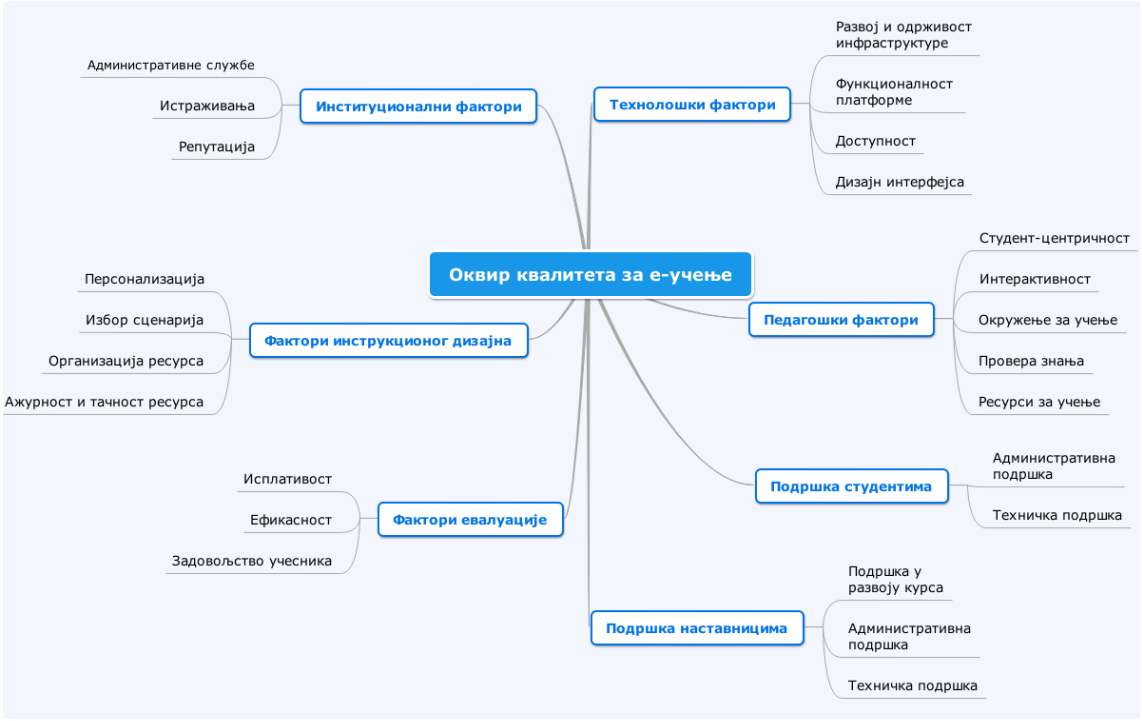


Слика 2 - Модел квалитета [61]

Поједини модели су даље реализовани у облику шема за обезбеђење квалитета, скупова критеријума, организованих по различитим категоријама. Одређене шеме намењене су за екстерну проверу квалитета и подразумевају издавање међународних сертификата.

У опширној анализи литературе Ли и Суоми дали су преглед фактора који утичу на квалитет услуге (quality of service) различитих е-сервиса [62]. Од 24 примера из литературе свега код 6 није експлицитно дата безбедност информација као фактор квалитета. Међутим, и код њих се безбедност може идентификовати посредно, на пример у склопу поверења.

Масуми и Линдстром су своје виђење оквира (framework) за промоцију и обезбеђење квалитета е-учења представили у виду мапе ума [63] - Слика 3. Разграничене су различите категорије фактора који утичу на квалитет, а у раду су детаљно наведени и показатељи који су везани за сваки од фактора.



Слика 3 - Оквир квалитета е-учења (E-Quality) из [63]

У овом оквиру безбедност је такође апострофирана у једном једином сегменту, који гласи: *"Security and Privacy of delivered, collected, and stored information in e-learning settings should be granted".* (Безбедност и приватност испоручених, сакупљених и сачуваних информација у контексту е-учења морају бити гарантовани.) Међутим, ако се генерално погледа мапа која представља оквир квалитета е-учења, питањима безбедности информација може се доделити место у различитим "гранама" мапе, тј. различитим категоријама фактора. Првенствено је логично место међу технолошким факторима. Са друге стране, ако се говори о регулативама и процедурама које се формирају на институционалном нивоу, питања безбедности могу се сврстати и у категорију "институционални фактор". Даље, безбедност информација повезана је и са ауторским правима, па тако питање безбедности има свој удео и у "педагошким факторима", тачније у вези је са "ресурсима за учење". Било који безбедносни инцидент да је у питању, у надлежности је "подршка", тачније "административна подршка", тако да је питање безбедности у вези и са овом категоријом.

Један општији модел задовољства у е-учењу дао је Тариган, у својој модификацији постојећег модела (ELS - E-Learning Satisfaction Model) [64]. Као кључни фактори у овом раду се наводе: квалитет интерфејса, квалитет садржаја, персонализације и подршке.

Поверење се наводи као веома битан фактор за квалитет е-услуга [65]. Овај фактор ће се испитати посебно.

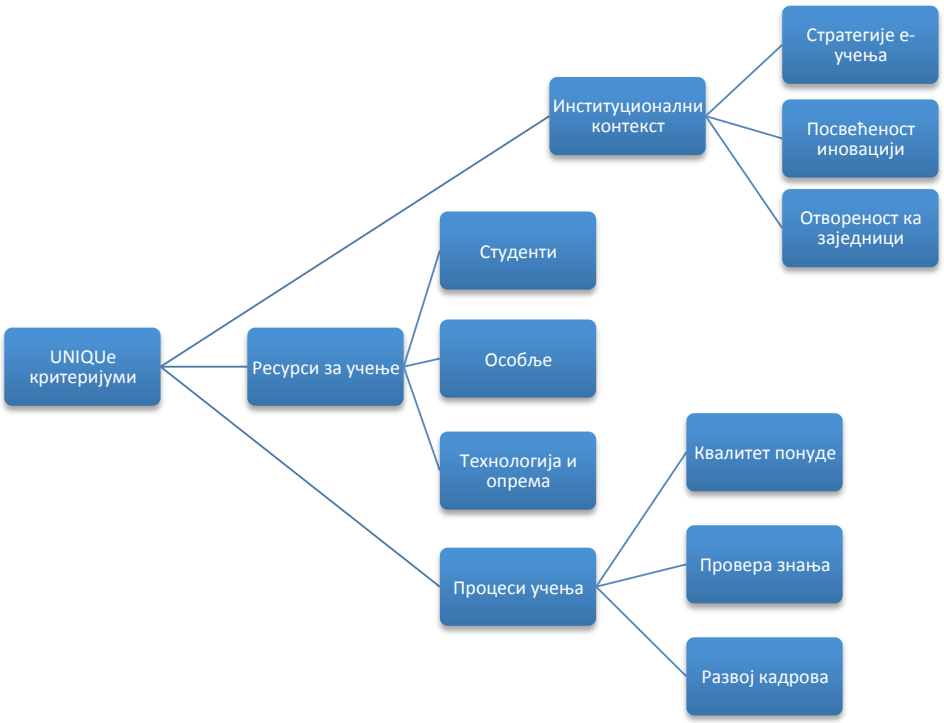
Може се закључити да је безбедност информација компонента која је укључена - посредно или непосредно - у готово све аспекте који утичу на квалитет е-учења.

3.2 Шеме за обезбеђење квалитета

Обезбеђење квалитета у е-учењу врши се на различитим нивоима: институционалном, на нивоу студијског програма, на нивоу курса итд. Од интереса за овај рад су шеме које узимају у обзир инфраструктуру, јер се у њеном склопу налазе елементи значајни за третирање питања безбедности.

3.2.1 UNIQUe

UNIQUe је шема фондације EFQUEL, и на њој се заснива процес истоимене сертификације. Примењује се на нивоу институције и обухвата критеријуме кроз три основне области: Институционални контекст/контекст учења, Образовни ресурси и Процеси учења [66]. Структура је дата кроз следећу хијерархију: област (area), критеријум и подкритеријум (слика 4).



Слика 4 - UNIQUe шема [66]

Питањима безбедности баве се углавном критеријуми друге области. У наставку ће бити дати искази који су посвећени безбедности.

Област *"Ресурси за учење"*, Критеријум 4

> 2.4.1. Особље и ученици имају јединствену пријаву (single sign on) за различите апликације.
>
> 2.4.5. Јако шифровање с-краја-на-крај се користи за заштиту свих личних података корисника.
>
> 2.4.7. За потребе креирања резервних копија (бекап) примењују се најбољи примери из праксе. У најмању руку то значи постојање mirroring-а и асинхроног одвојеног (off-site) бекапа.

На основу анализе исказа може се утврдити да сама шема не залази у детаље имплементације безбедносних механизама, као ни постојање одговарајућих докумената, већ обухвата најрудиментарније критеријуме. Такође, шема се не бави питањима оспособљености корисника и њихове свести о безбедности.

3.2.2 Модел зрелости у е-учењу

Модел зрелости у е-учењу (E-learning Maturity Model, у наставку eMM) настао је на основу методологија Capability Maturity Model и SPICE (Software Process Improvement and Capability dEtermination) [67]. У питању је веома опширан скуп критеријума, за чију примену сами аутори препоручују претходно скраћивање и прилагођавање конкретној намени.

Модел eMM [68] класификује способност институције да подржава е-учење у пет главних категорија или процесних области (Табела 1). У односу на SPICE модел, који се користи за софтверско инжењерство, код eMM-а уместо категорије Клијент/Добављач постоји категорија Учење.

Табела 1 - Категорије у eMM

Категорија	Кратак опис
Учење (L)	Процеси који директно утичу на педагошке аспекте е-учења
Развој (D)	Процеси који обухватају креирање и одржавање ресурса за е-учење
Подршка (S)	Процеси који обухватају надзор и управљање е-учењем
Евалуација (E)	Процеси који обухватају евалуацију и контролу квалитета е-учења кроз читав животни циклус
Организација (O)	Процеси повезани са институционалним планирањем

Свака категорија је описана одређеним бројем процеса. Нпр. категорија Развој (Development) је описана са седам процеса (D1-D7).

У eMM-у способност неке институције да пружи студије на даљину проверава се кроз следеће димензије процеса: испоруку, планирање, дефинисање, управљање и оптимизацију.

P1 Испорука подразумева креирање и пружање резултата процеса. Провере ове димензије имају за циљ да одреде ширину докле се тај процес спроводи унутар институције.

P2 Планирање испитује употребу раније дефинисаних циљева и планова у спровођењу самог процеса. Употреба раније дефинисаних планова потенцијално чини процесе способнијим да се њима ефикасно управља и да се репродукују ако су успјешни.

P3 Дефинисање покрива употребу институционално дефинисаних и документованих стандарда, водиља, темплејта и политика током процеса имплементације. Институција која ефикасно ради у оквиру ове димензије јасно је дефинисала како неки процес треба да се обави. Ово не значи да особље те институције прати ову водиљу.

P4 Управљање води рачуна о томе како институција управља процесом имплементације и осигурава квалитет резултата. Способност у оквиру ове димензије осликава мерење и контролу резултата процеса.

P5 Оптимизација обухвата ширину до које институција користи формалне приступе да побољша активности тог процеса. Способност ове димензије осликава културу сталног напредовања.

Сваки процес је уз помоћ ових димензија претворен у низ тзв. пракси (practice) од којих су неке кључне, а друге мање важне, зависно од конкретног процеса. На пример, процес D2 може бити описан кроз димензије P1, P2, P3 као есенцијалне и кроз преостале као мање важне.

Димензије се вреднују на четворостепеној скали, од „потпуно одговара“, до „не одговара“, док је на располагању и опција „није установљено“.

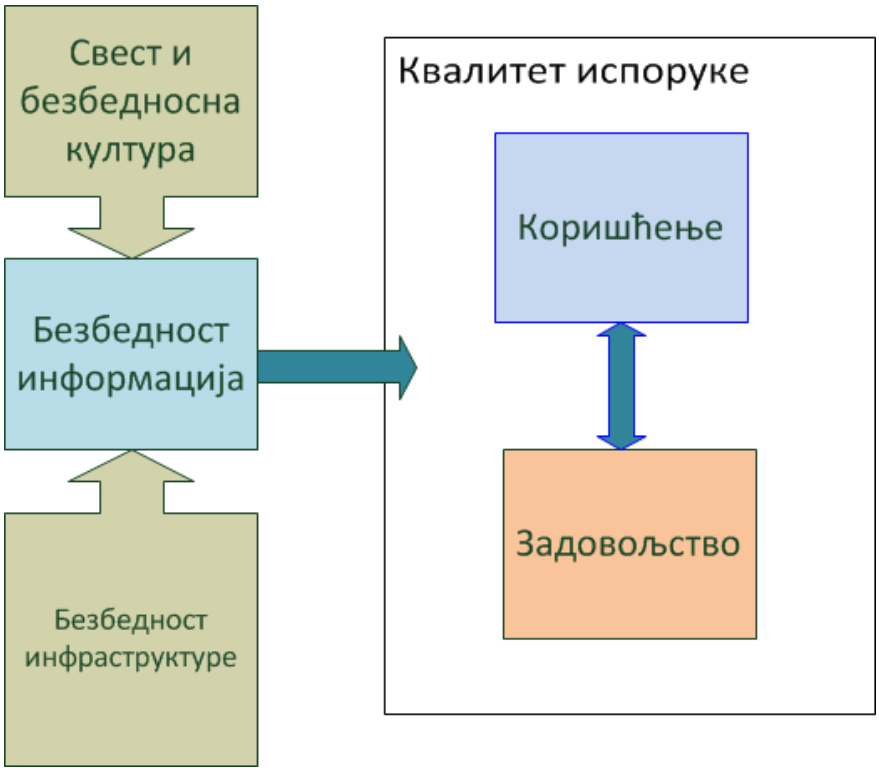
У наставку су издвојени елементи (праксе) који се тичу безбедности и приватности:

- Политика институције прописује захтеве за заштиту приватности података.
- Наставном особљу је пружена подршка у дизајну и развоју.
- Сви елементи физичке инфраструктуре су поуздани, робусни и довољни.
- Постоје проверене резервне копије (бекап) свих података.
- Сви елементи инфраструктуре се редовно контролишу ради осигурања валидности резервних копија и процедура повраћаја података у случају катастрофе.
- Приступ свим подацима студената захтева аутентификацију и ауторизацију.
- Формалним процедурама се експлицитно дефинишу питања употребе садржаја и њигове заштите од стране студената.
- Документована спецификација и планови осигуравају поузданост, целовитост и валидост прикупљања података, њихово чување и преузимање
- Целовитост и валидност дигиталних података се редовно надгледају.
- Процедуре за развој е-учења покривају целовитост и валидност дигиталних података.
- Ревизија метода процене ризика се врше у случају отказа система.
- Остварује се комуникација са ученицима о процедурама и технологијама које се користе пре почетка курсева.
- Редовно се прикупљају информације о проблемима са технологијом који нису већ покривени у склопу самог курса.

3.3 Модел квалитета е-образовања и безбедност информација

Ради проучавања утицаја безбедности информација на квалитет е-образовања, извршена је адаптација модела датог у [61] и креиран подмодел (слика 5). Овај подмодел има за циљ да апстрахује елементе који су значајни за квалитет е-образовања, гледано са стране безбедности информација. Као што је показано разматрањем модела и шема квалитета, безбедност информација, иако није детаљно апострофирана и експлицитно и детаљно елаборирана у моделима, фактички учествује у различитим категоријама фактора који утичу на квалитет е-образовања.

Подмодел апострофира елементе који су идентификовани као кључни за квалитет, а повезани су са безбедношћу информација.



Слика 5 - Подмодел квалитета е-образовања

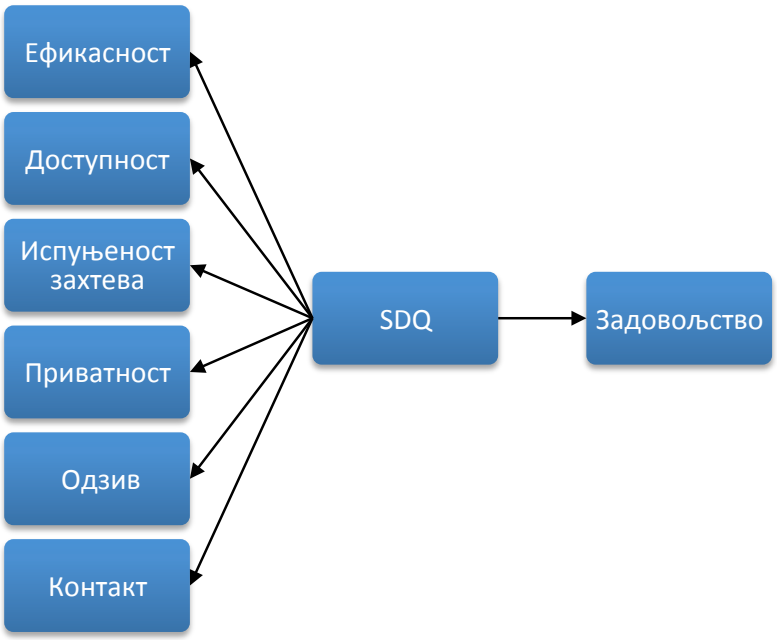
Овај подмодел издваја факторе који у оквиру различитих категорија утичу на безбедност информација, а онда даље на квалитет испоруке е-учења.

Безбедност информација подразумева све аспекте контроле ризика у свим релевантним областима е-образовања. У зависности од конкретног модела е-учења - да ли је у питању коришћење јединствене платформе (LMS), видеоконференције итд, разматрају се различите елементи који чине безбедност.

Два битна фактора (могу се назвати кумулативни фактори) су: безбедност инфраструктуре и свест и безбедносна култура. Безбедност инфраструктуре обухвата све оно што је под контролом установе, односно онога ко испоручује садржаје за е-учење. На пример, шифровање информација које се преносе ка систему за учење, део је питања безбедносне инфраструктуре.

Безбедносна култура није дословно наведена као фактор у постојећим моделима. Међутим, имајући у виду изузетан значај корисника на безбедност информација уопште, као и поједине критеријуме, који, донекле имплицитно, указују на потребу за едукацијом корисника (на пример ”Формалним процедурама се експлицитно дефинишу питања употребе садржаја и њигове заштите од стране студената” или ”Редовно се прикупљају информације о проблемима са технологијом који нису већ покривени у склопу самог курса”), појављује се јасна потреба за издвајањем овог елемента. Овај елемент је у ствари један од кључних доприноса саме тезе.

Оба елемента чине фактор звани ”безбедност информација”. То је фактор који директно утиче на квалитет испоруке. У том смислу може се говорити о квалитету услуге испоруке (SDQ - Service Delivery Quality). Током истраживања о томе како квалитет испоруке делује на задовољство корисника, развијен је модел у којем је представљена веза различитих елемената који чине квалитет испоруке [69]. Овај модел је, на основу опсежне анализе литературе, изнедрио таксономију квалитета испоруке, тако што је увео неколико елемената који су се у претходним истраживањима показали као кључни.



Слика 6 - Модел квалитета испоруке [69]

Елементи су приказани на слици 6. Безбедност информација није експлицитно међу овим факторима, али се ту појављују ”приватност” (значи безбедност личних података), доступност (један од фундамената безбедности), одзив (који може бити тесно повезан са безбедношћу) и контакт (чији један значајан део може чинити комуникација везана за безбедносне проблеме).

Из анализе модела квалитета и постојећих шема може се закључити следеће:

- **И модели и шеме углавном у неком облику апострофирају безбедност информација као фактор који у склопу инфраструктуре, али и других елемената, учествује у обезбеђењу квалитета е-образовања.**
- **Безбедност информација се најпре може одредити кроз факторе који делују на испоруку е-учења.**
- **Безбедносна политика је веома значајна.**
- **Квалитет е-учења је тесно повезан са квалитетом испоруке и задовољством корисника.**
- **Критеријуми који се налазе у шемама квалитета могу се класификовати у инфраструктурне и процедуралне.**

У складу са представљеним моделима и шемама квалитета, могу се дефинисати следећи генерални критеријуми од значаја за обезбеђење квалитета у е-образовању:

- **Обезбеђена аутентификација и ауторизација.**
- **Обезбеђено шифровање.**
- **Спровођење креирања резервних копија и њихово тестирање.**

- **Дефинисане процедуре које прописују безбедност личних података.**
- **Комуникација са корисницима о процедурама и начинима заштите садржаја и обавештавање о примењеним технологијама.**

4. Поверење и прихватање технологија за е-образовање и безбедност информација

Поверење корисника кључан је елемент за успех он-лајн бизниса [70], а у овом случају он-лајн бизнис је е-образовање.

Прихватање технологије је основ за имплементацију и сложен је конструкт у којем суделују различити људски и технолошки фактори. Прихватање технологија дефинише се кроз спој два основна показатеља: корисност и лакоћу употребе (perceived usefulness, perceived ease of use) и овакав приступ дат је у тзв. TAM (Technology Acceptance Model) теорији и њеним модификацијама [71].

4.1 Модел поверења у е-образовању

Поверење је дефинисано као ”чврсто убеђење у компетенцију ентитета да делује поуздано, сигурно и безбедно у датом контексту” [72]. У оквиру е-учења наглашен је значај поверења као ”обезбеђење поузданости нечијег својства” услед експанзије интернет алата [73].

Поверење у е-учење и е-образовање је сложено, и као и квалитет, заснива се на већем броју параметара. Већ постоје опсежна истраживања везана за ову проблематику. Једно од значајнијих је код Дајане Ванг [54]. У овом раду дат је оквир (framework) поверења. Овај оквир подсећа на оквир квалитета, јер су суштински квалитет, поверење и прихватање тесно повезане категорије. Нпр, уколико квалитет није на одређеном нивоу, корисник неће бити задовољан и неће имати поверење у коришћење, нити ће прихватити дату технологију.

У моделу Ванг предвиђа неколико категорија које утичу на поверење у е-учењу. То су: кредибилитет, дизајн, социо-комуникациони стил инструктора и - приватност и безбедност. У даљој анализи, сви фактори су класификовани у две категорије - инструкциони дизајн и приватност и безбедност. У провери овог оквира, добијени резултати говоре о томе да је утицај Безбедности и приватности (као конструкта који је такође састављен из више фактора) значајан, али нешто мање значајан од димензије инструкциони дизајн.

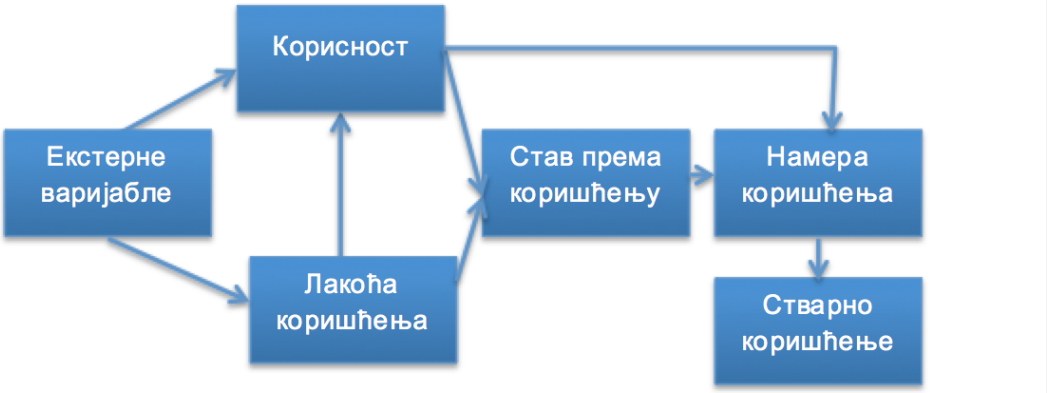
За потребе овог истраживања коришћен је поменути оквир [54], као и Костантин модел [74]. Суштина је да су формулисани кључни фактори који утичу на поверење корисника. Међу тим факторима налази се и безбедност информација. Фактор безбедности биће представљен одговарајућим модулом, који ће бити пројектован у наставку.

Поверење је означено као један од значајних индикатора квалитета е-сервиса [75] и истраживање утицаја безбедности (безбедносног модула) на поверење може расветлити и утицај на квалитет уопште.

4.2 Прихватање система за учење и безбедност информација

Прихватање технологија је такође мултидисциплинарни појам, за чије истраживање је креиран већи број модела [76]. У конктексту ове тезе реч је о технологијама које се користе за испоруку елемената е-учења, а још специфичније о LMS-у - систему за управљање е-учењем.

У моделу TAM (слика 7), који је најпопуларнији и на којем се заснивају многе друге варијанте [77] основни елементи који утичу на прихватање технологије могу се класификовати у два ”слоја”. Први представљају спољашње варијабле, које затим утичу на веровања корисника о корисности (percieved usefullnes) и лакоћи коришћења (easiness of use). Корисност говори о схватању корисника о томе у којој мери дата технологија може да унапреди његов посао. Ова два уверења утичу на став о намери коришћења (intention to use, да ли намерава да користи) и о томе колико ће заиста користити (actual use) .



Слика 7 - Модел TAM [77]

TAM је у суштини општи модел. За специфичне случајеве развијени су посебни модели, као што је на пример UTAUT или ELAM [78] који проширује UTAUT у сферу е-учења. Конкретна примена код Moodle може се наћи у [79].

TAM у подразумеваном облику не третира безбедност информација као варијаблу која може имати утицаја на ставове према коришћењу. Да ли и на који начин она утиче на ове елементе у конкретном случају (е-образовање) један је од задатака ове тезе.

Код е-трговине проверен је модел који предвиђа директну корелацију перцепиране безбедности (perceived security) и намере коришћења intention to

use). У том смислу проширен је класичан TAM тако да се компонента ”перцепирана безбедност” додаје као утицај на лакоћу коришћења, корисност и на крају и намеру коришћења [80]. Варијанта овог модела изабрана је за проверу у овом раду. Претпоставља се да ће корелација (ако се установи) ипак бити мање значајна, него код е-трговине, с обзиром на критичност процеса, тачније перцепцију корисника о критичности.

5. Стандардизација и безбедност е-учења

При креирању било ког модела потребно је узети у обзир стандарде који се баве датом облашћу генерално (у овом случају безбедношћу информација), као и стандарде који се баве безбедношћу у специфичној области (е-учењу), у склопу посебног вида регулативе. У наставку је дат крађи преглед стандардизације у безбедности и релевантне стандардизације у е-учењу.

5.1 Стандардизација безбедности

Званична стандардизација представљена је кроз скуп докумената фамилије ISO/IEC 2700x [81]. Неки од најзначајнијих су:

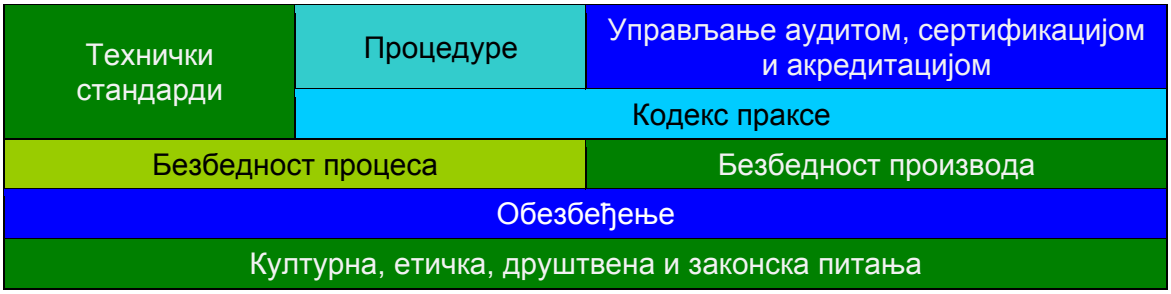
- 27000 – Системи за управљање безбедношћу информација – Преглед и речник
- 27001 - Системи за управљање безбедношћу информација – Захтеви
- 27002 – Прописи праксе (code of practice) за системе за управљање безбедношћу
- 27003 – Водич за имплементацију
- 27004 - Системи за управљање безбедношћу информација – мерење
- 27005 – Управљање ризицима итд.

Филозофија управљања безбедношћу у верзији стандарда из 2005. године ослањала се на PDCA методологију (слика 8), док се у новој верзији (2013) такав приступ ставља у други план, а акценат је на евалуацију квалитета безбедности организације и на компатибилности са другим стандардима, нарочито са ISO 9000.

Улаз у овај круг представљају захтеви и очекивања заинтересованих страна (interested parties, stakeholders), а излаз је управљање безбедношћу.

Слика 8 - Круг квалитета

Слика 9 представља елементе који фигуришу у стандардима 27000



Слика 9 - Елементи управљања безбедношћу (стандард ISO)

Стандард 27002 (2015) представља конкретан сет препорука добре праксе, који се могу применити у широком дијапазону информационих система, укључујући и систем за е-учење [82].

Први корак је процена ризика, којом се установљавају, квантификују и приоритетизују ризици према датим критеријумима за прихватање ризика и циљевима битним за саму организацију. Резултати би требало да послуже као водич за даље акције менаџмента и постављање приоритета у управљању безбедносним ризицима и за имплементацију мера заштите.

Ризик се може процењивати на нивоу читаве организације, њених делова, посебних компоненти система или чак на нивоу сервиса. По извршеној процени ризика, потребно је определити се за одговарајући модус управљања ризиком:

- применити одговарајућу меру заштите
- прихватити ризик
- избећи ризик не спроводећи активности које би до њега довеле
- пренети ризик на другога (добављача, осигуравајуће друштво)

Кроз једанаест класа мера заштите дефинисан је низ категорија релевантних за безбедност, као што је нпр. “Information security awareness, education, and training“, и дати су циљ мере заштите и једна или више мера заштите које се примењују за остваривање циља. ISO „меру заштите“ назива контрола („control“).

У оквиру документа Guidlines for auditors on information security controls [83] дата су упутства аудиторима за вршење прегледа имплементације и исправности мера заштите, укључујући проверу техничке компатибилности ових мера и успостављених стандарда организације. Уколико је са поступком заштите обухваћен систем за е-учење, ове препоруке могу бити даље искоришћене управо за проверу тог система, односно његових мера заштите.

5.2 Остали стандарди

Поред званичне стандардизације, отелотворене кроз ISO фамилије стандарда, постоје и други облици. Једна од познатих група препорука потиче од ITU-T, комитета за комуникације. У класи препорука са ознаком X, од X-800, па надаље, налази се низ докумената који се баве безбедношћу комуникација[84]. Нпр: ITU-T X.811 је Security frameworks for open systems: Authentication framework. Све препоруке су отвореног типа и доступне су преко официјелног сајта (http://www.itu.int).

Platform for Privacy Preferences Project (P3P) представља протокол организације W3, којим се веб-сајтовима омогућава да се изјасне о начину коришћења информација добијених из веб-читача (browser-a) [85]. Иако је предвиђена примена овог стандарда и у он-лајн образовању [41], сам стандард је напуштен и више се не одржава. Ипак, основне идеје и препреке у развоју могу бити на неки начин водиља у пројектовању неких других модела приватности ма Интернету. Овај стандард се заснивао на томе да веб-читач може да протумачи декларацију приватности веб-сајтова који се посећују и на основу тога омогући контролу приватности корисника. Већина произвођача веб-читача није увело

подршку за овај стандард, тачније само Microsoft Internet Explorer и Edge га подржавају.

5.3 Безбедност информација у оквиру стандарда из области е-учења

Постоје бројне организације које се баве креирањем стандарда и препорука у области е-учења. Међу најзначајнијим су: Learning Technology Standardization Committee (LTSC), the IMS Global Learning Consortium, the Aviation Industry CBT Committee (AICC) , and the U.S. Department of Defense's Advanced Distributed Learning (ADL).

Стандарди који се баве е-учењем углавном се састоје из неколико делова [41]. Први описује модел података и даје нормативе и апстракт садржаја, други је формални опис (углавном кроз XML) и трећи представља API, интерфејс за сарадњу са другим системима.

Веома детаљан преглед стандарда у области е-учења дат је у [86].

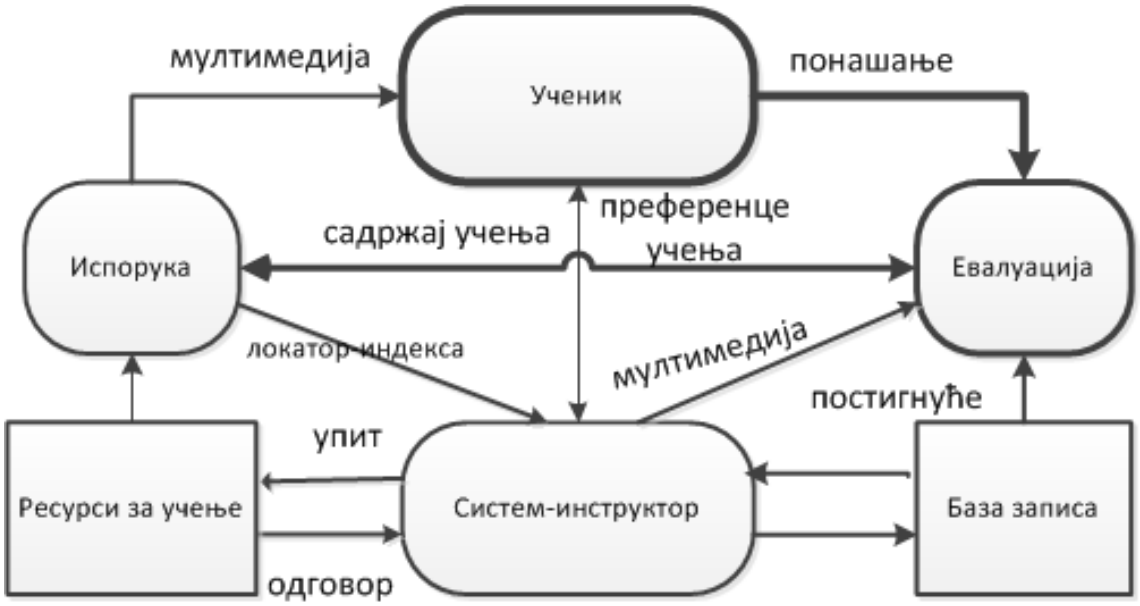
5.3.1 IEEE 1484

Најпознатији и најдетаљнији стандард је IEEE 1484 [87] (слика 10). У склопу његовог сегмента 1484.1-2003 IEEE Standard for Learning Technology-Learning Technology Systems Architecture, дат је и модел е-учења високог нивоа. Задатак ове архитектуре је да пружи оквире (framework) високог нивоа за развој различитих система за е-учење и олакша њихову евалуацију и поређење.

Поред радне групе IEEE 1484, LTSA је израђен кроз активности различитих других организација:

- ADL (DoD Advanced Distributed Learning http://www.adlnet.org)
- AICC (Aviation Industry Computer-Based Training (CBT) Committee http://www.aicc.org)
- ANSI IISP (American National Standards Institute, Information Infrastructure Standards Panel): http://www.ansi.org/iisp)
- "Architecture Abstraction Hierarchy Reference Model", by Frank Belz, Dan Suthers, Tom Wheeler. http://advlearn.lrdc.pitt.edu/its-arch/p1484/ARM.html
- ARIADNE Project of European Union: http://tina.lancs.ac.uk/computing/research/cseg/projects/ariadne/
- CMU (Carnegie Mellon University), "Tool/Agent Communication", by Steven Ritter. http://domino.psy.cmu.edu/ieee/tooltutorspec.html
- CORBAMED (Common Object Request Broker Architecture of Object Management Group (OMG), Medical Infomatics): http://www.omg.org/corbamed

- EOE (Apple Computer's Educational Object Economy): http://www.eoe.org/
- IMS (Educom's Instructional Management Systems) Project http://www.imsproject.org
- ISO-IEC JTC1 BT-EC (International Standards Organization - International Electrotechnical Committee, Joint Technical Committee 1 -- Information Technology, Business Team on Electronic Commerce): http://www.din.de/ni/aktuell/j1btechtml
- ISO-IEC JTC1 GII (Global Information Infrastructure) Standards Roadmap: a catalogue and analysis of GII standards. http://www.GlobalCollaboration.ORG/jtc1/gii-roadmap
- ISO-IEC JTC1 CAW (Cultural Adaptability Workshop): http://www.itscj.ipsj.or.jp/caw
- ISO-IEC JTC1 SORT (Standards Operations Roundtable): http://www.GlobalCollaboration.ORG/



Слика 10 - LTSA архитектура [88]

Компоненте LTSA су:

- Процеси: Ученик (Learner), Евалуација (Evaluation), Систем-инструктор (System Coach), Испорука (Delivery process).
- Токови: Понашање (Behavior), Тестирање (Assessment), Постигнуће (Performance), Индекс упита и садржаја (Query Index, Content Index), Индекс локатора (Locator Index), Садржај учења (Learning Content), Мултипедија (Multimedia), Стил учења (Learning Style)
- Складишта: База записа (Records Database), Библиотека знања (Knowledge Library)

Процес "Ученик" (Learner Process) је апстракција ученика и може представљати појединачног ученика, групу ученика која учи индивидуално, групу која учи колаборативно итд.

Ученик добија поставку Мултимедије и његово Понашање се посматра. На овом нивоу апстракције, Мултимедија и посматрано Понашање су приказани посебно. Међутим, реалне имплементације обично комбинују ове елементе у један или више интерфејс-модула, као што су прозорски системи (Windows), презентација у веб-читачу, специјализоване апликације итд.

Стил учења је установљен у сарадњи са Системским инструктором.

Ток Понашање представља Учениково кодирано понашање, од Ученика ка процесу Евалуације. Код овог процеса Понашање је уклопљено у одговарајући контекст упаривањем Садржаја учења са одређеним распоном одговора Понашања.

Кодирање Понашања је начин на који су информације о Понашању организоване, нпр. притисак тастера, клик миша, гласовна команда итд. Кодирањем се представља Учениково понашање независно од Садржаја учења.

Процес Евалуација резултује информацијом за Евалуацију и шаље податке о Евалуацији даље Систем-инструктору. Процес Евалуација креира информацију о Постигнућу, која се чува у Бази записа.

Процес Евалуација користи објекат Садржај Учења да омогући контекст Учениковом понашању и одреди одговарајућу Евалуацију.

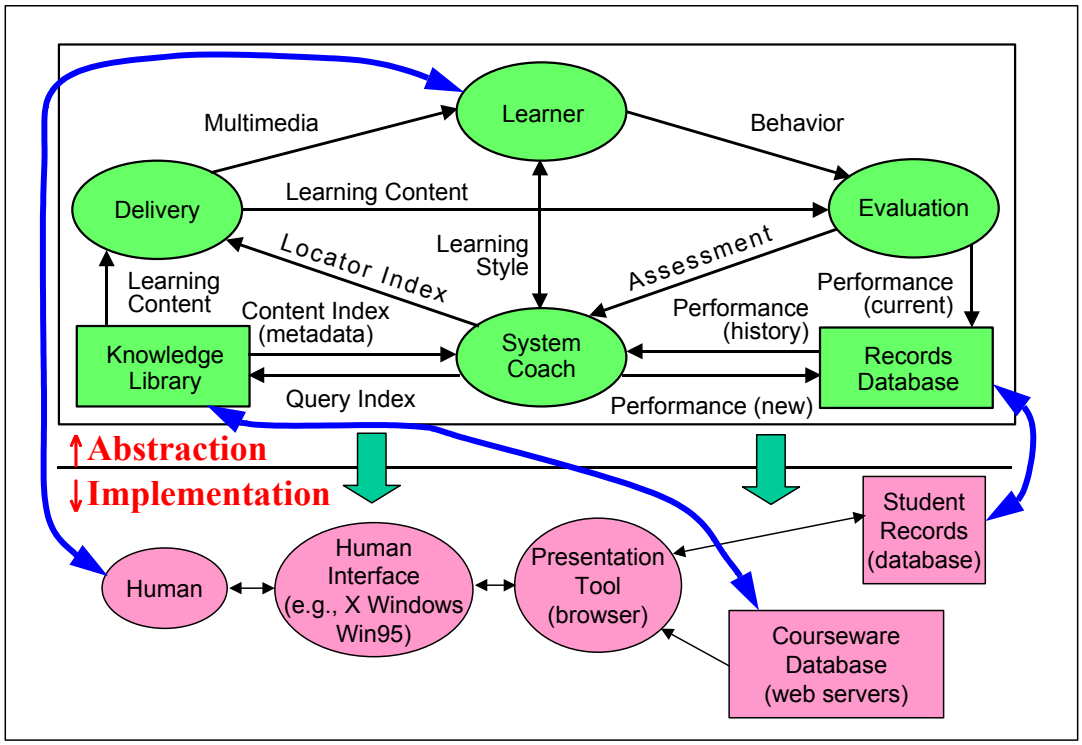
Процес Евалуација шаље информације о постигнућу и чува у Бази (на пример ”питање 17, одговорено тачно, потрошено 85 секунди”)

Библиотека знања чува различите податке (туторијале, алате, експерименте... Одговарајући материјал се доставља на основу Индекса Контекста (метаподатака). На основу ових метаподатака процес Испорука добавља Садржај.

Процес Испорука трансформише садржаје добијене из Бибилотеке знања у одговарајући мултимедијални облик.

Имплементација LTSA у онлајн учењу

Као што је већ наведено: LTSA је генеричка архитектура. У конкретној имплементацији (на пример у е-образовању), остварује се мапирање појединих компоненти у одговарајуће репрезенте електронског система за учење. На слици 11 приказано је да је ”човек” (корисник, ученик) мапиран у компоненту LTSA Learner, а база курсева у Библиотеку знања (Knowledge Library).



Слика 11 - Мапирање компоненти LTSA код онлајн сценарија учења (из [89])

Елементи безбедности у IEEE 1484

У табели 2 приказани су детаљи стандарда IEEE 1484 везани за безбедност и приватност [36].

Са **D** су означене ставке које су дефинисане стандардом, са I ставке које варирају зависно од конкретне имплементације, са **O** ставке које превазилазе оквире стандарда и са **N** оне које стандард није дефинисао.

Табела 2 - Елементи стандарда IEEE 1484 везани за безбедност

Модел	Спецификација	Модел	Спецификација
Session-View безбедносни модел	D	Модел непорецивости	I
Модел преговарања о безб. параметру	D	Модел порецивости	I
Модел безбедносне екстензије	D	Модел приватности	N
Модел контроле приступа	D	Модел поверљивости	N
Модел идентификације	I	Модел шифровања	N
Модел аутентификације	O	Модел целовитости података	N
Модел деидентификације	O	Провера сертификата	N
Модел ауторизације	I	Модел дигиталног потписа	N
Модел делегације	I		

У склопу LTSC стандарда посебан део – PAPI (Public and Private Information) се бави самим учеником, односно синтаксом и семантиком његових информација и облицима приступа. Елементи којим се бави су: вештине, способности, контакт-информације, стил учења, перформансе, лични портфолио, безбедносни параметри. Стандард предвиђа различите типове прегледа информација, према одговарајућим улогама: наставник, ученик, родитељ, послодавац.

Два дела PAPI стандарда се посебно баве безбедношћу: IEEE 1484.2.3 и 1484.2.23. Први даје препоруке за имплементацију ставки везаних за безбедност, док други разматра кључеве и приступне параметре.

Безбедност, приватност и заштита података дефинисани су посебним моделима (Session-View Security Model). Сесија и преглед (view) су посебно третирани. Преглед је аналоган прегледу код базе података, представља приступ одређеном запису о ученику. Сесија представља трајање прегледа и започиње одговарајућом провером идентитета. Конкретни механизми аутентификације и ауторизације нису специфицирани, као ни захтеви по питању дигиталног потписа, али су подржане различите опције, нпр. ISO/IEC 15945.

PAPI посебно обрађује питање приступа спољним репозиторијумима и предвиђа креирање тзв. сурогат идентификатора, којим се ученик пријављује на спољни сервис, тиме укидајући могућност његовог праћења.

5.3.2 IMS Global Learning Consortium – LIP

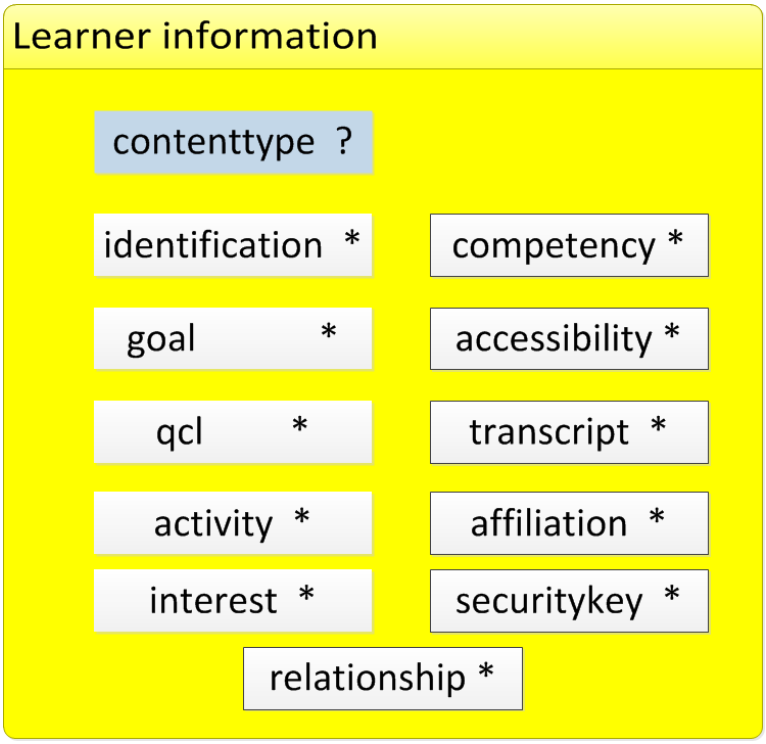
IMS Global Learning Consortium је организација која се бави развојем отворених препорука за е-учење, разматрајући кључне проблеме и изазове у дистрибуираним окружењима за учење кроз низ спецификација, укључујући метаподатке, ентерпрајз-спецификације, спецификације пакета учења, тестова и питања [90]. Између осталог, IMS спецификација Learner Information Package (IMS LIP) обрађује интероперабилност информационог система ученика са другим системима за учење [91] (слика 12). Подаци о ученику обликовани су као колекција података о ученику и типично садржи запис о степену образовања, дневник учења, дневник целоживотног учења итд.

IMS LOM се бави питањима приватности у верзији 1.0 и овом сегменту придаје велики значај. Предложена су два механизма:

- Подршка за укључивање података које описују ниво приватности, права приступа и целовитост података. Ови подаци су дефинисани кроз посебну метаструктуру.
- Подршка за податак о кориснику који би се користио за обезбеђење преноса података. Овај податак је дефинисан као ученикoв безбедносни кључ (learner security key).

Безбедносни кључеви чине структуру која чува различите кључеве који обезбеђују комуникацију између ученика и система и сервиса за е-учење.

За разлику од PAPI-a, IMS поред података пружа и модел, односно метаподатке који подржавају моделовање. Такође, сам модел је изузетно флексибилан.



Слика 12 - IMS LIP модел података према (према [92])

5.3.3 EDUCAUSE – Internet2 EduPerson

EduPerson је спецификација потекла од Internet2 иницијативе и EduCause [93]. Представља покушај уобличавања типичних информација о ученику, али и другим лицима у институцији, у склопу LDAP шеме, која би олакшала креирање институционалних директоријума, дајући одговарајуће шаблоне.

EduPerson није опширна као PAPI и, будући да покрива ширу класу корисника него што су то ученици (запослене, алумни), предвиђа мање специфичне информације: име, надимак, организацију, контакт информације, фотографију, преферирани језик и сл.

Кључни атрибути везани за безбедност су userCertificate и userSMIMECertificate. Дефинишу X.509 сертификат ученика, односно сертификат за MIME апликације е-поште.

Остали стандарди везани за е-учење углавном се баве садржајем и не третирају област безбедности. На пример [94]:

- AICC (Aviation Industry CBT Committee) се фокусира на практичне аспекте, дајући препоруке за платформе за е-учење, периферије, аудио-уређаје и сличне детаље имплементације

- Aliance of Remote Instructional Authoring and Distribution Networks for Europe (ARIADNE) се бави углавном метаподацима са циљем дељења и поновног коришћења материјала
- Learning-Sharable Content Object Reference Model (ADL-SCORM) је оријентисан ка начинима агрегације, описа и секвенцирања објеката учења.

Упркос постојању различитих стандарда и њиховој детаљној спецификацији, питање њихове имплементације остаје отворено. Код многих популарних окружења за е-учење није у старту укључена подршка за стандарде, било зато што они тада нису били развијени, било због непридавања кључног значаја стандардима (проценом да је имплементација неисплатива). Стога код система који су већ у функцији није једноставно додати подршку за стандарде, јер би то у појединим сегментима захтевало комплетан реинжењеринг.

Из прегледа стандарда релевантних за тематику ове тезе, могу се извести следећи закључци, којима ће се даље руководити у раду:

- **Постоје детаљни општи међународни стандарди који се баве безбедношћу информација и који се могу користити за пројектовање безбедносног информационог система, односно одговарајућег модула у било ком окружењу. Те могућности односе се на методологију пројектовања, али и на конкретне праксе (према ISO 27002). PDCA је препозната као методологија погодна за пројектовање модула.**
- **Постоји већи број неусаглашених стандарда из области е-учења и одређен број тих стандарда разматра и безбедност информација. У пракси ови елементи нису имплементирани у ширем обиму. Разлози за то могу се тражити у комплексности предложених решења. Са друге стране, стандарди су и релативно флексибилни, тако да се могу проширити и прилагодити одређеној потреби.**

6. Безбедност и е-учење у Србији: Студија случаја

Да би се установиле конкретније информације у вези свести корисника о примени безбедносних механизама, односно општим показатељима безбедности, извршена су одређена истраживања на нивоу Републике Србије (крајем 2012. године).

Релативно мали број студијских програма је акредитован за комплетне студије на даљину. Године 2016. тај број износи укупно 42, што је 1,85% од укупног броја програма [95]. Са друге стране, постоји велики број студијских програма који су подржани неком варијантом е-образовања. Ова форма није озваничена, тако да је веома тешко одредити колико студијских предмета је организовано на овај начин.

Најпопуларнија платформа за е-учење Moodle је широко заступљена и, према подацима са званичног сајта Moodle.org постоји око 250 регистрованих сајтова са инсталираним Moodle-ом [96]. Одређен број сајтова није излистан јавно.

Од постојећих сајтова за потребе истраживања је изабрано 89. Изостављени су сајтови без курсева, као и сајтови са бесплатних домена, на којима су углавном биле присутне рекламе и који у самом старту нису валидни за даље истраживање. Само три сајта су користила SSL, али са својим сертификатом (самоиздатим). Тридесет седам сајтова је имало затворен приступ (без могућности саморегистрације).

Од 52 сајта са отвореном регистрацијом 21 није имао никакву политику лозинки, а три су омогућавала приступ са Facebook налогом. Свега пет сајтова имало је captcha анти-бот проверу.

Ниједан од сајтова са саморегистрацијом није имао политику коришћења. Овакав документ у јасно истакнутом облику није установљен ни код других инсталација (без саморегистрације).

Иако је истраживање обухватило само део инсталација, добијене информације су једнозначне и доводе до закључка да безбедносни механизми нису приоритет код платформи Moodle-а, као најпопуларнијег окружења за е-учење.

6.1 Свест корисника о безбедности у е-учењу

На Техничком факултету (данас Факултету техничких наука) у Чачку се од 2007. године у озбиљнијем обиму реализују наставне активности коришћењем он-лајн учења/наставе. Изабрана платформа је Moodle [97], из неколико разлога: отвореног је кода, обилује могућностима, интуитивног је интерфејса, добро

подржан (преводи, закрпе), лако проширив и прилагодив и веома распрострањен (поседује многобројну заједницу).

На факултету су активна два Moodle система: један се користи првенствено у виду потпоре за традиционалну наставу и налази се на адреси https://itlab.ftn.kg.ac.rs/moodle, а други је био делом у функцији за потребе потпуног он-лајн учења (на једногодишњем мастер студијском програму Техника и информатика - Мастер за е-учење), а делом, такође, као blended варијанта за потребе других мастер-програма и налази се на адреси https://e-lab.ftn.kg.ac.rs/moodle

У званичним актима факултета не постоји систематизација он-лајн учења, није дефинисано на који начин се спроводи овај вид учења/наставе, каква су права и обавезе студената и наставника, нити ко је одговоран за рад самог система, а самим тим и за безбедност података.

Спроведена је мини-анкета на оба система са циљем утврђивања односа студената према безбедности и приватности у он-лајн учењу. Учествовала су 163 ученика (студента).

На питање да ли је у реду саопштити колеги сопствено корисничко име и лозинку, више од трећине испитаника првог система је одговорило потврдно, док је само 10% тако одговорило на другом систему.

На питање да ли треба чувати извештаје о активностима на сајту, на првом Moodle систему 48% је одговорило потврдно, док је на другом чак 86% одговорило потврдно (Табела 3).

Табела 3 - Ставови студената у вези чувања података о њиховим активностима (у %)
треба чувати извештаје о вашим активностима

Потребно је чувати извештаје о вашим активностима на сајту за е-учење	
Уопште се не слажем	7
Не слажем се	13
Немам мишљење	28
Слажем се	44
Потпуно се слажем	9

Индикативне информације су добијене као одговор на питање о томе ко би требало да има приступ подацима профила. У табели 4 приказана је дистрибуција одговора.

Табела 4 - Ставови студената у вези приступа подацима профила (у %)

Ко би требало да има приступ подацима мог профила?	
Нико	10
Само наставник	25
Само колеге са курсева	21
Само регистровани корисници	25
Свако	2
Хтео/ла бих да одредим видљивост података	18

Ставови по питању података из профила нису искристалисани. Делом се то може објаснити тиме што корисници уписују различит број информација, те на тај начин управо ограничавају укупне информације које су видљиве, без потребе да се то ради системски. Такође, могуће је да известан број корисника није сигуран ко већ може видети које податке из профила, те су стога дали резервисане одговоре.

Интересантни су и одговори везани за политику лозинки (Табела 5 - Ставови везани за политику лозинки (у %))

Табела 5 - Ставови везани за политику лозинки (у %)

Какве лозинке користите?	
За сваки систем (сајт, рачунар) користим посебну јаку лозинку	29
За већину система користим посебне јаке лозинке	29
За најважније системе користим једну јаку лозинку, за остале системе користим једноставну лозинку	21
Користим једну јаку лозинку за све системе	18
Користим једну једноставну лозинку за све системе	2

Значајан проценат корисника има једну лозинку за различите системе. Ово представља озбиљан сигурносни ризик, јер компромитовањем лозинке на једном систему, бивају компромитовани и остали.

У табели 6 дати су ставови испитаника о томе да ли им је потребна додатна едукација из области сигурности и приватности на интернету.

Табела 6 - Ставови о потреби за додатном едукацијом

Потребна ми је додатна едукација из области безбедности информација	
Уопште се не слажем	12
Не слажем се	23
Немам мишљење	26
Слажем се	34
У потпуности се слажем	5

Интересантна су запажања и сугестије које су студенти оставили у отвореном облику. Следе неке од њих:

> *„Потребно је писменим путем утврдити правила у вези заштите личних података.“*

> *„Требало би додати IP trace за сваког студента, да се при сваком приступу памти IP адреса са које је приступао, тако да касније при нежељеном упаду на други профил може да се одреди ко је у питању“*

> *„Генерално мислим да смо врло мало обавештени о ризицима које доноси Интернет, и да ретко размишљамо о томе колико и на које све начине је угрожена наша приватност док смо на Интернету. Правила безбедног понашања се у пракси ретко користе чак и од стране оних корисника који их знају.“*

На основу ових истраживања, која су ограничена по свом обиму и репрезентативности узорка, може се ипак стећи дескриптивна слика која говори о стању е-учења у Србији, а посебно о безбедносним аспектима:

- **Основни безбедносни механизми које пружа сам систем без додатних интервенција, као што су безбедносна политика (site policy), captcha код, шифровани приступ страни за пријаву (TLS) у великој већини случајева нису искоришћени.**
- **Свест корисника о безбедносним ризицима и њихова безбедносна култура је на нивоу који захтева додатну едукацију.**

Комбиновањем ове две околности, повећава се укупна вероватноћа угрожавања безбедности, односно ризик од различитих претњи нарушавања приватности и угрожавања података самог система.

7. Креирање безбедносног модела корисника

Е-ученик је основни корисник система за е-учење. Како је образложено у претходним поглављима, корисник је витална карика у ланцу безбедности и често најслабија. Ојачавањем ове карике могу се комплетирати постојеће, конвенционалне безбедносне контроле и подржати изградња целовите безбедносне архитектуре. На тај начин испунили би се и поједини захтеви обезбеђења квалитета.

Да би се добио што бољи увид у то како се понаша типичан корисник система за е-учење, потребно је дефинисати његов модел. Стандарди покривају модел ученика превасходно у контексту образовних активности. У том смислу и IMS LIP дефинише податке и метаподатке којима се описују едукативне карактеристике ученика, док се фактички само једним елементом дотиче безбедности. Овакав приступ је суштински оправдан, јер је фокус стандарда на моделовању у контексту образовања. Са друге стране, не постоје препреке да се модел прошири потребним структурама које би служиле за заокруживање модела корисника са стране безбедности.

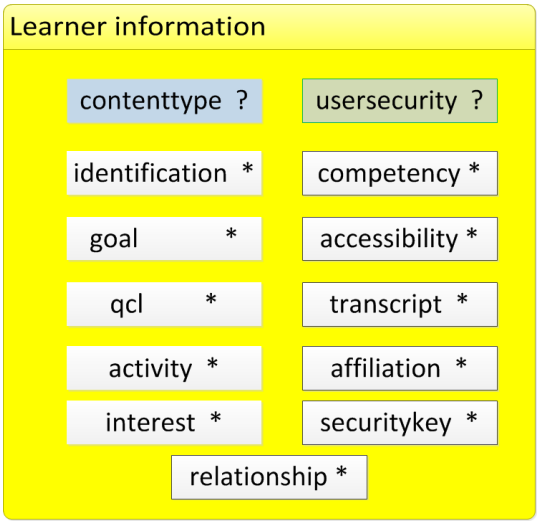
Поред е-ученика, постоје и друге класе корисника, међу којима су најбројнији наставници (тутори, предавачи...). Модел ученика може се применити на било ког корисника, међутим приоритет је е-ученик из следећих разлога:

- број ученика је за ред (или више) величине већи од броја особља и аутоматизација процеса је од већег значаја
- ученик проводи значајно време примајући информације и интеграција садржаја везаних за безбедност се логички наставља на процес који ученик већ изводи

Упркос томе, не постоји препрека да сви корисници имају профил ”ојачан” безбедносним елементима.

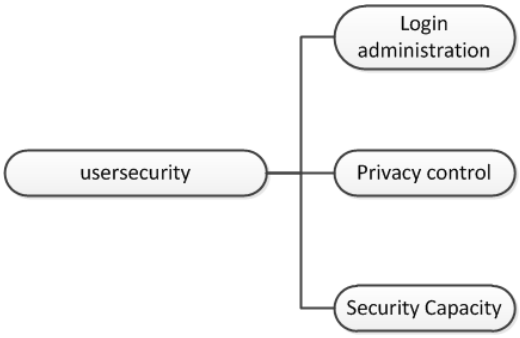
7.1 Проширење IMS LIP

Стандардни модел је потребно проширити релевантном структуром помоћу које би се евидентирали параметри који су значајни за унапређење корисникове безбедносне позиције. На основу спроведених истраживања (анкетирања) е-ученика, као и на основу релевантне литературе, модел је проширен структуром названом **usersecurity**, која има задатак да обезбеди управљање корисниковом безбедношћу (слика 13).



Слика 13 - Проширени IMS-LIP модел корисника

Предвиђено је да постоји једна оваква структура (знак кардиналности ”?” указује на то). Интерни изглед структуре дат је на слици 14.



Слика 14 - Структура usersecurity

Основу структуре чине три елемента. Први, назван ***Login administration*** карактерише корисниково управљање пријавом. С обзиром на исказану неодговарајућу праксу креирања лозинки, управљања сесијом и вишеструке употребе идентичних слабих лозинки, одлучено је да се формира посебан елемент којим ће се евидентирати корисников статус по питању управљања пријавом и одржавања сесије. Овај елеменат се аутоматски генерише од стране система и корисник не може да га директно мења. У зависности од корисникове праксе, елеменат се ажурира аутоматски. Предвиђено је да узима вредности од 1-3, при чему је број 1 низак степен управљања и подразумева да корисник минимално води рачуна о својим подацима за пријаву, док број 3 означава висок степен управљања пријавом. Суштина елемента је да у спрези са осталим

компонентама архитектуре утиче на безбедносну свест корисника по питању овог сегмента, који се показао као критичан, а то је управљање пријавом.

Други елемент је ***Privacy Control***. Овај елеменат дефинише ниво приступа личним подацима корисника, тј. подацима које садржи профил корисника, као што су нпр. адреса е-поште, број телефона, адреса, фејзбук страна итд. Предвиђено је да овај параметар може задавати сам корисник, али и да се може поставити на аутоматски контролисану вредност. Ова вредност у том случају зависи од степена безбедносне свести корисника. Могуће су, дакле, следеће поставке:

- аутоматски (регулише систем на основу понашања)
- потпуна видљивост
- видљивост на нивоу курса (сви који похађају исти курс, могу видети податке)
- видљивост на нивоу наставника (само наставник на курсу може видети податке)
- видљивост на нивоу администратора - овлашћеног лица (нико осим администратора нема приступ подацима)

Трећи елемент је безбедносни капацитет *(**Security Capacity**).* Овај елеменат описује општи капацитет корисника, односно целокупну оцену понашања у односу на безбедност - за све параметре система који се прате. Вредности елемента су:

- висок капацитет
- средњи
- низак капацитет.

Тенденција је да се сама структура **usersecurity** дефинише на једноставан начин, који није превише захтеван за имплементацију и одржавање, а са друге стране даје довољно елемената за спровођење корективних акција од стране безбедносног модула. Такође, компатибилност са постојећим стандардима је императив, будући да се на тај начин обезбеђује преносивост и релативно једноставна могућност усклађивања са системима који тренутно подржавају стандарде или ће имати подршку у будућности.

Структура елемента usersecurity формално се представља кроз одговарајућу XML структуру у маниру који иначе користи IMS LIP, на следећи начин:

<usersecurity>

loginadmin, element, positive integer

privacycontrol, element, positive integer

securitycapacity, element, positive integer

Структура би требало да буде портабилна, тако да у склопу података о кориснику буде извезена у XML и касније увезена у други систем, односно тако да може размењивати податке са другим системом.

8. Креирање модела безбедности информација у е-учењу

Безбедност је дефинисана као мултидисциплинарни концепт и управљање безбедношћу захтева иновативан приступ, с обзиром на сложеност модерних информационих система и разноврсност напада и злоупотреба. У том смислу императив је развијање свеобухватног, холистичког модела, који узима у обзир разноврсне факторе од значаја за безбедност. На тај начин омогућава се систематична реализација одговарајућих контрола (механизама и процедура заштите) и формира оквир за константно унапређење безбедности утицајем на све релевантне категорије од којих она зависи.

Формирање модела има за задатак да концептуализује безбедносне факторе е-учења, што би требало да пружи основу за пројектовање модула.

У наставку су представљени битни кораци при дефинисању холистичког модела и дати примери одговарајућих архитектура, са циљем прегледа елемената који би могли бити значајни за развој одговарајуће безбедносне архитектуре у контексту е-образовања и касније реализације модула као њеног кључног елемента.

8.1 Методологије и модели холистичког приступа

Да би се безбедности приступило на свеобухватан начин, неопходно је издвојити различите елементе који чине сам концепт. Неке од идентификованих категорија од значаја за овакав приступ су [98]:

- Политика безбедности информација. Потребно је дефинисати предвиђено понашање корисника и документовати га на начин који апстрахује техничке детаље и разумљив је крајњим корисницима и менаџменту.
- Анализа и управљање ризицима.
- Дефинисани оквири за обезбеђење континуитета у раду.
- Управљање конфигурацијом: свака измена софтвера је документована и следљива.
- Раслојавање дужности: распоређеност одговорности и привилегија на више од једне особе.
- Развој свести о безбедности информација код корисника. Праћење поштовања процедура.

Са циљем одговарајућег управљања поменутим разноврсним категоријама, уведен је појам архитектуре безбедности информација (ISA - Information Security

Architecture). ISA се дефинише као процес развоја свесности о ризицима, провере постојећих контрола и усклађености постојећих и нових контрола са безбедносним циљевима организације [99]. ISA је управљачки процес усмерен ка постизању и одржавању безбедносних сервиса као што су нпр. аутентификација и ауторизација.

Формирани су многи модели ISA са циљем обухватања технолошких, организационих и законских аспеката. Примери се могу пронаћи код Трчека, Тјудора и других. Један од примера је стандардизовани модел (ISO 27000), о којем је било речи у поглављу о стандардизацији, оформљен од стране међународне организације за стандарде [100]. Такође, у српском закону, истиче се потреба за свеобухватним приступом - у члану 3, став 2 наводи се:

> *начело свеобухватне заштите* – мере се примењују на свим организационим, физичким и техничко-технолошким нивоима, као и током целокупног животног циклуса ИКТ система [101]

8.1.1 Модел ISO 27000

У склопу фазе планирања (Plan) одређује се опсег система за управљање безбедношћу (ISMS) и усваја безбедносна политика. У оквиру фазе извођења (Do) врши се имплементација контрола и процедура. Ова фаза ослања се на Code of Practice [102] у којем се опширно дефинише скуп контрола које покривају разноврсне аспекте, као што су безбедносна политика, безбедност запослених, мрежна безбедност, управљање континуитетом итд.

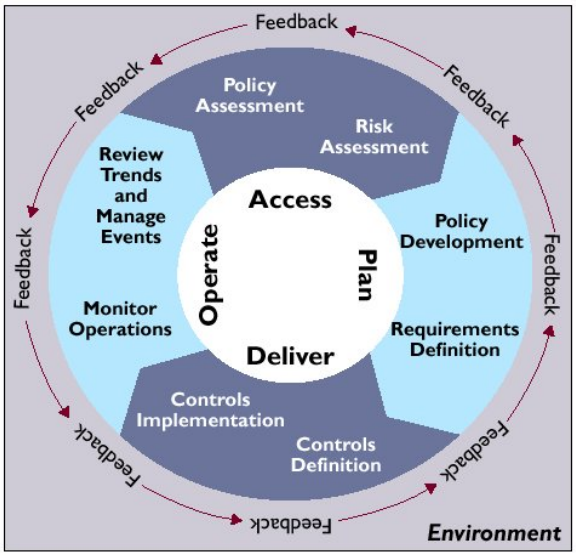
У фази провере (Check) имплементиране контроле се проверавају, а затим спроводе унапређења.

У фази деловања (Act) систем се константно прегледа и прати, а информације прослеђују фази планирања.

Према ISO 27005:2005, предвиђа се мапирање активности при успостављању и одржавању система за управљање безбедношћу информација, које одговара PDCA кругу квалитета. Крајем 2013. године издати су нови стандарди серије 27000. Дошло је до измена у концептима и терминологији [103]. Одређен број контрола је избачен, а такође је додат низ нових. Нарочит напор је уложен у усаглашавање са другим стандардима (ISO 9000, 22301) Такође, PDCA циклус није обавезна методологија за изградњу информационог система за управљање безбедношћу.

8.1.2 Остали приступи

Приступ сличан ISO-у дали су и Рис и др. у свом PFIRES моделу [104] (слика 15). PFIRES је првобитно био намењен електронској трговини, али је касније проширен. Основу налази у циклусу развоја производа и софтвера. Модел предвиђа краткорочне циљеве, који су оперативни и разрађени до дневног нивоа и дугорочне стратегије, које захтевају значајније укључивање вишег менаџмента.



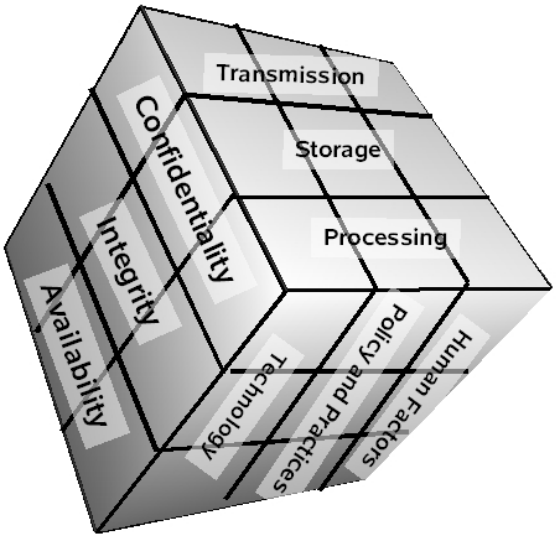
Слика 15 - Животни циклус PFIRES модела [105]

Тјудоров приступ илустрован је сликом 16 [99]:

Слика 16 - Тјудоров модел [99]

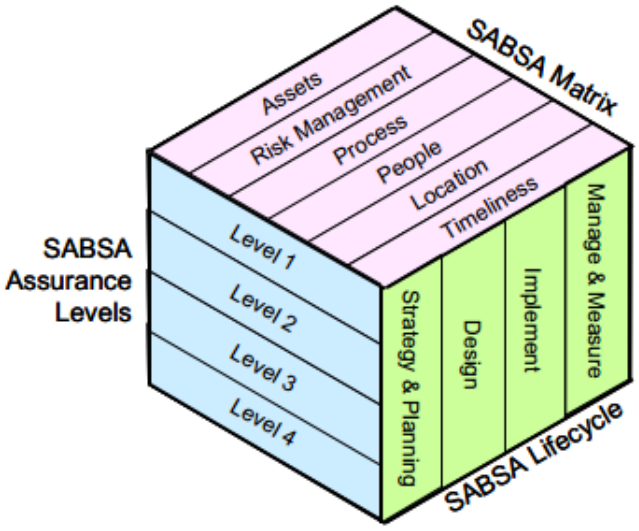
Иако су у наведеним примерима учињени покушаји да се формирају ISA у холистичком маниру, није остварен приказ контрола које би покриле мултидисциплинарни дијапазон захтева једног информационог система. Дефинисање контрола произилази из наредних фаза, пре свега из анализе ризика.

МекКамбер је развио истоимену коцку безбедности, која такође има за циљ интеграцију различитих аспеката безбедности [106] (слика 17).



Слика 17 - Меккамберова коцка [106]

Једно од најкомплекснијих окружења (оквира - framework) за развој безбедносне архитектуре је SABSA (Sherwood Applied Business Security Architecture). Такође подразумева циклус налик PDCA, а матрица се може приказати и у виду коцке [107] (слика 18).



Слика 18 - SABSA матрица [107]

Када се погледају различити приступи, може се закључити да су у својој суштини веома слични. Било да су дословно дефинисани као вишедимензиони (као што су Sabsa матрица или Меккамберова коцка) или не, модели јесу по природи вишедимензиони, јер интегришу различите процесе, односно техничке

и не-техничке аспекте безбедности у једну повезану целину. Из датих модела могли би се издвојити и заједнички имениоци: политика безбедности, праћење мера и људски фактор (People: свест о безбедности).

8.2 Место свести о безбедности у холистичком моделу безбедности

Као што је приказано у моделима, али и наглашено у претходним поглављима, људски фактор је ”најслабија карика” безбедности и унапређење овог елемента може имати директан позитиван утицај на целокупан биланс безбедности датог система.

Постоји више нивоа на којима се може унапређивати свест корисника. У публикацији америчког националног института за стандарде и технологију детаљно је описан процес изградње програма унапређења безбедносне свести корисника [108]. У овом раду се између осталог каже: *"Learning is a continuum; it starts with awareness, builds to training, and evolves into education."* (Учење је непрекидно; почиње са свешћу, изграђује се до нивоа тренинга и еволуира у образовање.)

Програми унапређења безбедносне свести су ”пасивни”, тј. корисник је превасходно рецептор информација. У случају тренинга (обуке), корисник добија активнију улогу. Тада се за потребе одређеног радног места профилишу знања и умећа из области безбедности информација, које корисник треба да поседује да би био успешан у обављању својих дужности. На крају, образовање је већ крајње формалан вид унапређења познавања материје и укључује посебну стратегију, планирање процеса, евалуацију знања итд.

ISO стандарди посвећују посебну пажњу свести корисника. Тако се на пример у ISO 27002 наводи на страни 18[102]:

"Програм о подизању свести у погледу безбедности информација треба да тежи ка томе да запослени и, онда када то одговара, уговарачи буду свесни сопствене одговорности по безбедност информација и средстава којима се ове одговорности испуњавају."

8.3 Архитектура е-образовања

За сврху креирања одговарајућег специфичног безбедносног модела, важно је утврдити структуру процеса е-образовања, представити компоненте које чине архитектуру система, односно елементе који представљају реализацију архитектуре у пракси.

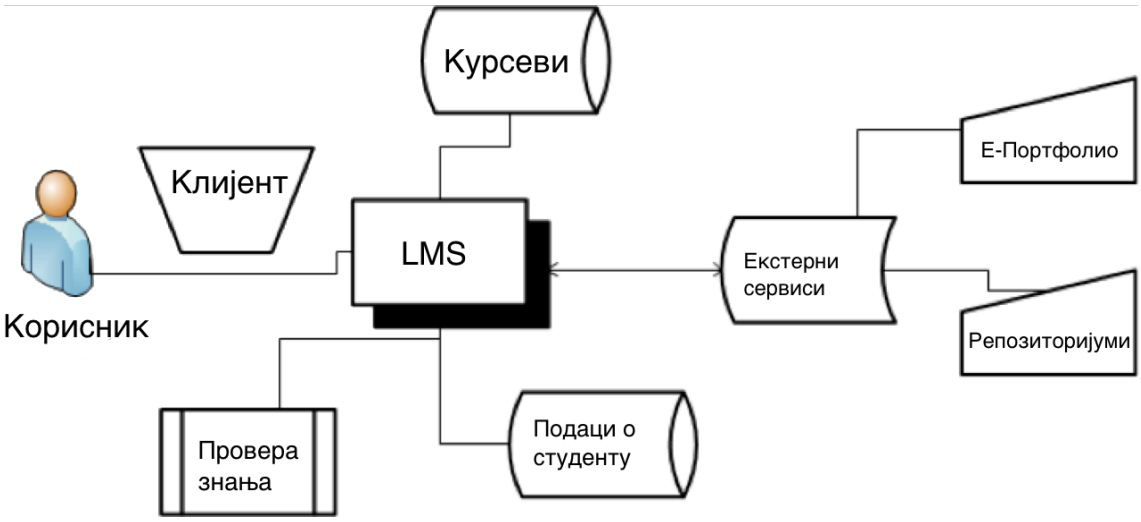
Архитектура система е-образовања стандардизовано је представљена кроз LTSA (Learning Technology System Architecture) [88]. Будући да је овај модел по природи генерички, дата су и пресликавања која одговарају различитим сценаријима, између осталог и веб-имплементација, која одговара е-образовању. Пример је приказан у поглављу 5.

Даље се овај модел може проширити дистрибуирањем библиотеке знања и других извора података. Наиме, институција под својим ингеренцијама одржава систем за управљање е-учењем у виду LMS платформе или портала, који може бити повезан са спољним изворима знања у виду репозиторијума. Репозиторијум према стандардизованом моделу представља складиште пакета (SCORM), који се добављају и презентују на основу својих метаподатака. Овај посао врши System Coach, који се реализује управо кроз одговарајуће модуле самог система за управљање е-учењем. Међутим, репозиторијум може бити и било који други извор података који је систематски подржан за потребе укључивања разноврсних фајлова, видео-материјала и других образовних ресурса. Према томе, сам Courseware Database се представља двојако: као систем за управљање учењем са садржајима и механизмима под контролом институције и као спољни извор, са којим је систем повезан (што подразумева интероперабилност). Такође, оставља се могућност двостране комуникације система са спољним изворима, нпр. у сврху извоза информација о ученику у спољне портфолио системе, који могу, али и не морају нужно бити под ингеренцијама институције. Такође, LMS може бити повезан и са другим LMS-овима, платформама за управљање е-портфолијом итф.

Модел LTSA не укључује експлицитно улоге корисника, већ у њему фигурише само ученик. За потребе изградње безбедносног модела, неопходно је дефинисати и друге улоге, осим ученика. У том смислу потребно је проширити интерпретацију модела LTSA додавањем улога других корисника који могу имати утицаја на сам систем. То могу бити администратори, наставници, модератори, родитељи.

Компонента за евалуацију такође изискује да буде издвојена као посебна.

На слици 19 приказан је уобичајени модел инфраструктуре е-образовања (адаптирано на основу [55]).



Слика 19 - Модел инфраструктуре е-образовања

Модел инфраструктуре представљен је кроз ентитете који фигуришу у процесу е-образовања.

8.3.1 Компоненте инфраструктуре

У овом моделу фигуришу три основне компоненте: хардверски, софтверски и комуникациони сегмент.

Хардверски сегмент представљају физичке компоненте које омогућавају одвијање онлајн активности и на којима се извршава софтверска компонента. Хардверски сегмент формира хардверску платформу, у оквиру које се налазе сервери, терминали, различити мултимедијални уређаји итд.

Софтверски сегмент означава различите програмске елементе: веб-сервер, сервер базе података и сл, који чине софтверску платформу и оријентисани су око система за управљање учењем.

Комуникациони сегмент обухвата опрему и пратеће протоколе намењене за размену података између ентитета.

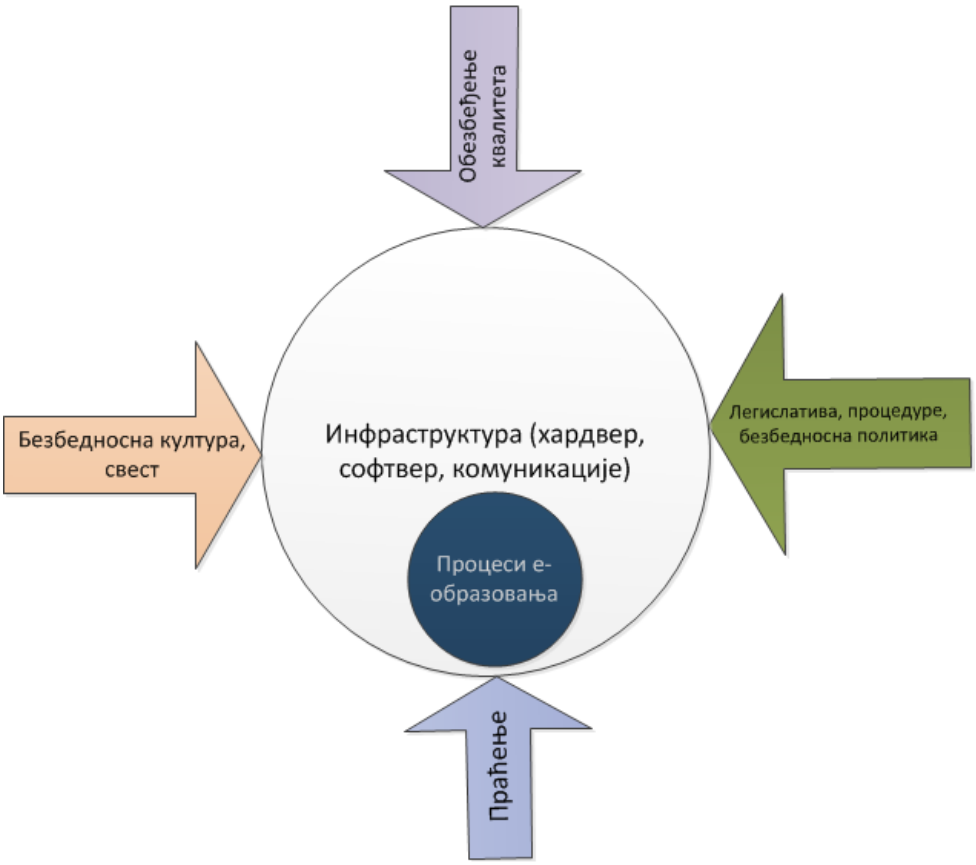
Инфраструктура, састављена од датих сегмената, пружа логистику за извршавање различитих процеса е-образовања: колаборације, провере знања итд.

Безбедност инфраструктуре односи се на безбедност свих елемената и њихове међусобне комуникације.

8.3.2 SeLMa модел безбедности у е-образовању

Архитектура представљена кроз LTSA је флексибилна, али и врло уска, у смислу да одражава искључиво процес учења. За изградњу холистичког модела, потребно је укључити читав екосистем у којем се е-учење одвија.

Узимајући у обзир специфичности е-образовања, студије случаја и постојеће приступе, формиран је следећи холистички модел, назван SeLMa (Security in E-Learning Model towards the quality Assurance) [109] (слика 20).



Слика 20 - Модел SeLMA

Инфраструктура подразумева све програмске и физичке елементе (хардвер и софтвер) који представљају логистику процеса е-образовања.

Процеси е-образовања су сви бизнис-процеси који се одвијају у склопу е-образовања: нпр. упис курса, постављање домаћег задатка, унос у вики-стране.

Безбедносна култура и свест (awareness) заузимају посебно место у моделу. Едукација, формирање свести о значају безбедности и безбедносној култури врши утицај на различитим нивоима безбедности: од физичког до логичког,

односно на све елементе безбедносне тријаде (CIA). Како је показано у студији случаја, постоји низ индикатора да је безбедносна свест код корисника (е-ученика) на незавидном нивоу, а такође су сами корисници установили потребу за сопственом едукацијом у овој области.

Обезбеђење квалитета може се посматрати као улазни, али и излазни процес. За систем чији се квалитет проверава морају се прво установити потребе квалитета, имплементирати тражени захтеви и стандарди, чиме само обезбеђење квалитета представља фактор улаза у процес изградње безбедносног модела и његове имплементације. По формирању окружења код којег су примењени критеријуми осигурања квалитета, врши се евалуација и у том случају је сам елемент е-образовања улаз у процесу евалуације.

Праћење подразумева константно прикупљање повратних информација, евидентирање активности и свих пропратних информација које могу бити од значаја за процесе унапређења постојећег модела. Праћењем се константно добијају информације на основу којих се предузимају одређене акције, односно које говоре о степену успешности тренутних контрола.

Легислатива и безбедносна политика представљају формалне факторе у чијим оквирима се рализују безбедносни циљеви. Законски оквири о очувању информација су дефинисани одговарајућим законским и подзаконским актима и било какав информациони систем, па и систем е-образовања мора бити усклађен са одговарајућим прописима. Процедуре представљају систематизовану формализацију интерних облика понашања. Нпр. процедура у случају компромитовања лозинке или проналажења вируса. Основни документ који фигурише је безбедносна политика, којом се разумљивим језиком дефинишу безбедносни циљеви. Безбедносна политика заправо је срж, доктрина око које се даље формирају остали елементи.

8.4 Изградња безбедносног модула PDCA методологијом

SeLMA је представљена статички са својим елементима. За спровођење циљева безбедности потребно је спровести динамичан процес, јер је према дефиницији безбедност контунуалан процес. Управљање ризицима представља језгро безбедносног модела било ког информационог система.

Водећи се методологијом ISO 27000 и пратећим PDCA циклусом, предвиђена је следећа структура активности:

Планирање (Plan): Дефинисати процесе који су од значаја за формирање модела безбедности е-образовања. Дефинисати циљеве заштите и заштитних механизама (контрола) узимајући у обзир циљеве система и захтеве квалитета

везане за безбедност. Извршити анализу ризика. Формирати модел. Формирати одговарајућу архитектуру. Одредити приоритете ризика и ингеренције самог модула унутар архитектуре, односно унутар система за е-учење.

Реализација/Имплементација (Do): Имплементирати изабране заштитне механизме. Потребно је превести архитектуру, односно њене делове у одговарајући модул, развити софтвер и имплементирати његове функције. Потребно је определити се за одговарајућу методологију развоја решења, која одговара намени.

Провера (Check): Извршити праћење рада модула, његов утицај на прихваћеност и поверење код корисника. Потребно је евидентирати и документовати евентуалне грешке (багове) и сакупити повратне информације од корисника.

Деловање (Act): Дефинисати корективне мере на основу повратних информација од корисника, односно од механизама за праћење рада модула, као и на основу процедура за евалуацију безбедности.

8.5 Планирање безбедносног модула

У фази планирања неопходно је :

- Идентификовати оквире система, релевантне процесе, добра (assets) и технологију
- Дефинисати политику безбедности информација
- Дефинисати приступ испитивању ризика
- Идентификовати ризике
- Анализирати и проценити ризике
- Идентификовати и проценити опције за третирање ризика
- Установити циљеве контрола и контроле за третирање ризика
- Набавити одобрење од стране менаџмента.

Анализа процеса

Е-учење је дистрибуирана мултидисциплинарна делатност. Самим тим постоји извесна сложеност у дефинисању домена и одређивању фактора када је реч о безбедности.

Специфичности управо диктирају дидактички захтеви који се постављају пред е-образовање.

- Доступност учења са било ког места. Тзв. свеприсутно учење (ubiquitous learning [110]) подразумева могућност приступа ресурсима за учење и учествовање у наставним активностима без обзира на место на којем се корисник (ученик) налази. Овај приступ подразумева да ученик може приступати са разичитих рачунара, таблета, паметних-телефона, из различитих мрежа. Овакав приступ даје широке могућности е-образовању, али са друге стране шири питање безбедности, будући да се смањује контрола над приступом ресурсима.
- Могућност колаборативног рада. Колаборација подразумева заједнички рад на одређеним активностима. На пример на вики странама. При томе може доћи до конкурентног рада, али и опасности од брисања туђег садржаја.
- Укључивање спољних садржаја преко програмских додатака. Прегршт технологија које проширују могућности стандардног веба могу обогатити искуство е-учења. Flash, Java и други видови активних садржаја обогаћују ресурсе интерактивношћу. Са друге стране, омогућавање додатака отвара нове потенцијалне рањивости у целокупном систему, повећавајући тзв. површину напада (attack surface)

Друге специфичности е-учења које захтевају посебну пажњу су:

- Електронска провера знања. Законска регулатива дефинише начине провере знања као писмени и усмени [111]. Такође, провера знања се подразумевано врши у самој институцији. Да би се електронски тест (е-тест) квалификовао као валидно средство провере знања, потребно је дефинисати начин е-тестирања, односно верификација регуларности процеса тестирања, што укључује проверу идентитета, онемогућавање коришћења недозвољених средстава, праћење итд.
- Додатна права приступа и надгледања активности ученика. Уколико је регулативама то предвиђено, одређеним лицима је потребно омогућити увид у активности ученик. На пример родитељ који жели да провери да ли и колико дете приступа лекцијама.
- Корисник који је има улогу наставника на једном курсу може бити ученик на другом. На пример, асистент има улогу наставника на курсу основних студија, а улогу ученика (студента) на курсу докторских студија.

Од посебног значаја је одредити сегменте модела који су под директном ингеренцијом установе и разликовати их од оних који су независни од установе, тј. нису под њеном контролом. С обзиром на захтеве флексибилности учења, мобилности корисника и независности од платформе, клијентски део модела, који подразумева корисника, његов клијентски софтвер и хардвер и начин

повезивања на Интернет, нису под ингеренцијама образовне установе, тј. установа не може стриктно прописати услове приступа и проверавати да ли корисник поштује те услове. Питање идентификације корисника такође је отворено.

Е-образовање, без обзира на своју институционализовану природу и формалне методе рада, не може бити изоловано, сведено на ограничен скуп ресурса и одвојено од других извора. Било да су у питању најједноставнији облици укључивања спољних садржаја као што су слике и видео, образовни ресурси у облику SCORM пакета из спољних репозиторијума, намеће се потреба за повезивањем окружења за е-учење са спољним ресурсима – који се налазе ван ингеренција установе. Овакав приступ повећава површину напада, отварајући нове могућности за нападаче, односно изискујући одговарајуће механизме за обезбеђење везе са сервисима, потврду кредибилности извора итд.

Корисници

Корисници приступају окружењу за е-учење користећи своју клијентску платформу. Сваки корисник се идентификује користећи одређен механизам и мапира у одређену категорију корисника, кроз аутентификацију и ауторизацију.

У е-образовању могу се дефинисати различите категорије корисника, са специфичним правима. Уобичајене основне класе корисника су: администратор, наставник, ученик и гост.

Права су дефинисана као уређени подскупови, што значи да су права категорија са мањим правима подскуп од права категорије са већим правима. Неопходно је да права буду прецизно дефинисана, из чега произилази да је пожељна њихова што ситнија гранулација.

Администратор је улога која подразумева максимална права на нивоу окружења за учење: по питању конфигурације самог окружења, садржаја и корисника.

Наставници имају права на курсевима на којим су надлежни. Права се односе на конфигурацију курса, креирање и постављање садржаја, управљање уписом на самом курсу.

Ученик има права на курсу на којем је уписан: право читања садржаја, учествовања у активностима, постављање одређених садржаја.

Гост има искључиво права читања на нивоу на којем има омогућен приступ. Нпр, уколико курс има опцију приступа за госте.

Обично се могу дефинисати и друге улоге, зависно од конкретног окружења. Такође, права појединих категорија корисника се могу подешавати на одређеном нивоу, поново зависно од окружења. На пример, ученик добија права уређивања (модерације) форума, што значи да поред својих ученичких права, добија и додатне опције - премештање тема, брисања порука итд.

Додела улога може бити вршена аутоматски или ручно, од стране надлежног лица (углавном такође корисника са улогом администратора). Аутоматски би додела била извршена на основу курикулума и података из студентске службе. Наставник који води дати предмет и студенти који су уписани на одговарајућу годину студија, добијају улоге на е-курсу датог предмета. У оптицају су и друге могућности, на пример самостални упис, коришћењем лозинке, затим упис од стране самог наставника итд. Опције исписивања ученика (студената) са курса такође су актуелне, нпр. у ситуацији када студент положи одговарајући испит, испише се са факултета, пређе на други студијски програм и сл.

Онемогућавање приступа кориснику и/или уклањање одговарајућег записа такође може бити потребно, у случајевима када корисник више није студент (дипломирао, исписао се), није више запослен у установи итд.

Корисници могу приступају окружењу са фактички свих врста платформи: рачунара, таблет рачунара, паметних телефона, са различитим оперативним системима и софтвером, са променљивих локација и користећи различите опције приступа интернету.

Подаци корисника

Сваки корисник поседује одређене личне податке, који чине његов профил. Поред статичких личних података (нпр. и-мејл адреса, број телефона), ученици могу имати и друге податке, од којих су неки динамични и прате њихово учење: на којим су курсевима уписани, резултате тестова, личне фајлове итд. Дакле, постоје подаци профила и подаци процеса учења. Такође, могу се пратити приступ и активности сваког корисника у окружењу.

Курсеви

Курсеви представљају склоп одређених садржаја и активности структурираних у једну целину. Курс се може састојати из разноврсних ресурса, који могу укључивати садржаје специфичне за саму платформу, односно стандардизоване пакете и друге спољне ресурсе. Садржаји који се користе у настави могу подлегати ауторским правима.

Екстерни сервиси подразумевају сервисе који нису интегрални део инфраструктуре за е-учење, тј. заснивају се на спољним инфраструктурама. То

могу бити спољне базе података, образовни репозиторијуми, видео-конференцијски системи итд.

LMS, односно окружење за е-учење је ентитет који повезује поменуте компоненте модела. Гледано према LTSA спецификацији окружење интегрише System Coach, али може бити и контејнер за друге елементе модела инфраструктуре, нпр. библиотеку знања. Окружење је реализовано у виду апликације којој се приступа са удаљених клијената. Окружење за учење представља виртуелни амбијент у којем се изводи процес учења/наставе и централну компоненту инфраструктуре. На нивоу окружења се могу контролисати многи параметри којима се профилише целокупан процес учења: дефинише облик курса и начини интеракције, групишу учесници и бирају алати за креирање и испоруку садржаја.

Физичка добра и физичка безбедност

Софтверске компоненте које чине окружење за е-учење имају подлогу у одговарајућем хардверу, који заузима одређен простор са одговарајућим правима приступа и физичке заштите.

Основни безбедносни циљеви

Сваки процес има одређене дефинисане циљеве који су приоритетни и условљавају правилно функционисање. Код е-образовања, на основу представљеног модела, могу се дефинисати следећи циљеви процеса, на основу којих се даље може креирати безбедносни модел:

- Континуитет процеса учења. Односи се на доступност ресурса свим легитимним корисницима који имају Интернет-конекцију.
- Омогућавање што ширег дијапазона комуникационих метода и облика учења.
- Праћење активности ученика и његовог напретка.
- Очување приватности личних информација у складу са важећим регулативама.
- Очување аутентичности и приватности информација о учењу, односно напретку.
- Спровођење провере знања онлајн.
- Очување ауторских права ресурса.

Полазећи од основних принципа безбедности: CIA, даље се могу ближе дефинисати циљеви безбедносног модела.

Поверљивост

Посматрајући модел е-образовања и његове циљеве, могу се дефинисати следећи циљеви везани за поверљивост:

- Ограничење приступа ресурсима курса. Само одобреним (аутентификованим и ауторизованим) корисницима може се дозволити приступ информацијама самог курса: материјалима, активностима итд.
- Ограничење приступа личним подацима. Приступ подацима ученика могућ је само према дефинисаним правима у одређеном контексту.
- Тајност података за пријаву, укључујући и средства за аутентификацију у било ком облику. Искључиво ауторизовани корисници могу учествовати у е-учењу обавезно под својим идентитетом.

Интегритет (целовитост)

- Право измене информација било ког облика имају једино ауторизовани корисници. То се односи на ресурсе за учење, личне податке, параметре самог окружења итд.
- Целовитост резултата и оцена је од критичног значаја.

Расположивост

- Подразумева доступност сервиса е-учења уз задовољавајуће перформансе. Перформансе могу зависити од безбедности, али су и питање планирања и оптимизације окружења, односно његове скалабилности.

Аутентификација и ауторизација

Основним принципима придружују се још неки, као што су аутентификација и ауторизација. Кроз процес аутентификације проверава се идентитет корисника, затим се ауторизује, тј. одобрава се (или не) приступ сервисима и одређује који облик приступа постоји. Аутентификација се може вршити на основу онога што корисника зна (нпр. лозинка), онога што има (идентификациона картица) или онога што јесте (биометријске методе: скен рожњаче, отиска прстију).

Е-учење је специфично по томе што ученик, као и члан било које друге категорије корисника, може бити лоциран на било ком месту, односно приступати са било које платформе. У том смислу, методе аутентификације које захтевају додатне инвестиције нису практичне. На пример, уколико се аутентификација заснива на биометријским информацијама, корисник може имати читач отиска на кућном рачунару, али онда остаје проблем аутентификације уколико жели да учи из Интернет-кафеа или са мобилног

уређаја. У том смеру постоје одређена решења која не захтевају посебан хардвер, већ се заснивају на снимку са веб-камере, које већина лаптопова данас има уграђене [112].

Оно што преостаје као опција се углавном своди на "стари добри" систем аутентификације коришћењем корисничког имена и лозинке.

Аутентификација може бити интегрисана са другим системима кроз примену јединственог приступа (SSO - Single Sign On): исти извор података користи се за аутентификацију за различите системе. То даље онда значи да политика лозинки може бити диктирана независно од самог окружења за е-учење. Иако се са једне стране препоручује SSO, а такве захтеве постављају и поједине шеме обезбеђења квалитета, постоје и анализе које показују лоше стране овог приступа [113].

Политика лозинки је један од битних елемената који се мора дефинисати и саставни је део безбедносне политике. Посебан је изазов дефинисати политику која ће са једне стране омогућавати коришћење јаких лозинки, а са друге стране бити поштована у смислу употребљивости, памтљивости, стратегија бележења и сл.

Осетљивост клијентског дела модела захтева посебан третман из поменутих разлога: неопходности што флексибилнијег приступа и немогућности контроле клијентске стране. На пример, корисник може приступати у незаштићеној отвореној бежичној мрежи, што је све чешћи случај и тада се његова рањивост рапидно повећава. Такође корисник може приступати са незаштићеног рачунара, који може потенцијално бити заражен, чиме се даље отвара могућност ширења малициозних програма кроз комуникацију преко окружења за е-учење. Аспекти клијентске безбедности биће посебно разматрани због наведених својстава.

Ауторизација подразумева доделу одређених права кориснику који је успешно аутентификован. Улоге је потребно дефинисати на нивоу курсева. Посматрајући предметни систем и модел е-учења, долази се до закључка да се основна ауторизација врши на нивоу курса. С обзиром да корисник добија одређену улогу у односу на курс, тек уписом курса, односно доделом улоге на одређеном курсу, корисник постаје ученик или наставник на њему. При томе један исти корисник може имати улогу наставника на једном курсу, а улогу ученика на другом.

У оквиру самог курса такође може постојати опција дефинисања права приступа над појединачним објектима који чине тај курс: ресурсима, активностима.

Поступак уписа на курс може бити аутоматизован и интегрисан са системима плаћања или дефинисан појединачним уписом од стране других корисника са одговарајућим правима.

Интероперабилност

Систем за е-образовање у ужем смислу (нпр. LMS) није изолована целина. Поред тога што је интегрисан у информациони систем установе, постоји и интероперабилност на нивоу других система, односно на нивоу наставних материјала. На пример. повезивање са спољним storage сервисима, као што је GoogleDrive. Или повезивање са е-портфолио системима, као што је Mahara или други систем итд. Парадигма е-учења уско је повезана са флексибилношћу и у том смислу потребно је омогућити проток података између два система, што доноси нове потенцијалне ризике.

По питању интероперабилности на нивоу садржаја, постоји пуно повезаности са интероперабилношћу на нивоу система. Поента је да је садржај учења стандардизован, тако да се може преузети са спољне локације и успешно (чак "on the fly") инкорпорирати у курс, односно лекцију. Са друге стране, учесници курсева могу да постављају своје материјале који су креирани на другом систему, односно у посебном софтверу.

Најпопуларнији формат, који интегрише различите друге стандарде је SCORM [114]. Јединице (лекције или делови лекције) које се израђују познате су као SCORM-пакети. У њима је садржано само "знање", али и метаподаци, који дефинишу понашање делића – објеката учења. Технолошки, SCORM је заснован на JavaScript-у и у том смислу постоје ризици везани за злоупотребу самог пакета.

Безбедност LMS-а

LMS је средишњи део инфраструктуре за е-учење и углавном је реализован у виду веб-апликације. Безбедност LMS-а може се анализирати са аспекта слојевитости која се подразумева код апликације овог типа, што подразумева безбедност на нивоу хардвера, софтвера, пратећих сервиса итд. Оваквих истраживања било је у више наврата и могу се погледати нпр. у [37]. Кроз модел ће посебно бити анализирани аспекти безбедности који се односе на специфичне процесе који су везани за е-учење, односно за које је емпиријски и теоријски утврђено да су од виталног значаја за унапређење квалитета е-учења. Питања безбедности на нижим нивоима биће апстрахована, јер су генеричка и студије везане за њих се могу преузети из других познатих модела.

8.5.1 Формирање безбедносног модела е-учења

У наставку ће на основу представљене архитектуре система е-образовања бити формиран безбедносни модел, на основу којег ће се у наставку пројектовати и реализовати безбедносни модул интегрисан у самом систему за е-учење.

Анализа концепта безбедности у е-учењу

Први корак је дефинисање добара (assets) система.

На основу специфичности процеса е-образовања, формиран је следећи модел безбедности, у којем су посебно приказани аспекти директно везани за безбедност специјалних процеса, док су остали аспекти безбедности енкапсулирани. Модел има за циљ да што комплетније представи различите елементе које чине безбедност у е-учењу. Представљен је мапом ума [115] - Слика 21.

Слика 21 - Безбедност у е-учењу - холистички приказ

Одређени елементи модела представљени су у претходним поглављима, на пример *Стандарди.*

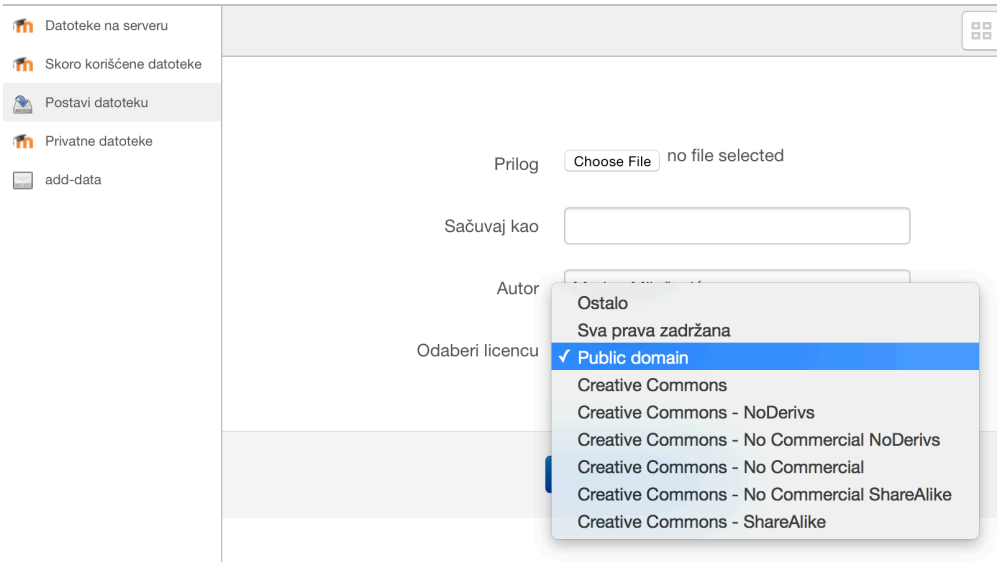
Безбедност клијентске стране

Природа е-образовања је таква да омогућава приступ ресурсима учења са било ког места у било које време. Бројни параметри који фигуришу у овом процесу стога су остављени произвољним и није могуће утицати на њих, за разлику од

других делатности. На пример, радник банке који долази на посао приступа затвореном интерном систему, који није доступан споља, идентификује се картицом и врши активности над апликацијом за банкарство: трансакције, плаћања, прегледе стања, штампање извода итд. Постоји прецизна интерна процедура приступа, чувања података, као и обавезни тренинг особља. Са друге стране, у е-образовању партиципира корисник са произвољне локације, потенцијално необезбеђене мреже и рачунара (или другог уређаја), без специјалне идентификације, без процедура и тренинга. Иако посао банкарског службеника може изгледати многоструко критичнији и значајнији од активности корисника окружења за учење, не треба занемарити специфичности е-ученика (и е-наставника), односно њиховог приступа и потенцијалних претњи које из њега могу проистећи.

Ауторска права и безбедност садржаја

Садржаји за учење доступни су у дигиталном облику, у одређеном формату: pdf, HTML, SCORM, flash итд. Сваки садржај би требало да поседује дефинисана права приступа, на основу којих се одређује да ли је и под којим условима могуће вршити измене, копирање и дистрибуцију. За ове потребе постоје дефинисане структуре на нивоу самог садржаја (уколико је у питању стандардизован пакет, као што је SCORM) или на нивоу самог окружења. На пример, код SCORM-а постоји метаструктура rights којом се дефинишу права коришћења садржаја. Код окружења за е-учење у питању може бити нпр. избор одговарајуће лиценце из листе предефинисаних вредности.



Слика 22 - Избор лиценце у Moodle систему

Слика 22 приказује начин дефинисања лиценце код система Moodle. Треба нагласити да су ова права видљива само другим корисницима са правом уређивања (фактички наставницима) и дефинишу да ли се и како тај фајл може користити.

Дефинисање права приступа и коришћења је један аспект везан за ауторска права и јасно одређивање правила коришћења образовног материјала је важан сегмент на путу заштите. Међутим, само означавање ни издалека није довољно. Неопходно је да корисници (ученици, наставници, инструкциони дизајнери, тутори...) буду упознати са значењем појединих облика лиценци и ауторских права и начином њихове примене и поштовања.

Нарушавање поверљивости садржаја за учење подразумева појаву неовлашћеног коришћења материјала, односно копирање и дистрибуцију противно дефинисаним правима коришћења. У ширем смислу, пошто садржаји учења не представљају само статичке материјале у смислу који је близак традиционалном појмању ”материјала”, већ и садржаји настали колаборацијом (форумски постови, чет, вики-стране), треба узети у обзир и ову врсту садржаја.

Приватност и анонимност

Приватност је поверљивост личних података, односно могућност појединца да контролише степен видљивости својих података. Анонимност је могућност појединца да сакрије свој идентитет. Обе ставке се могу разматрати у е-образовању.

Међутим, у процесима е-образовања није једноставно одржати анонимност корисника, због потребе за праћењем активности, оцењивања и осталих формалних процедура које прате образовни процес. Ипак, постоје одређени напори уложени у том смеру [116]. Остаје закључак да се анонимност може остварити у неформалним, неинституционализованим облицима учења, док у е-образовању као формално дефинисаном облику то није случај.

Одржавање приватности такође може бити супротстављено одређеним циљевима образовања, али се може реализовати уз мање тешкоћа него анонимност. Штавише, различити контексти у којима се образовни процес одвија захтевају контролу личних информација. На пример, ученик би желео да његову мејл-адресу виде сви који су уписани на исте курсеве, али не и остали корисници.

Безбедност при провери знања

Провера знања у системима е-образовања ”под лупом” је критичара. Када је реч о провери знања, акценат је на тестовима знања. Међутим, провера и оцењивање могу се вршити и путем других активности: есеја, пројекта итд. Сви ови облици могу бити критички посматрани са аспекта специфичности извођења у окружењу електронског образовања, али ће у наставку највише пажње бити посвећено управо тестовима.

Удаљена провера знања представља изазов превасходно због тога што је компликовано утврдити идентитет испитаника који ради тест од куће, али и спречити друге видове варања на тесту. Веома детаљан преглед изазова дат је у литератури, нпр. [117] и [118]. Углавном се технике установљавања идентитета своде на непосредно снимање и надзор (веб-камером) и биометријске методе (препознавање лица, пријава скеном отиска прста). Треба нагласити да све ове методе захтевају значајна средства, а поставља се и питање до које границе је нарушена приватност корисника.

8.5.2 Безбедносна политика

Важно је да безбедносна политика буде установљена и добро документована [119], али и што боље раширена међу корисницима. Како је установљено у поглављу са студијом случаја, најчешће уопште не постоји безбедносна политика, нити као посебан документ, нити као део политике коришћења сајта на пример.

Како сугерише ISO 27002, политика треба да буде дефинисана на нивоу институције, а онда следе политике на нижим нивоима, којима се детаљније дефинишу потребе и отвара простор за успостављање одговарајућих контрола.

Посебан скуп регулатива односи се на политику крајњег корисника [102]. У стандарду се наводи (стр. 9):

> *”Ове политике треба да буду саопштене запосленима и одговарајућим екстерним странама у облику који је одговарајући, прихватљив и разумљив читаоцу, нпр. у контексту „упознавања са безбедношћу информација, програма образовања и обуке””*

У раду је превасходно реч о политици која се односи на коришћење система за е-учење. У питању је документ који треба да буде састављен на основу захтева специфичног система, какав је нпр. информациони систем за учење или чак сам LMS, односно на основу различитих важећих регулатива.

За систем који је креиран у овом раду формирана је посебна политика коришћења у којој кључно место заузимају управо питања безбедности. Политика је креирана на основу више познатих примера добре праксе, као што је политика универзитета Принстон [120], односно [121] и на основу примера из литературе, као што је [122], формулисана је политика за крајњег корисника. Корисник система обавезан је да прихвати ову декларацију, да би уопште користио систем.

Целокупан текст политике дат је као прилог (13.1).

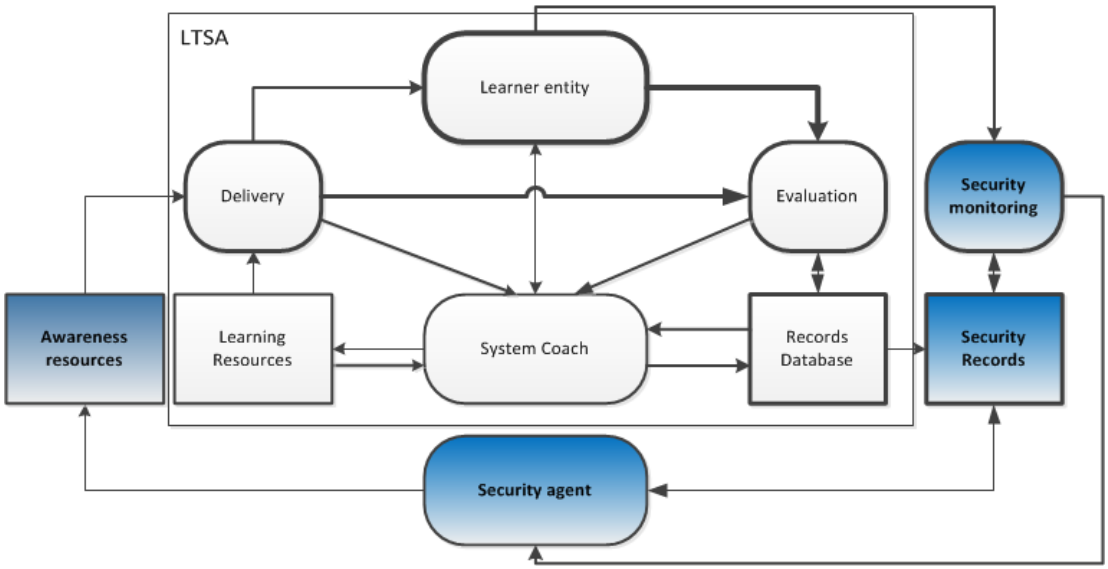
8.5.3 seLTSA - Надградња стандардне архитектуре

Претходним анализама добијене су потребне информације помоћу којих је могуће успоставити одговарајућу архитектуру.

Модел корисника је фактички само један "плагин" безбедносне архитектуре, односно одговарајућег модула. У стандарду IEEE1484 је са намером формулисана LTSA архитектура као крајње генеричка, са високим степеном флексибилности и могућности за надоградњу, адаптацију и пресликавање у различите сценарије.

У том смислу, формулисана је и адаптирана верзија архитектуре, названа seLTSA (Security Enhanced LTSA), која за задатак има побољшање безбедносне свести корисника кроз интеграцију механизама за заштиту, дисеминацију безбедносне политике у самом окружењу за е-учење и управљање другим аспектима безбедности.

Основна идеја је додати слој на основну генеричку архитектуру, тако да се омогући интегрисан приступ безбедности (слика 23). Ова надградња је у ствари безбедносни модул. Модул је назван **eLearnion** [123].



Слика 23 - seLTSA архитектура

8.5.4 Елементи модула eLearnion

Разликују се следећи елементи проширене архитектуре:

- Праћење (security monitoring) подразумева процес прикупљања и анализе података о активностима корисника
- Безбедносни записи (security records) означавају скуп прикупљених података који се бележе за потребе аудита. Ови записи могу се заснивати на конвенционалним записима који се иначе бележе, с тим да се они на одређени начин издвоје и припреме за интерпретацију, али такође и на специфичним записима, који се бележе искључиво за потребе самог агента.
- Безбедносни агент (security agent) је елемент који се реализује у виду софтверског агента и има задатак да на основу прикупљених информација на одговарајући начин ангажује ресурсе из наредног елемента (awareness resources), односно ажурира податке о самом кориснику уколико су испуњени услови за то.
- Ресурси (awareness resources) су различите врсте садржаја које агент ангажује и прослеђује стандардном Delivery модулу. Овај садржај треба да утиче на корисникову свест о безбедности. Који садржај ће се и на који начин пласирати, одређује агент на основу излаза претходних елемената. Превасходно је реч о садржајима који проистичу из политике коришћења сајта: било да су у питању непосредно репродуковани делови, било да је реч о детаљима којима се разрађује неки елемент политике.

eLearnion је тесно повезан са образовним моделом, јер је један од његових основних задатака управо рад на унапређењу свести корисника о безбедности, за шта је кључ едукација.

8.5.5 Безбедносна архитектура и анализа ризика

Безбедносна архитектура, надграђена на стандардни LTSA модел архитектуре, има као витални део *безбедносног агента.* Агент функционише на основу одређених података, а превасходно на основу корисниковог безбедносног профила. Безбедносни профил се, са друге стране ажурира на основу информација које су прикупљене праћењем активности корисника. Поставља се питање које су то информације које треба пратити да би овај читав систем функционисао.

Одговор се крије у анализи ризика. Потребно је у домену холистичког модела извршити анализу ризика и класификовати оне ризике у које је директно умешан сам корисник, односно који су повезани са његовом свешћу о безбедности (security awareness). На тај начин може се доћи до оних ризика код којих сам агент може играти улогу, односно којима се може управљати преко утицаја на самог корисника, тј. његову свест о безбедности. Безбедност информација је слојевита и не постоји дисјунктна подела на ризике који ће бити обрађени на један или други начин. Унапређење корисникове културе задатак је којим се могу обрадити многи ризици, али ти ризици имају и друге контроле којима се врши управљање. На пример, кориснику се напомиње да не чува своје податке за пријаву у веб-читачу на јавном рачунару. Међутим, додатно, после одређеног броја пријава, може се активирати двофазна аутентификација (нпр. шаље се код на мобилни, који се мора унети у логин-форму).

Анализа ризика

У наставку биће представљени одговарајући записи: претње и ризици, као и то да ли је могуће реализовати заштитни механизам путем представљеног безбедносног агента и како се то предвиђа.

Претња	Ризик	Заштитни механизам
Корисник поставља заражен фајл	Други корисници преузимају фајл и заражавају своје рачунаре. Интегритет система је нарушен, појављују се рекламе итд.	Корисник се обавештава о ризику, безбедносни капацитет опада, администратор добија додатне информације
Корисникови подаци о пријави су	Нападач се лажно представља, поставља садржаје у име	Корисник и администратор су обавештени, понуђене су

Претња	Ризик	Заштитни механизам
изгубили тајност. (Нпр. корисник је одао податке, оставио их убележене у веб-читачу и сл.)	оригиналног корисника	опције за повратак података; презентују се информације о управљању налогом
Корисник шаље велики број приватних порука	Други корисници добијају спам	Корисник је информисан о безбедносној политици, смањен је безбедносни капацитет и проверава се корисников ниво свести о безбедности - на основу чега се евентуално врши рестрикција права приступа
Приступ подацима профила није контролисан	Корисник добија нежељену пошту или чак бива узнемираван на друге начине (скајп, телефон)	Корисник може да самостално дефинише ниво приватности. Додатно је информисан о начинима да управља приватношћу.
Корисник има проблеме са пријавом	Сервис е-учења није доступан	Корисник се упућује на стратегије креирања лозинке, смањује се вредност loginadmin, на основу које систем презентује одговарајуће информације
Корисник се не одјављује са система	Долази до неауторизованог приступа других особа	Кориснику се смањује вредност логинадмин, на основу које се презентују одговарајуће информације о безбедносној култури. Корисник добија посебне савете о потреби одјаве.
Искоришћена слабост софтвера	Појављују се симптоми малвера, нпр. рекламе.	Корисник има једноставан механизам за пријаву проблема.

8.5.6 Праћење безбедносних информација

Праћење (мониторинг) рада било ког система од кључног је значаја за добијање информација о његовом функционисању ради детекције евентуалних проблема и предузимања одговарајућих акција у сврху корекције елемената система.

Праћење се врши у реалном времену или у приближно реалном времену. Изводи се прикупљање разноврсних података: од параметара хардвера, података о стању мреже, до различитих сервиса и апликација.

Без одговарајућих механизама за праћење практично је немогуће доћи до података за евентуалну форензичку анализу, пост-мортем решавање проблема везаних за упаде и детекцију неовлашћених приступа и упада у реалном времену. У том смислу потребно је:

- прикупити што више информација од различитих уређаја, сервиса и апликација у маниру што приближнијем реалном времену
- безбедно добавити и чувати записе у што дужем временском интервалу
- редовно спроводити скенирање рањивости рачунара и уређаја и вршити корелацију рањивости са упозорењима и другим догађајима од интереса у циљу смањења лажних упозорења.

О системима за детекцију упада и посебним апликацијама које на нижим нивоима прикупљају и анализирају дневнике догађаја различитих сервиса, више се може сазнати у специјализованој литератури [124]–[126].

8.5.7 Праћење безбедносних информација у е-учењу

Информације од значаја за безбедност могу се прикупити на различитим нивоима инфраструктуре: од мреже до апликације. Синтезом информација из више извора и њиховом корелацијом могу се добити конкретнији закључци о томе шта се догађа у инфраструктури. О месту праћења у безбедносној архитектури, аутор је дискутовао у [127].

У ужем смислу, информације се добијају од саме апликације, тј. платформе за учење, у конкретном случају од LMS-а. Сваки LMS поседује механизме за праћење догађаја који су везани за кориснике и модуле самог окружења. Овакви елементи су корисни за добијање информација о академском ангажовању студената на пример, добијању података за аналитику учења, али могу бити од значајне помоћ и код превенције и отклањања проблема везаних за безбедност. Уколико сами механизми за праћење нису планирани за прикупљање довољно детаљних информација, постоји могућност да се прикупљање унапреди, тако да обухвати оно што је потребно.

9. Развој и имплементација модула eLearnion

У претходним поглављима дат је приказ безбедносних изазова у електронском образовању. Анализирани су закључци истраживања која су обрађивала ову област, са посебним осврtом на изузетно важну карику, а то је корисник. У склопу прве фазе PDCA циклуса креиран је модел којим се надграђује стандардизована LTSA архитектура са основним циљем праћења корисника и унапређења његове безбедносне културе. Кључна улога у моделу припада агенту, ентитету који оркестрира читав процес: анализира акције корисника, ажурира профил, презентује одговарајуће информације кориснику итд.

Планирано је да се модул имплементира у Moodle систему за управљање учењем [97] и овај сегмент представлља **D** фазу пројектовања. Систем Moodle изабран је из следећих разлога:

- Отвореног је кода, што омогућава измену постојећих функционалности и прилагођавање.
- Модуларан је, што омогућава релативно једноставно додавање функционалности у виду ”плагинова”.
- Изузетно је популаран, што даље повлачи постојање бројне заједнице која се може консултовати, односно која ради на усавршавању кода, проналажењу багова итд.
- На Факултету техничких наука у Чачку Moodle се користи већ више од 8 година, што олакшава евалуацију и омогућава поређење система са безбедносним модулом и варијантом без модула. Такође, ауторово богато искуство као администратора и корисника система у улогама наставника/ученика показало се као драгоцено за развој.

У наставку ће бити дат опис основних могућности које пружа Moodle, након чега следе детаљи витални за имплементацију модула.

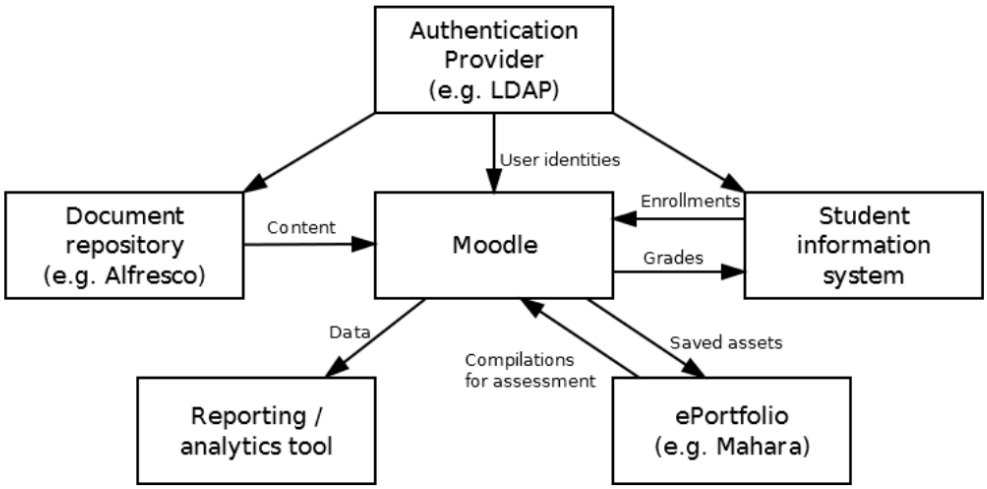
9.1 Moodle као окружење за интеграцију

Moodle је настао као део истраживања Мартина Дугијамаса (Martin Dougiamas) са основом идејом креирања окружења за учење које је флексибилно и засновано на конструктивистичким теоријама. Акроним Moodle настао је од речи Modular Object Oriented Dynamic Learning Environment, чиме се управо наглашавају ове идеје.

Специфичност Moodle-а и најзначајнији разлог за његову популарност, је у томе што је интерфејс врло интуитиван и садржаји се креирају и презентују у истом приказу: није потребно посетити посебан део апликације да би се креирао и

поставио неки садржај, већ је приступ из угла креатора и из угла корисника садржаја идентичан.

Moodle се може користити потпуно засебно, као апликација која у свом склопу садржи све што је потребно за рад: податке о корисницима, фајлове, резултате итд. У комплекснијим и добро организованим интегрисаним окружењима, Moodle је ”само” део већег система (слика 24).



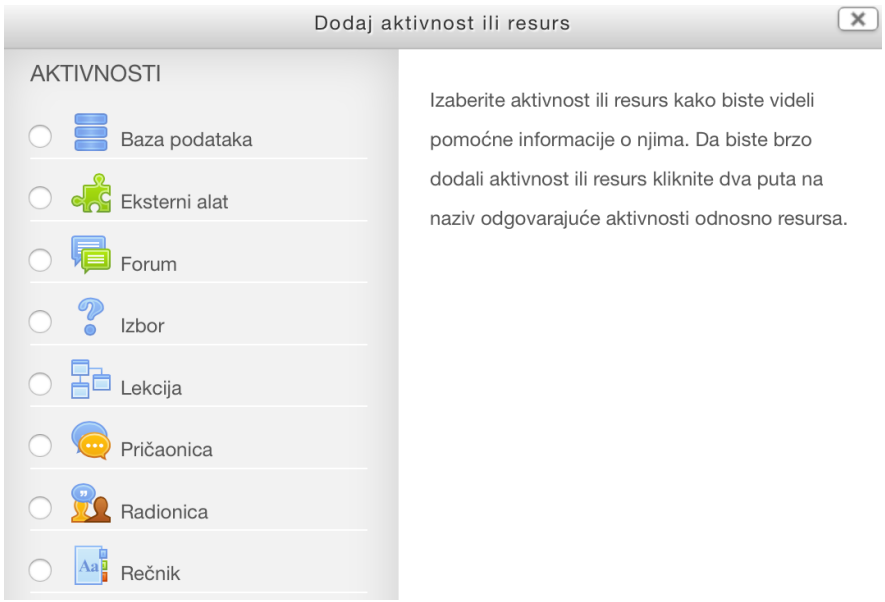
Слика 24 - Moodle у типичној сложеној универзитетској архитектури - према [128]

У оваквој архитектури Moodle има улогу окружења за е-учење у ужем смислу, јер се многи задаци делегирају другим системима:

- Провајдер аутентификације може бити већ постојећи систем (неки облик LDAP-а, у склопу Active Directory-ја нпр.). У Moodle-у је подешено да се провера идентитета врши коришћењем екстерних извора података, уместо интерне базе.
- Студентски информациони систем (нпр. ИС студентске службе). Омогућава хармонизацију рада самог окружења за е-учење омогућавајући упис на одређене курсеве и достављајући основне информације о студентовом статусу.
- еПортфилио систем је извор информација о учинку, студентовом CV-у и агрегатор његових укупних постигнућа.
- Репозиторијум докумената служи за чување фајлова и праћење активности на креирању фајлова.
- Алати за анализу и извештавање пружају могућност генерисања прегледа дешавања на институцији у глобалу.

Основна јединица организације наставе у Moodle-у је курс. На располагању је више начина за организацију садржаја унутар самог курса (седмични, тематски итд.). Основни градивни елементи курса су активности и ресурси (слика 25). Ово је Moodle терминологија и њоме се наглашава разлика између динамичке и статичке природе садржаја који чине један курс. Тако у активности спадају динамички садржаји, као што су тестови, форуми, упитници и лекције, што значи садржаји који захтевају активно учешће крајњих корисника (ученика), док у ресурсе спадају статички садржаји, који су ”сервирани” и могу се само конзумирати: фајлови, линкови, IMS пакети и тако даље.

Поред ових наведених елемената, курс се може уобличити и коришћењем блокова: то су елементи за приказ и контролу различитих информација у оквиру самог курса, постављањем елемента приказа са стране основног садржаја - у виду блока. Блокови садрже углавном мању количину информација, у складу са тим да је њихов наставни значај незнатан у односу на основне садржаје курса и да често имају административну улогу. На пример, од наставног значаја може бити блок са RSS вестима са удаљеног сајта, док административну улогу може имати блок ”HTML” или ”Поруке”. Администратор може дефинисати који су блокови доступни, као и ко може управљати њима, нпр. да ли ученик може да искључи блок.

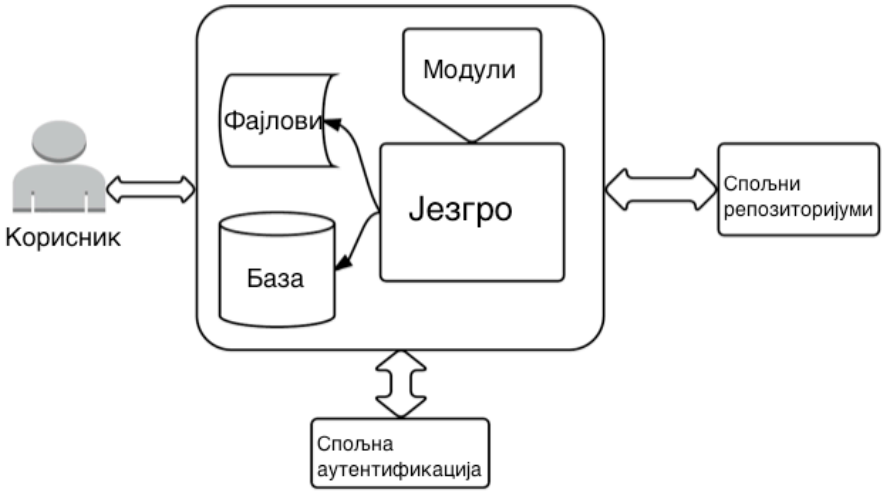


Слика 25 - Додавање градивних елемената курса

9.1.1 Moodle архитектура

Moodle LMS је у својој основи класична веб-апликација са тро-нивоском (3 tier) архитектуром, што значи да има одвојене нивое презентације, апликационе логике и базе података. Слој презентације реализован је са HTML/JavaScript-ом, логика је реализована у PHP-у, док је избор конкретног система за управљање базама података веома флексибилан. Подржане су бројне базе. Најчешће су у употреби MySQL/MariaDB, али је могуће користити и Oracle, MS SQL и PostgreSQL. Оваква флексибилност омогућена ја захваљујући апстракцији приступа бази кроз веома опсежан API, чиме је питање која је база иза Moodle-а углавном транспарентно за програмера, тј. програмер махом не користи никакве команде које су специфичне за конкретну базу, већ јој се обраћа преко Moodle-овог API-а.

Moodle је модуларан (слово ”M” у акрониму је управо од речи ”модуларан”). Модули омогућавају додавање различитих функционалности основној варијанти система. Одређени модули су присутни у изворној инсталацији и потребно их је укључити и конфигурисати, док је веома велики број модула доступан за преузимање из званичног репозиторијума са moodle.org. На слици 26 приказана је архитектура Moodle LMS-а.



Слика 26 - Moodle архитектура

У средишту система је језгро. Језгро садржи кључне елементе око којих су изграђене све остале функционалности, на пример библиотеке функција за графички приказ, рад са базом, управљање догађајима итд. Измене језгра су координисане од стране Moodle развојног тима. Било какве самосталне измене

даље могу довести до проблема са ажурирањем система новим верзијама, јер се при свакој надградњи мења и језгро. Са друге стране, уколико се жели извршити промена језгра ради добијања неке специфичне функционалности, потребно је дати кôд изоловати и задржати промене и након надградње. Наравно, и у том случају остаје питање компатибилности надграђених елемената језгра и тог, измењеног дела.

Широк спектар функционалности може бити реализован кроз модуле, који се у терминологији Moodle-а називају и плагинови (plugins). Комплетна листа доступних врста модула дата је на званичном сајту [129]. Као што је поменуто, одређени плагинови су већ део језгра, док остали могу да се накнадно додају. Поједини плагинови који се покажу као веома корисни, временом могу постати део језгра и тада се испоручују са основном инсталацијом. Следе неки од најважнијих модула.

- Активности. Активности представљају елементе којима се реализују динамички сегменти наставе. На пример: тест, форум, предаја фајла,вики-страна итд. У основној инсталацији доступно је 13 активности (верзија 2.9), док је могуће додати произвољан број плагинова којима се проширује број доступних активности. На пример, уколико је потребна интеграција Moodle-а и система видео-конференције (као што су Adobe Connect или BigBlue Button), на располагању су плагинови којима се то омогућава: реализацијом јединствене пријаве (single sign-on), дефинисањем параметара видеоконференције (трајање, право приступа, тип) унутар самог Moodle-а итд. На развоју оваквих плагинова углавном раде управо програмери из фирми чији се производи интегришу. Активности су лоциране у *mod* или ређе *local* подфолдеру.

- Плагинови за аутентификацију. У подразумеваној варијанти Moodle подржава различите начине аутентификације, укључујући интерну (корисници се чувају у Moodle бази) и екстерне облике. Могуће је и умрежавати више Moodle инстанци кроз јединствену аутентификацију.

- Типови питања. Тест (изворно - квиз) је један од најсложенијих модула Moodle-а. Подржани су сви конвенционални типови задатака (питања). Међутим, могуће је додавати и нове типове помоћу одговарајућих плагинова.

- Теме. Подразумевају предефинисан изглед система и приказа његових елемената. Иницијална инсталација садржи пар основних тема, док је за преузимање и инсталацију доступан широк избор на званичном сајту.

- Блокови. Веома популарна врста плагина. Често долази у пару са одређеним плагином, допуњавајући његове функционалности. Блокови су лоцирани у blocks подфолдеру.

Са стране организације саме апликације, плагинови су класификовани према фолдерима у којима се налазе и њихово име (које се појављује у коду) реферише се према такозваној ”франкенстајл” конвенцији, што значи да се назив плагина добија комбинацијом типа и локације - имена фолдера (Табела 7).

Табела 7 - Конвенција именовања Moodle плагинова

Тип плагина	Назив	Франкенстајл	Фолдер
активност (mod)	форум	mod_forum	/mod/forum
активност (mod)	квиз (тест)	mod_quiz	/mod/quiz
блок	навигација	block_navigation	/blocks/navigation
тип питања	кратак одговор	qtype_shortanswer	/question/type/shortanswer

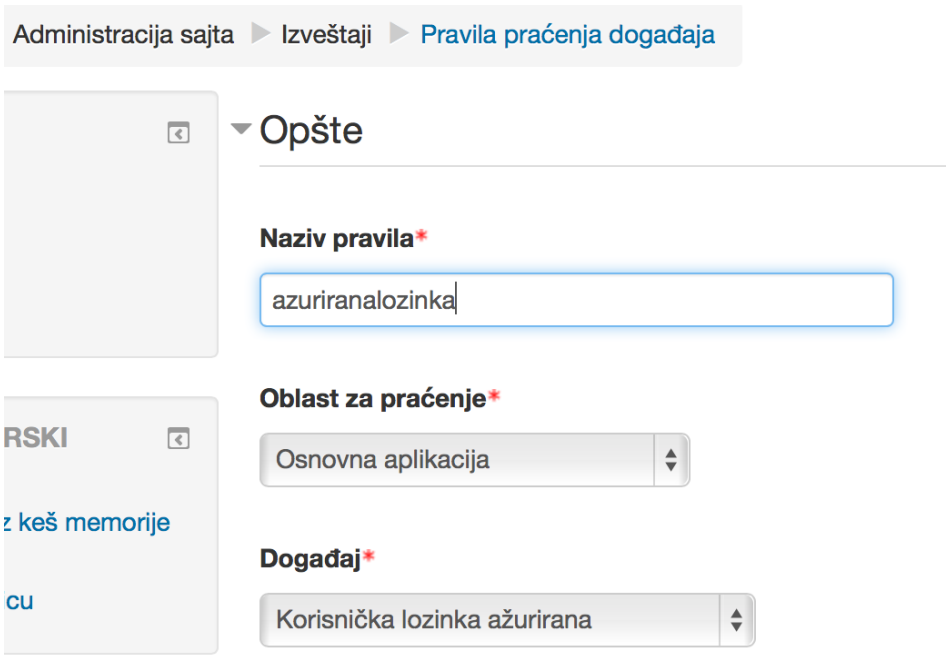
Као што се види из примера, активности су подразумевано инсталиране у /mod фолдеру, дакле у првом нивоу подфолдера апликације. Назив фолдера (мод) јесте скраћеница од ”модул”, која је преостала из првобитних верзија Moodle-а, када је активност управо и била једини вид модула.

Такође, активности су специфичне и по томе што омогућавају креирање суб-плагинова. У примеру из табеле тип-питања је субплагин самог плагина питања.

9.1.2 Догађаји у Moodle-у

LMS Moodle је у последњих неколико година постао изузетно комплексан софтвер са подршком за интеграцију са бројним системима, а верзија 2.9 ”тешка” је преко 100 мегабајта. Због саме комплексности и флексибилности, у верзијама од 2.7 уведен је механизам догађаја (events). Догађаји су појаве које садрже одређене информације о различитим активностима. На пример, написана порука на форуму, креирање новог корисника, детекција малициозног софтвера итд. Механизмом догађаја преносе се информације између различитих делова система, кроз модел произвођач/претплатник

(producer/subscriber)[1]. Догађаји су дефинисани као издвојени елементи који се затим активирају у одређеним сегментима апликације, а затим се врши позивање функција (хендлера) које су претплаћене на догађаје. Овакав приступ омогућава веома једноставно асинхроно повезивање модула са језгром и претплату на постојеће догађаје, као и креирање нових догађаја. У новијим верзијама (2.7+) администратор може да се претплати на било који догађај и добије обавештења уколико се појави чешће од задатог броја пута (слика 27).



Слика 27 - Претплата на догађаје у Moodle-у

При окидању догађаја, позивају се све функције које су претплаћене на њега. Такође, у дневник догађаја се уписују детаљи о томе која компонента је окинула догађај, као и основне информације о догађају. Претплата на догађаје може се вршити из самог кода - на пример из кода плагина.

9.2 Преглед основних безбедносних механизама у Moodle-у

Moodle је комплексан LMS и може се класификовати као својеврстан информациони систем. За заштиту информационог система потребно је анализирати слојеве који фигуришу у раду самог система: од хардвера до саме софтверске платформе, како је напоменуто у поглављима која се баве моделом

[1] Уместо термина претплатник (subscriber), у употреби је и израз потрошач (consumer).

и холистичким приступом. У наставку ће бити представљени механизми који су имплементирани у самом Moodle-у и са којима се сусрећу крајњи корисници и администратори. Овај аспект је важан због деловања самог модула, који је повезан са постојећим механизмима и има за циљ да олакша њихово коришћење, али и да по потреби интерагује са њима.

Анализе безбедносних механизама и саме проблематике заштите Moodle LMS-а могу се наћи у литератури [130], [131], а у наставку су наведени неки од основних облика заштите на нивоу самог система за управљање е-учењем.

9.2.1 Регистрација и пријава на систем

Moodle подржава изузетно широк спектар начина аутентификације: од IMAP-а до Radius-а и ови начини су такође модуларни: могуће је додавати модуле и накнадно, у виду плагина. Најједноставнији начин регистрације, уколико не постоји или није потребна интеграција са спољном базом је - саморегистрација заснована на електронској пошти. Тако је организована регистрација и на самом сајту moodle.org. Корисник самостално попуњава податке профила и потврђује регистрацију путем електронске поште. Овај приступ олакшава посао администратору (за разлику од ”ручног уноса”, на пример, где све уноси администратор), али постоји проблем контроле ко се региструје. Поред тога, да се не би регистровали ботови, тј. да скриптови не би аутоматски креирали спамерске налоге, обавезно треба користити CAPTCHA заштиту. За ове потребе неопходно је креирати налог на бесплатном Google-овом сервису под именом Recaptcha (https://www.google.com/recaptcha/intro/index.html) и одговарајуће кључеве унети у Moodle конфигурацију.

За потребе безбедносног модула, инсталиран је плагин A2FA [132] којим се омогућава 2-делна (2-факторска) аутентификација. Овакав вид аутентификације подразумева да се поред стандардног пара корисничко име/лозинка, систему достави и једна додатна информација, привремено генерисани токен који корисник добија путем мобилног уређаја (телефон, таблет), а на основу посебног тајног броја, који је убележен у његовом профилу. На тај начин се евентуално ”цурење”, тј. нарушавање поверљивости лозинке, може ”поправити” коришћењем додатне информације, коју потенцијални нападач не може имати, тј. која потиче из онога што корисник ”има”. Неопходно је да администратор подеси датом кориснику A2FA проверу идентитета, креира му тајну (secret) и достави је кориснику. Од тог тренутка, корисник се пријављује преко посебне адресе. За потребе безбедносног модула унете су одређене модификације модула, о чему ће бити речи касније.

Посебно треба поменути опције јединствене пријаве, тзв. SSO - Single Sign On. У појединим шемама квалитета овај начин пријаве се декларише као обавезан.

Подразумева јединствену пријаву за низ сервиса на којим корисник треба да има налог. Овакав облик аутентификације је могућ са различитим модулима, на пример CAS или Shibboleth. Такође, могућност јединствене пријаве коришћењем google налога могућа је уз применом OAuth протокола [133], а путем одговарајућих додатних модула, као што је googleoauth[2] плагин. Упркос бенефицијама јединствене пријаве, треба напоменути и да је то ”мач са две оштрице” [134].

Низ поставки везаних за безбедност налази се у посебном администраторском подменију ”Безбедност”, а највећи број је под опцијом ”Правила о коришћењу сајта” (Site Policy).

У старијим верзијама софтвера, омогућено је да се корисник пријави са истим налогом са више рачунара. У верзији 2.9 могуће је ограничити број истовремених пријава. Што се тиче неуспешних пријава, односно евентуалног брут-форс напада на страну за пријављивање, корисник може бити блокиран на нивоу веб-читача (што се лако елиминише брисањем колачића) и на нивоу самог сервера. Такође, администратор добија обавештење о неуспешним покушајима пријаве.

Треба нагласити и то да је већина поставки администраторског типа, па самим тим и оних које се тичу безбедности, сачувана у табели са конфигурацијом система (mdl_config) и да су у коду доступне преко глобалне променљиве $CFG.

На нивоу самог система Moodle, на располагању је и ”примитиван заштитни зид” (фајервол). Функционише тако што се у једно поље уносе IP адресе које је потребно блокирати и онда је приступ са тих адреса онемогућен. Проблем је у томе што је неопходно да се овим уносима управља ручно, тј. администратор мора да уноси и брише адресе.

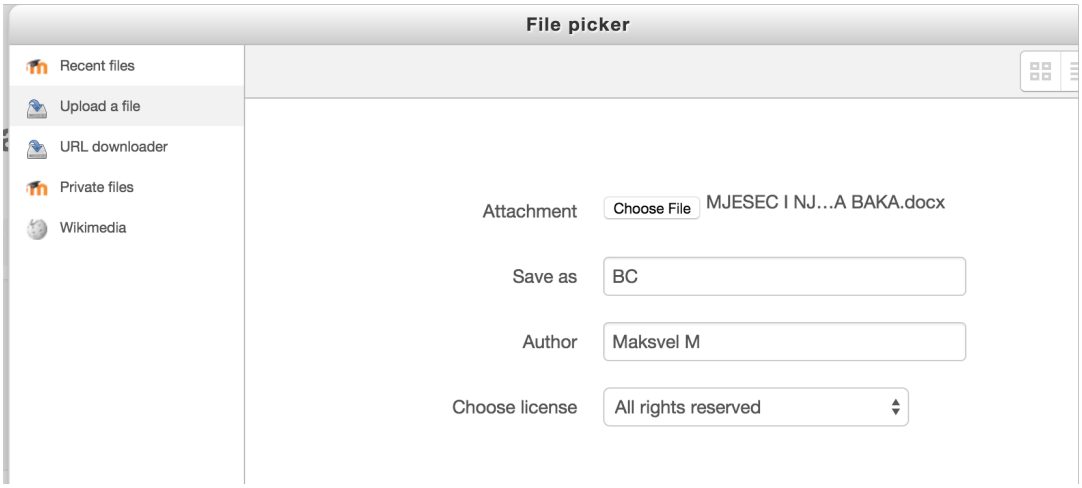
За преглед фајлова послатих на сајт на располагању је антивирус. Тренутно је могуће користити само ClamAV[3]. Ово антивирусно решење је отвореног кода и, осим изворне варијанте за оперативни систем Linux, доступне су верзије за Windows, Solaris, BSD, као и специјализоване верзије за заштиту различитих мејл-сервера, веб-сервера итд. Верзија за MacOS није бесплатна.

Корисник има на располагању различите видове постављања фајлова. Свакако, наставник има већи број доступних опција, с обзиром на то да има привилегије постављања наставног материјала. Ученик (студент) поставља фајл у следећим сценаријима:

[2] https://moodle.org/plugins/view/auth_googleoauth2
[3] http://www.clamav.net

- Фајл је захтеван као задатак (активности - задатак-постављање фајла, радионица).
- Фајл је прилог поруке на форуму (подесиво на нивоу поставки форума или чак на нивоу сајта)
- Фајл се поставља на профилу - слика корисника поставља се као фајл.
- Фајл се поставља као ”приватан фајл”. Сваки корисник подразумевано има на располагању одређен простор који може користити за сопствене фајлове.
- Додатни модули могу пружати опције (или захтевати) постављање фајлова од стране корисника

За управљање фајловима на располагању је посебна компонента, уведена од верзија 2.X: FilePicker (слика 28). Помоћу FilePicker-а могуће је поставити фајл (upload) са сопственог рачунара, преузети са спољне адресе (URL) или пронаћи и поставити из неког репозиторијума (нпр. Alfresco, DropBox...).



Слика 28 - Компонента ”File Picker"

При слању самог фајла, врши се скенирање антивирусом, уколико је та опција омогућена на нивоу система. Ако је фајл заражен, неће бити сачуван, корисник ће добити информацију о томе у самом FilePicker-у. Сам фајл може бити или изолован или обрисан. Изворно не постоје посебни записи о томе да је вирус пронађен.

Политика (полиса) коришћења сајта је, као што је дискутовано претходно у раду, документ којим се дефинише шта је дозвољено, а шта не, током коришћења платформе. Уколико постоји дефинисана политика, потребно је њену адресу унети у поље (такође на страни ”Правила коришћења сајта”) и у том случају ће се приказати приликом регистрације, тј. корисници који се региструју, морају пристати на услове који се полисом прописују, да би се уопште регистровали.

Уколико је на снази неки други вид регистрације или полиса није била дефинисана када су регистровани, могуће је ”пустити” полису да се прикаже свим корисницима први наредни пут када се пријаве и тада ће такође бити потребно да потврде да се слажу са њеним наводима. Поново, важно је нагласити да само прихватање полисе не доприноси нужно вишој свести корисника о коришћењу платформе.

Самом кориснику на располагању је ограничен број опција којима може утицати на сопствену безбедност. Те опције су следеће:

- Промена лозинке. У оквиру свог профила корисник има могућност да иницира промену лозинке. Такође, корисник може иницирати и ресетовање лозинке. С обзиром на то да се у бази лозинке чувају у хеш-варијанти, није могуће дознати оригиналну лозинку, него се прибегава ресетовању, преко опције доступне на самој форми за пријаву.
- Контрола приватности. У склопу својих преферираних поставки корисник може контролисати како добија обавештења од различитих модула. Основни начини су: приватне поруке и е-пошта. У склопу свог профила корисник може контролисати да ли је адреса е-поште уопште видљива, видљива свима или само полазницима истих курсева.

9.3 Аспекти интеграције - место модула у платформи за е-учење

Модул је специфичан софтвер у смислу да није независтан, већ је директно повезан на основни софтвер. На тај начин долази и до условљености изградње и компатибилности са основним софтвером, у овом случају Moodle платформом. Слично би се могло констатовати и за безбедносни модул у случају неке друге платформе.

Модул би требало да поседује одређену аутономију: није предвиђено да корисник константно интерагује са модулом, нити да модул функционише искључиво на основу улаза који добија од корисника (укључујући и администратора), већ одређене активности изводи и периодично самостално.

У том смислу, безбедносни модул се може категорисати као софтверски агент.

9.3.1 Софтверски агент eLearnion

eLearnion има за задатак да реагује на промене у понашању корисника и самог система, спрегнут је са основним системом (LMS-ом), али своје алгоритме спроводи независно, а параметри могу да се задају издвојено. Поседује задате циљеве, а основни циљ је управо повећање безбедносне свести корисника. Да

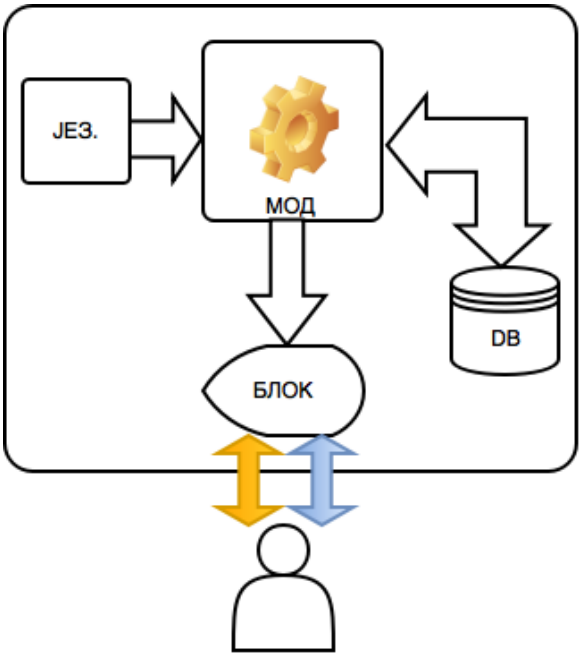
би у томе успео, агент неизоставно мора комуницирати са самим корисницима (слика 29).

eLearnion испуњава следеће услове:

- реактивност - агент реагује на одређене промене система
- аутономија - поседује извесну независност у раду у односу на систем
- проактивност - није искључиво реактиван, већ има задате циљеве
- комуникативност - комуницира са другим системима или чак људима

Ови услови квалификују eLearnion као софтверског агента [135].

Да би се детаљније дефинисале улоге агента који се пројектује, потребно је анализирати димензије његовог понашања.



Слика 29 - Основни концепт архитектуре агента-модула

За реализацију агента потребно је предвидети начине на које он може деловати, а на основу модела који је предвиђен. Основна функција агента јесте комуникација са корисником. То подразумева различите модусе путем којих се информације могу презентовати кориснику. Предвиђа се углавном једносмерна комуникација. Агент презентује одређене информације кориснику, док се, са друге стране, корисник не обраћа агенту директно, већ управо својим понашањем на посредан начин даје информације о томе да ли је и у ком смислу променио своју безбедносну свест. Основна функција самог LMS-а је учење. То

даље подразумева: отварање фајлова, итерацију кроз лекције, решавање тестова, учешће у форумским дискусијама, слање личних порука и низ других активности које су део активног е-учења и е-образовања. Кључно је да се овај процес не ремети радом агента, на пример да агент константно поставља одређена питања, да производи поп-ап обавештења, да шаље велики број мејлова итд. **Агент треба да има балансирану улогу: да утиче на понашање корисника и доприноси унапређењу његове безбедности, али да не омета основни, може се слободно рећи, пословни процес.**

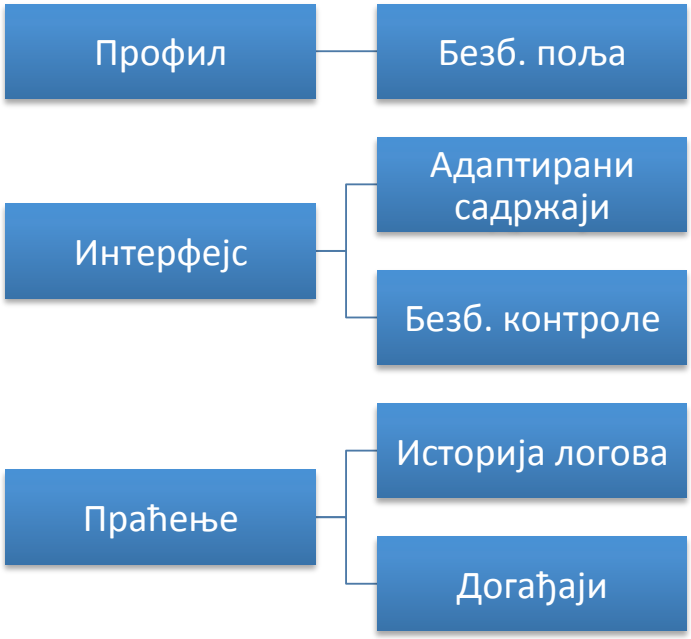
Безбедност је увек супротстављена корисничком искуству и проналажење баланса је изазов који је константан предмет истраживања [136]. Агент који се реализује у овом раду сам по себи није безбедносни механизам у конвенционалном смислу. Крајњи корисник у ствари нема директне интеракције са агентом у смислу да користи одређене безбедносне контроле, подешава га итд. Такође, агент не штити директно и проактивно у маниру у којем то ради антивирусни софтвер, на пример. Основна улога агента јесте да прати понашање корисника и самог корисника (и администратора) обавештава о акцијама које су пожељне или не, о начинима за унапређење безбедносне свести, као и да му помогне да користи поједине, већ постојеће безбедносне контроле. Чињеница да корисник углавном не управља понашањем агента не значи да агент не би могао да наруши квалитет употребљивости (usability) основног система. Управо у томе је основни изазов дизајна оваквог агента. Такође, елементи комуникације које агент има са администратором система додају димензију пасивног IDS-а (система за детекцију упада[4]): администратор је обавештен о одређеним инцидентима или променама које би могле бити значајне за систем и на њему је да даље предузме одређене мере.

Сам агент мора бити конципиран тако да се наслања на систем за управљање учењем. Међутим, основни принцип рада агента је генерички и може се применити и на друге информационе системе, о чему ће касније бити дискутовано. **Оно што је специфичност примене код самог система за е-учење јесте могућност искоришћења управо едукативних алата које тај систем нуди. У неком другом информационом систему би такве алате требало додатно развијати и додавати, док у систему за е-учење већ постоје потребне варијанте.**

[4] Intrusion Detection System

Основни елементи агента

Како је напред наведено, агент заснива рад превасходно на два елемента: комуникацији са корисником и праћењу активности. На слици 30 дат је концепт функција које је потребно реализовати.



Слика 30 - Функције eLearnion-а

Контуре агента аутор је представио на конференцији eLearning 2015 [137].

Праћење активности корисника

Агент би требало да функционише на основу праћења корисника. Праћење подразумева добијање информација о активностима корисника. У зависности од природе активности, праћење може бити ”пост-мортем”, тј. на основу белешки (логова) система у неком задатом интервалу или у реалном времену. На пример, да бисмо добили одређену законитост или образац понашања, корисно је разматрати већи број инстанци, односно више записа о понашању и за то је најпогоднији лог. Конкретно, ако желимо да проверимо како се понашао корисник по питању одјаве своје веб-сесије, можемо погледати у историју понашања и видети да ли корисник има навику да се одлогује или не. За ове потребе може се искористити неки вид лога. Moodle бележи велики број догађаја, а могу се дефинисати и додати и нови.

Са друге стране, одређене активности је практичније испратити у реалном времену, то јест, узимати их у обзир одмах пошто се изврше. На пример, ако

антивирус пронађе малициозни код који је постављен у корисничком фајлу, потребно је одмах извршити обавештавање администратора, али и ажурирати информације о самом кориснику. За ове потребе могуће је искористити систем догађаја, доступан у новијим верзијама Moodle-а.

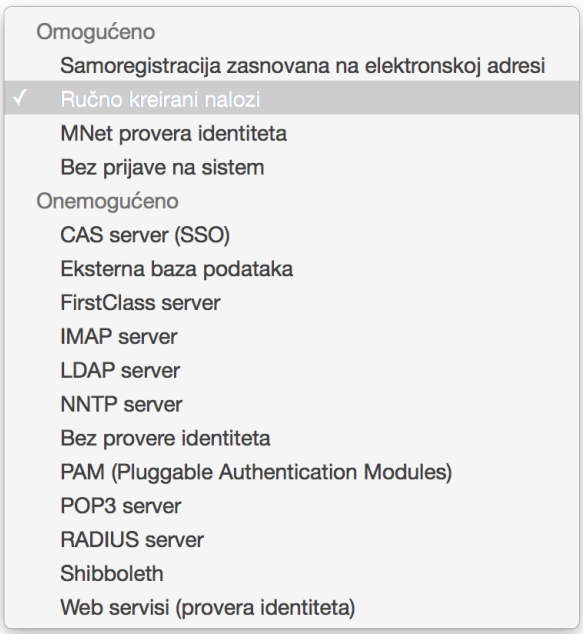
Комуникација eLearnion-а са корисником

LMS Moodle подржава више начина за комуницирање са корисником. Први, тривијалан, је путем садржаја на самим курсевима. На пример: корисник (ученик) има приступ одређеном садржају на страни курса и добија одређену информацију - као када учи. То може бити лекција, текстуални-фајл и сл. Други начини подразумевају циљану комуникацију, при којој се конкретном кориснику активно шаље информација. У такве начине спадају е-пошта и приватне поруке. Moodle подржава и екстерне облике комуникације један-на-један, односно чета (може бити и групни чет), нпр. путем Jabber-а. Као основни елемент који служи за комуникацију одабран је блок. Као што је поменуто у претходним деловима рада, блок је елемент који се поставља на ниву курса (или читавог сајта) и може садржати различите информације или помагати у административним операцијама (навигација). Програмски је могуће и персонализовати садрај, на пример тако да одређени корисник добије наменски одређену информацију.

У комуникацију са корисником може се убројити и промена интерфејса, као и додатне информације којима се опремају безбедносне контроле. На пример, на основу параметара корисника, приказује се одређени савет за употребу неког елемента заштите (задавање лозинке, постављање фајла).

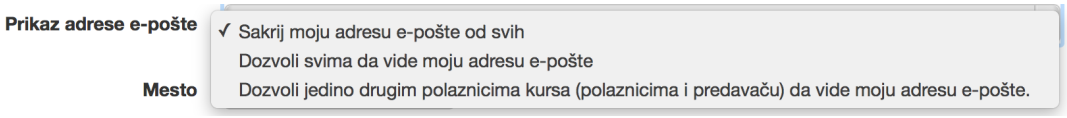
Профил корисника

Корисник у Moodle-у поседује велики број профилних информација, од којих су многе опционе. Ове информације могу се преузимати на основу повезивања са екстерном базом студентске службе, као и из различитих других извора (слика 31).



Слика 31 - Извори података за аутентификацију у Moodle-у

Профил нема посебних поља којима се значајније може контролисати безбедност корисника. Фактички, корисник може контролисати једино видљивост електронске поште (Слика 32).

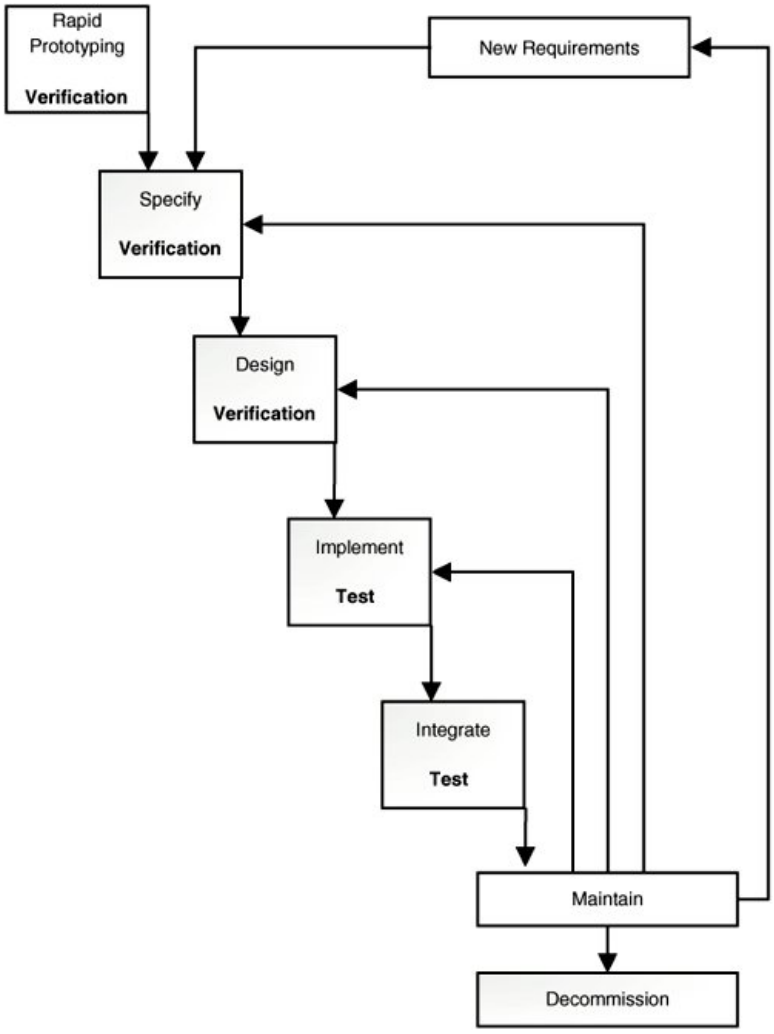


Слика 32 - Контрола видљивости адресе електронске поште

Модел безбедности дат у овом раду инсистира на унапређењу модела корисника, што подразумева постојање структуре у профилу самог корисника којом се означава његов безбедносни статус. Ова поља могу се дефинисати као додатна поља и то може учинити сам администратор или је могуће аутоматски задати да се инсталацијом плагина креирају у бази. Предвиђена су три таква поља, као што је дато у приказу модела корисника. Два поља (loginadmin, capacity) су контролисана од стране самог система и нису непосредно видљива кориснику, док поље privacy корисник може видети и мењати.

9.4 Развој софтверског агента eLearnion

За потребе што ефикаснијег и квалитетнијег пројектовања софтвера, установљене су различите методологије развоја [138]. Избор конкретне методологије зависи од самог софтвера, односно захтева клијента, комплексности и временских рокова.



Слика 33 - Rapid Prototyping (преузето из [138])

Код софтвера који захтевају брз развој и тестирање у примени, најчешћи избор је ”брз прототипски развој” (rapid prototyping) - слика 33. Код овог приступа развија се основна функционалност, а касније се могу уградити и додатни захтеви. Циљ је што пре развити софтвер и на основу повратне информације од крајњих корисника додати потребне елементе.

За развој безбедносног модула изабран је приступ брзе израде прототипа. У прилог овом избору иду следећи аргументи:

- Улазни параметри нису фиксни, тј. захтеви нису комплетно познати на почетку развоја, већ се могу појавити и додатни захтеви
- Постоји висок степен интерактивности корисника и модула
- Потребно је што пре доћи до повратних информација, које би допринеле доради модула, али и које би биле показатељ о томе какав је шири утицај самог модула

9.4.1 Дефинисање случајева коришћења

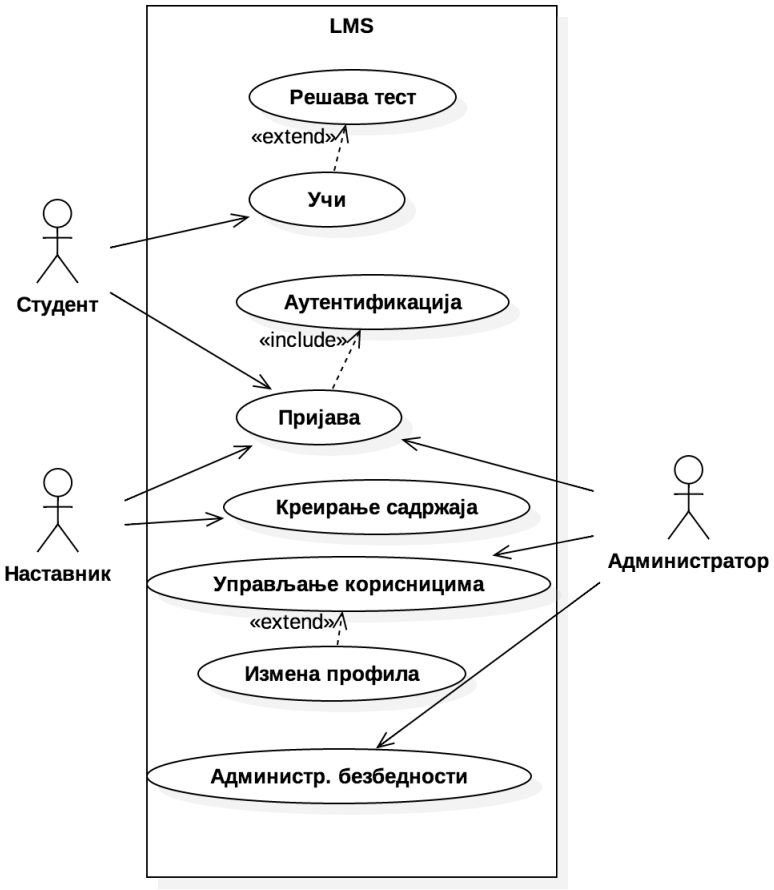
У развоју основне платформе за е-учење (самог Moodle-а) већ су коришћени одређени захтеви. Функционални захтеви платформе за е-учење односе се на могућности које софтвер треба да пружи у смислу образовних функција. На пример, функционални захтев био би да корисник у улози наставника може да постави фајл као ресурс на курс. Захтеви који се односе на безбедност јесу нефункционални захтеви, гледано из угла комплетне платформе. Њихово испуњавање је опција која је потребна, али не и неопходна. Међутим, на нивоу модула, ови захтеви постају функционални.

Модул нема за задатак да реимплементира постојеће механизме заштите или да побољшава сам систем за учење у смислу његових функционалних захтева, већ да дода могућности које се тичу управљања безбедношћу.

Захтеви су постављени превасходно на основу анализе ризика. Модул има задатак да имплементира механизме заштите до којих се дошло анализом ризика.

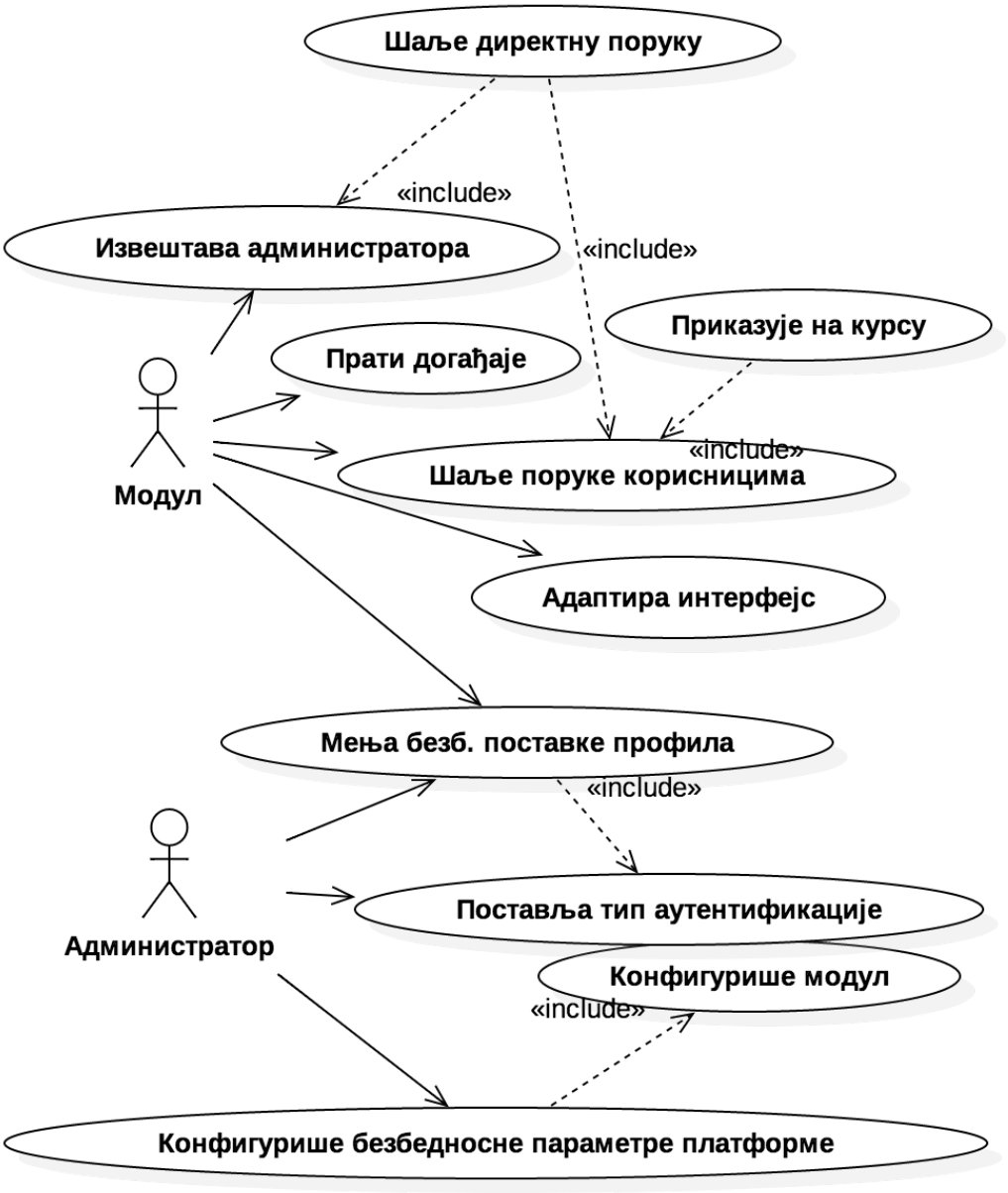
За потребе спецификирања захтева и понашања модула креирани су одговарајући UML дијаграми. Коришћени су алати StarUML и MS Visio 2010.

Дефинисане су три основне категорије корисника: администратор, наставник и ученик. Ове категорије приказане су кроз генерички случај коришћења (слика 34). За потребе дефинисања случајева који су релевантни за сам модул, потребно је креирати посебне, специфичније дијаграме.



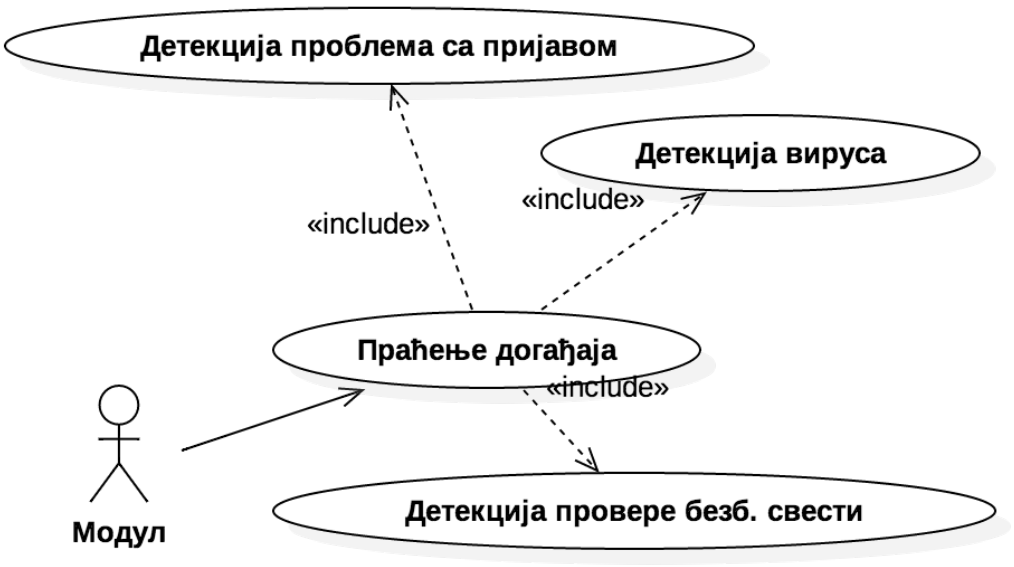
Слика 34 - Генерички случајеви коришћења у LMS-у

Безбедношћу се баве администратор и сам модул, који се може дефинисати као посебан корисник. Администратор конфигурише основне поставке модула. Овај случај коришћења назван је ”администрација безбедности” (слика 35).



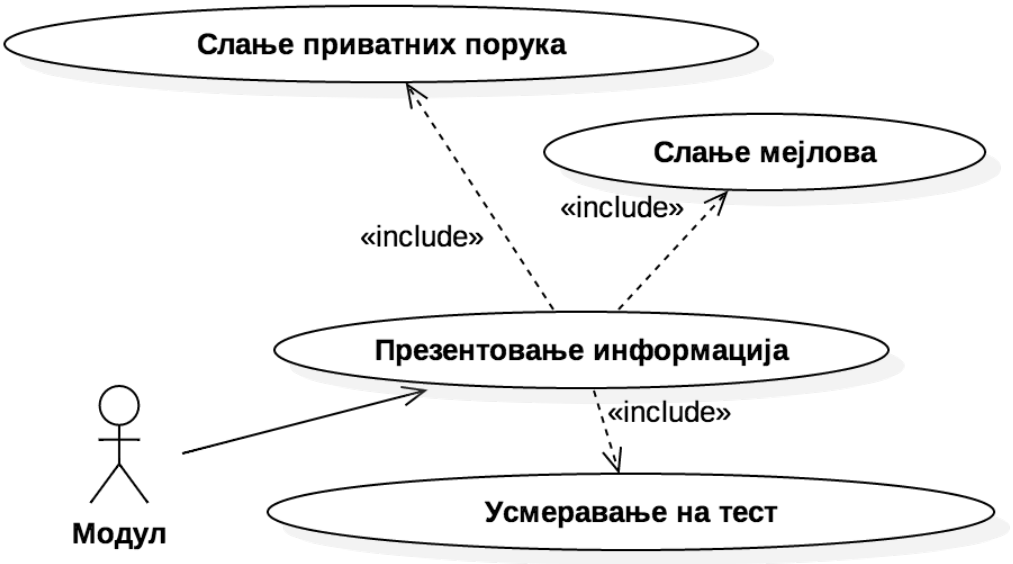
Слика 35 - Случај коришћења *Администрација безбедности*

Случај коришћења ”праћење догађаја” приближава овај важан сегмент рада модула (слика 36).



Слика 36- Случај коришћења *Праћење догађаја*

Модул/агент задужен је и за презентовање информација (слика 37).

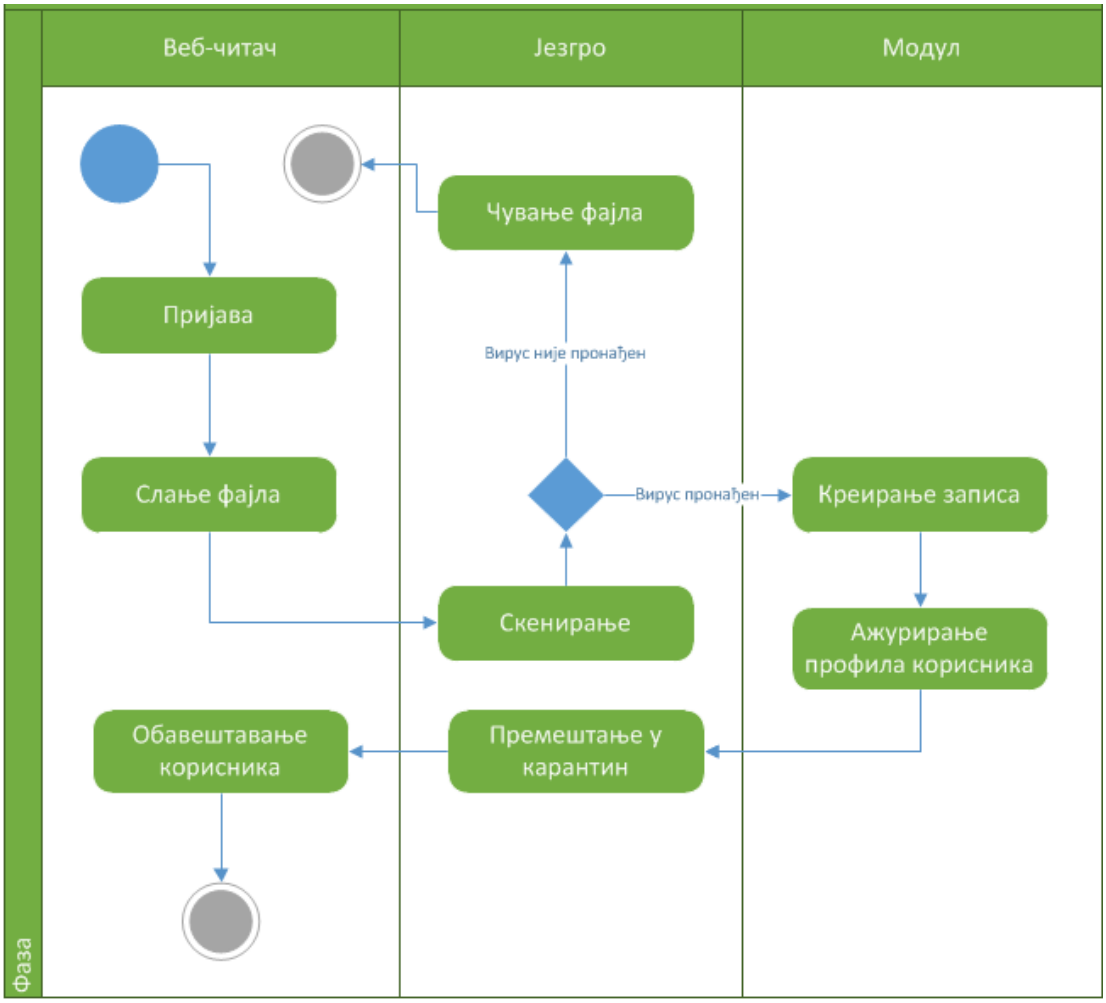


Слика 37 - Случај коришћења *Презентовање информација*

9.4.2 Дијаграми активности

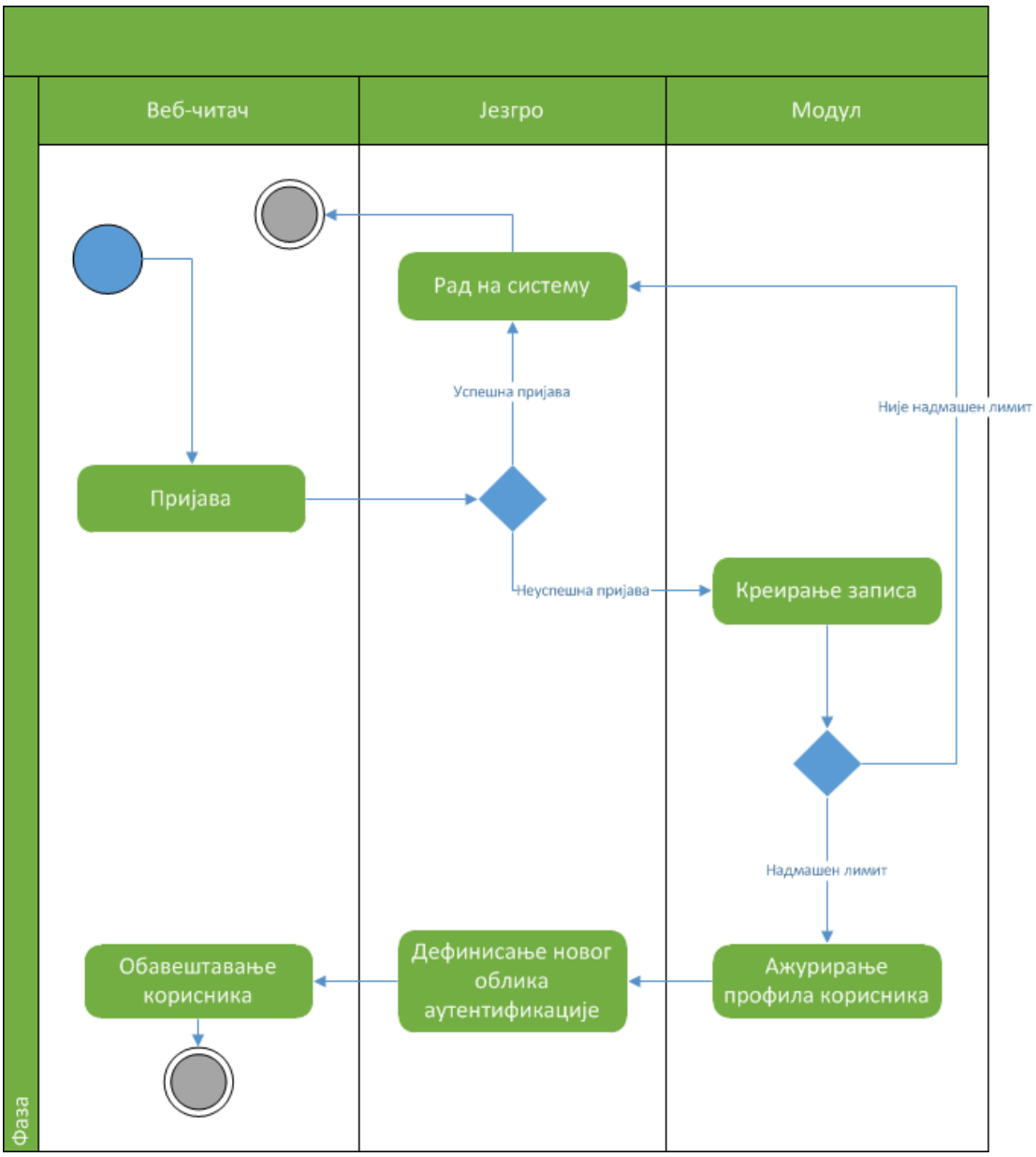
Помоћу дијаграма активности могу се расветлити и рашчланити активности које изводе различити актери и на тај начин боље сагледати динамичка природа процеса, у овом случају рада модула.

Постављање фајла је једна од потенцијално критичних активности и модул овакву активност треба да прати и реагује у случају да је фајл заражен (слика 38). Повезивањем са елементима језгра, модул добија информацију о томе да је фајл заражен и то се одражава на профил корисника.



Слика 38 - Дијаграм активности *Постављање фајла*

Корисниково управљање пријавом и рад модула такође се могу описати у динамичком контексту кроз дијаграм активности (слика 39).



Слика 39 - Дијаграм активности *Пријава*

9.4.3 Дефинисање захтева

На основу анализе самог модела и случајева коришћења и дијаграма активности могу се на почетку за модул дефинисати следећи захтеви:

- проширење профилних поља и могућност контроле од стране администратора, према моделу корисника

- презентовање информација на основу профила корисника
- омогућавање да администратор прати додатне активности проистекле из рада модула
- слање мејлова и порука са битним информацијама корисницима
- стално ажурирање корисниковог профила
- слање обавештења администратору
- обавештавање корисника
- усмеравање корисника на проверу безбедносне свести

9.4.4 Развојни алати и окружења

Основни систем (Moodle) диктира хардверске и софтверске захтеве и њих поштује и модул. У овом случају за развој је коришћено следеће окружење:

- MacBook Pro, 16GB RAM, Intel i7 2,2 GHz
- OSX Yosemite, MAMP 3.0.7.3 (Apache 2.2.29, PHP 5.6.2 (са потребним библиотекама), MySQL 5.5.38).

За тестирање у продукционом окружењу коришћена је следећа конфигурација:

- Windows 7 Professional, 8GB RAM, Intel i5 3GHz
- XAMPP (Apache 2.4.17, PHP 5.6.14, MariaDB 10.1.8)

За развој је коришћен NetBeans [139] (верзија 8.0.2, за MacOS, са потребним додацима за PHP развој). Разлози за избор овог окружења су: бесплатно је и поседује добру подршку за PHP дебаговање и тестирање PHP пројеката.

Напомена: Развој модула је изведен за у том тренутку последњу верзију 2.9. За продукционо окружење у реалним условима препоручује се инсталација и покретање на серверском оперативном систему (нпр. CentOS, Windows Server), са посебно инсталираним системиима за управљање базама података и веб-сервером. Због што бржег постављања у продукцију и ради обезбеђивања последњих верзија сервиса (које захтева ова верзија Moodle-а), тестни сервер је успостављен на Windows-десктоп оперативном систему.

9.4.5 Елементи развоја

Кôд агента грубо се може сврстати у две категорије: кôд блока и кôд језгра. Као што је претходно наведено, због природе модула, није могуће учинити га у потпуности одвојеним и независним од језгра основног софтвера. У том смислу, написан је кôд који представља блок - основни градивни елемент комуникације са корисником и кôд који модификује језгро система. Блок је сам по себи објекат, инстанца класе *Block* и као такав поседује низ наслеђених метода, а остале методе и подаци се додају на основу захтева. Блок комуницира са језгром у

донекле лабаво спрегнутом маниру (lously coupled), јер постоје функције за комуникацију и систем догађаја који омогућава размену информација кроз јасно дефинисане интерфејсе. Међутим, за одређене функције, неопходно је мењати код самог језгра.

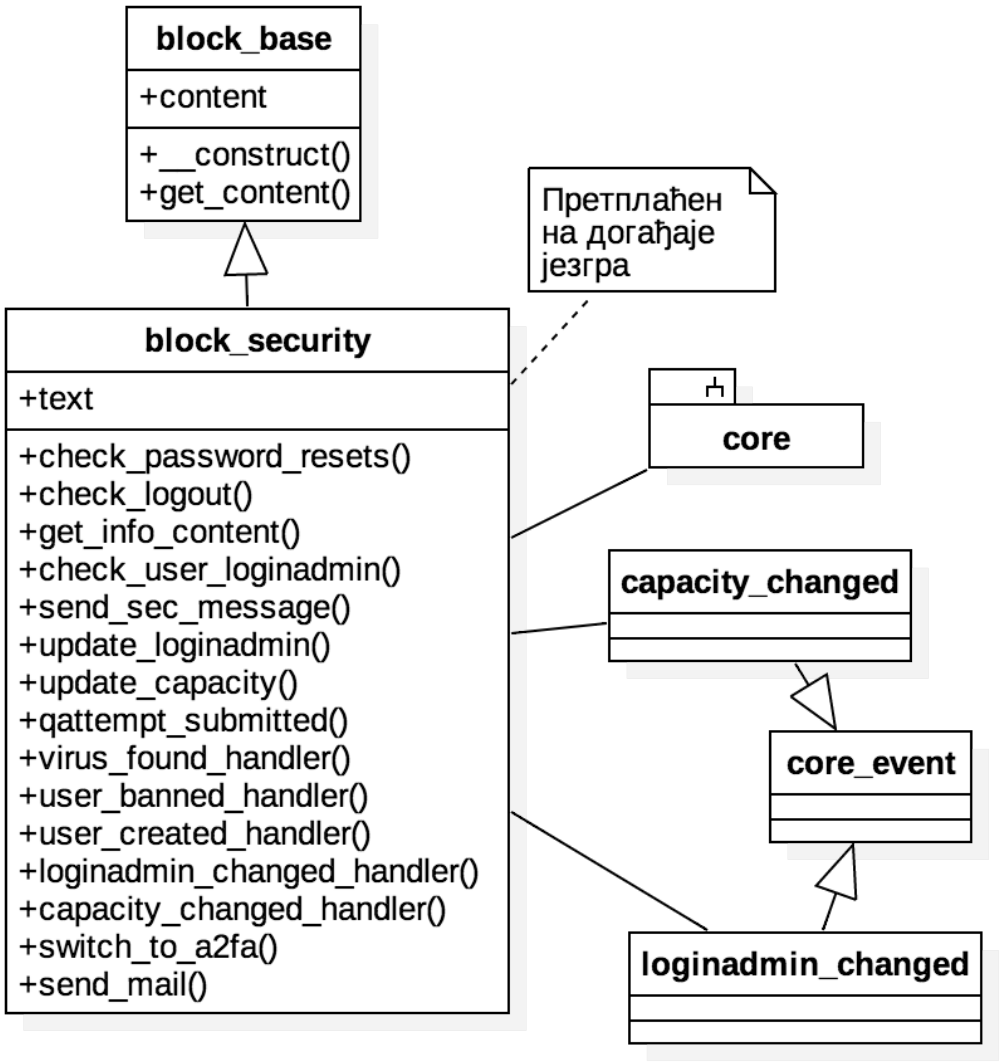
Овакав приступ (промена кода језгра) отежава надградњу система, јер свако ажурирање основног система (значи и језгра), мора бити испраћена поновном модификацијом, тј. хармонизацијом модула. Да би се модул креирао као потпуно модуларан, у смислу потпуне одвојености од основног система, неопходно је да се језгро додатно модуларизује, што је питање одлуке и стратегије самог развојног тима Moodle-а[5].

Moodle је добрим делом пројектован као објектно оријентисан софтвер. Ипак, постоји веома мало документације самом развоју у смислу UML дијаграма. Додаци се морају ослонити на постојеће класе и функције језгра.

Основни класни дијаграм модула садржи сам блок и апстраховане елементе језгра (слика 40).

Класа block је наслеђена и блок модула је претплаћен на одређене догађаје језгра. Такође, посебне класе, које припадају модулу, представљају нове догађаје, који су директно везани за модул. Ове класе се аутоматски учитавају и њихове хендлер-функције су чланице класе блока-модула.

[5] Током писања овог поглавља, издата је верзија 3.0, у којој је функционалност скенирања послатих фајлова антивирусом издвојена као модул.



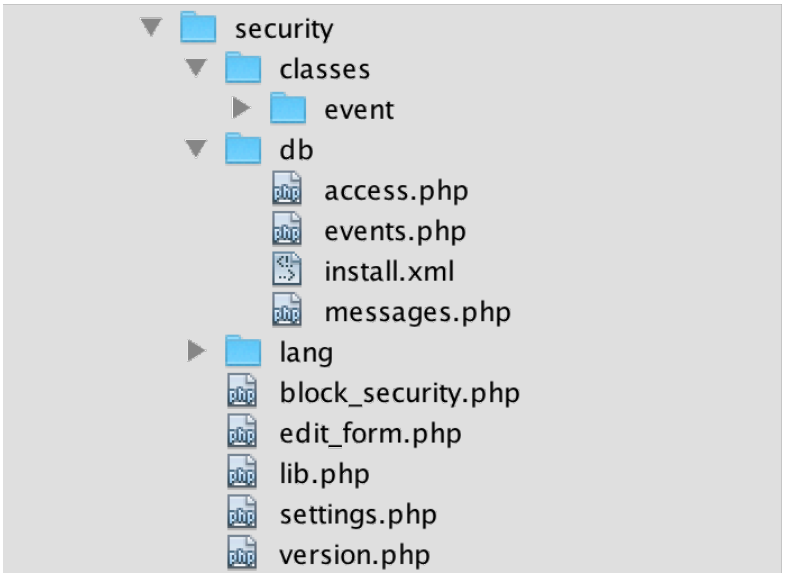
Слика 40 - Дијаграм класа модула

Физички, блокови се налазе у директоријуму *blocks*. Блок безбедносног модула назван је "security" и поред фајлова са кôдом, садржи и посебне директоријуме са одговарајућим помоћним елементима. У питању су следећи фолдери:

- *db* - по конвенцији Moodle кодирања, садржи дефинисана права приступа самом блоку - access.php, events.php - догађаје на које је претплаћен блок (односно сам модул), иницијални xml фајл са структуром потребних табела у бази података и фајл messages, који дефинише блок као један од извора порука за кориснике.

- *classes* у свом подфолдеру event садржи дефиниције догађаја које производи модул. На пример ”промењен безбедносни капацитет”
- *lang* садржи одговарајуће стрингове. Moodle све стрингове (натписе, поруке итд.) чува у виду променљивих, како би се омогућила вишејезичност. У оквиру lang фолдера модула налазе се фајлови са паровима променљива-приказан стринг.

Изглед структуре фајлова приказан је на слици 41.



Слика 41 - Структура фајлова са кодом

Објекат блок

Кључни фајл у којем се оркестрира овај део модула (реализован као блок) јесте block_security.php. У њему се дефинише класа самог блока и специјализује конкретна инстанца, са припадајућим променљивим. Гро функција блока измештено је у посебан фајл, lib.php, који се у ствари укључује у главни фајл блока (инструкцијом include). Основна конструкција која дефинише блок приказана је на слици 42. Укључене су неопходне библиотеке: основни конфигурациони фајл (config.php), библиотека за поруке, библиотека са функцијама самог модула и посебна библиотека за аутентификацију.

```php
<?php

require_once($CFG->dirroot .'/config.php');
require_once($CFG->dirroot .'/message/lib.php');
require_once($CFG->dirroot .'/blocks/security/lib.php');
require_once($CFG->dirroot .'/auth/a2fa/GoogleAuthenticator.php');

class block_security extends block_base {
    public function init() {
        $this->title = get_string('pluginname','block_security');


    }

    public function get_content() {
    if ($this->content !== null) {
      return $this->content;
    }
```

Слика 42 - Костур блока

Систем догађаја олакшава повезивање модула са деловима језгра. Одличан пример за ово је повезивање са догађајем ”креиран корисник”. Предвиђено је да модул, када корисник достигне минимум вредности *loginadmin* и *capacity*, буде преусмерен на алтернативну, двофакторску аутентификацију. У том смислу, инсталиран је додатак који то омогућава. Међутим, аутори овог додатка предвидели су да администратор треба да мануелно примени овај облик, а не да се то догађа аутоматски. Тада се врши и ”ручно” генерисање токена, на основу којег се корисник и пријављује. Такође, предвиђено је да (пошто корисник више не може да се пријави на класичан начин, нити је линк за пријаву важећи) администратор достави одговарајуће податке кориснику. Код модула је то решено тако што је написана хендлер-функција, која је у db/events декларисана као "observer", односно претплатник на догађај језгра ”креиран корисник” (user_created).

```php
array(
       'eventname'=>'\core\event\user_created',
       'includefile' => '/blocks/security/lib.php',
       'callback' => 'user_created_handler'
       ),
```

Чим се корисник креира (региструје самостално или унесе од стране администратора), аутоматски се генерише токен за 2-факторску аутентификацију. Онда, уколико се догоди да агент промени аутентификацију у 2-факторску, блок има задатак да пошаље поруку мејлом, тако да корисник може да добије све потребне информације за пријаву: коју апликацију преузима,

како приступа итд. У наставку је дат део кода који одговара хендлер-функцији која се позива при креирању корисника:

```
function user_created_handler($event)
    {
        global $DB;
        $userid=$event->objectid
        $user=$DB->get_record('user', array('id' => $userid));
        profile_load_data($user);
        $ga = new PHPGangsta_GoogleAuthenticator();
        if (empty($user->profile_field_a2fasecret))
        {
           $user->profile_field_a2fasecret = $ga->createSecret();

            profile_save_data($user);
        }
        return true;
    }
```

Променљива *$DB* спада у тзв. *глобалне променљиве* и веома често се употребљава у коду. $DB представља апстракцију базе података: то је објекат који подржава различите функције за приступ, измену и уопште манипулацију подацима у бази. У овој функцији потребно је да се, на основу података добијених од самог догађаја (променљива $event), конкретно идентификатора креираног корисника, генерише објекат ”корисник” (user), а затим његова додатна поља (једно од њих чува токен за 2-факторску аутентификацију) попуне вредностима. Уколико није задат токен (a2fa поље је празно, а то је подразумевани случај), генерише се нов токен, поставља у одговарајуће поље профила и затим чува.

На овом релативно једноставном примеру показано је како се одређене функционалности које су повезане са задацима самог модула, могу повезати са језгром, односно одговарајућим догађајима. Догађај се ”опрема” одређеним параметрима (на пример ”који корисник”), а затим окида у језгру, да би се затим сви претплатници аутоматски активирали, односно позвале одговарајуће функције-хендлери.

Ретроактивна провера логова

Да би корисник добио одговарајући садржај (који је у складу са вредностима пре свега поља *loginadmin* и *capacity*), позивају се одговарајуће функције из lib.php током самог приказивања блока (када се страна са блоком учитава). Међутим, за потребе анализе историје понашања корисника, потребно је да се прегледају логови у одређеном временском интервалу, како би се уочио одговарајући шаблон. На пример, да ли корисник има проблема са пријавом, да ли често мења IP адресе итд. У том смислу, функције које проверавају овакве шаблоне

позивају се периодично. Уопште, за одржавање Moodle-а, потребно је у позивати cron.php (/admin/cron.php). Овај скрипт је задужен за слање мејлова, чишћење налога који нису потврђени у одређеном интервалу, рачунање статистике итд. У случају овог безбедносног модула, потребно је да cron.php ”испрозива” и функције које су задате за периодично позивање унутар модула. Овакве функције се на нивоу блока или другог модула групишу у посебан блок кода, под локалном функцијом *cron*.

```
public function cron()
{
    mtrace("Cron security bloka");
    check_password_resets();
    check_logout();
    check_various_ips();
}
```

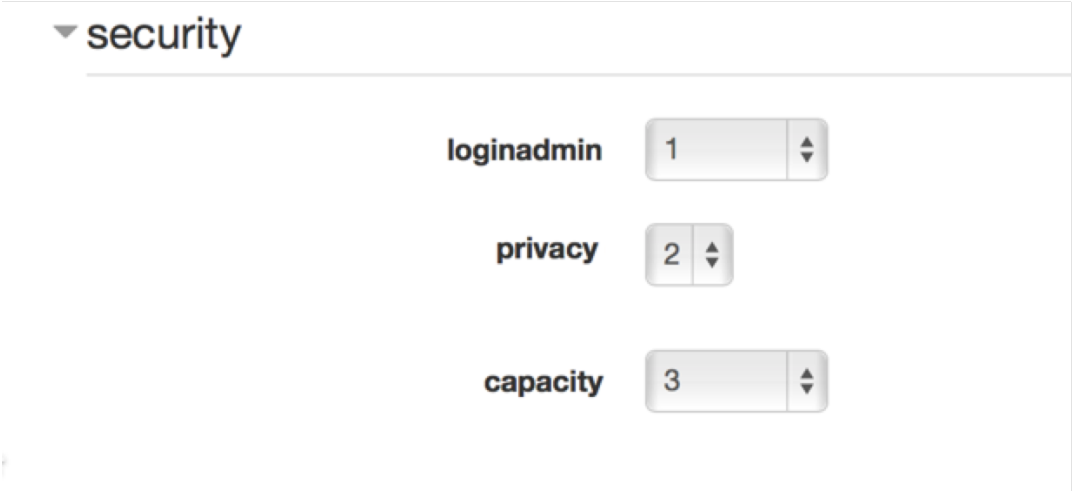
У конкретном примеру, при сваком позивању опште *cron* функције, позива се и ова, функција блока, којом се даље позивају функције за проверу да ли је корисник користио услуге ресетовања лозинке, да ли се редовно одјављивао и да ли је премашен одређени задати лимит IP адреса које је користио, након којег постоји оправдана сумња о злоупотреби налога.

Параметре на основу којих блок, па самим тим и читав модул, функционише, може мењати администратор.

Moodle чува конфигурацију система у табели mdl_config. Све вредности које се налазе у овој табели иницијализиване су у глобалној променљивој $CONFIG и кôд може приступити преко ове променљиве.

9.5 Кориснички приказ модула

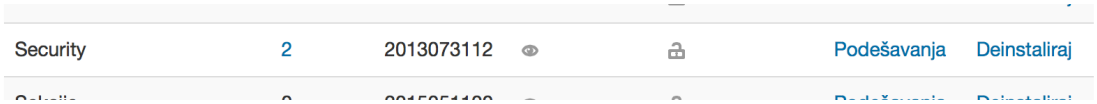
Модул се конфигурише од стране администратора. Такође, додатна поља профила задају се од стране администратора као тзв. *custom* поља (слика 43).



Слика 43 - Додатна поља профила - поглед администратора

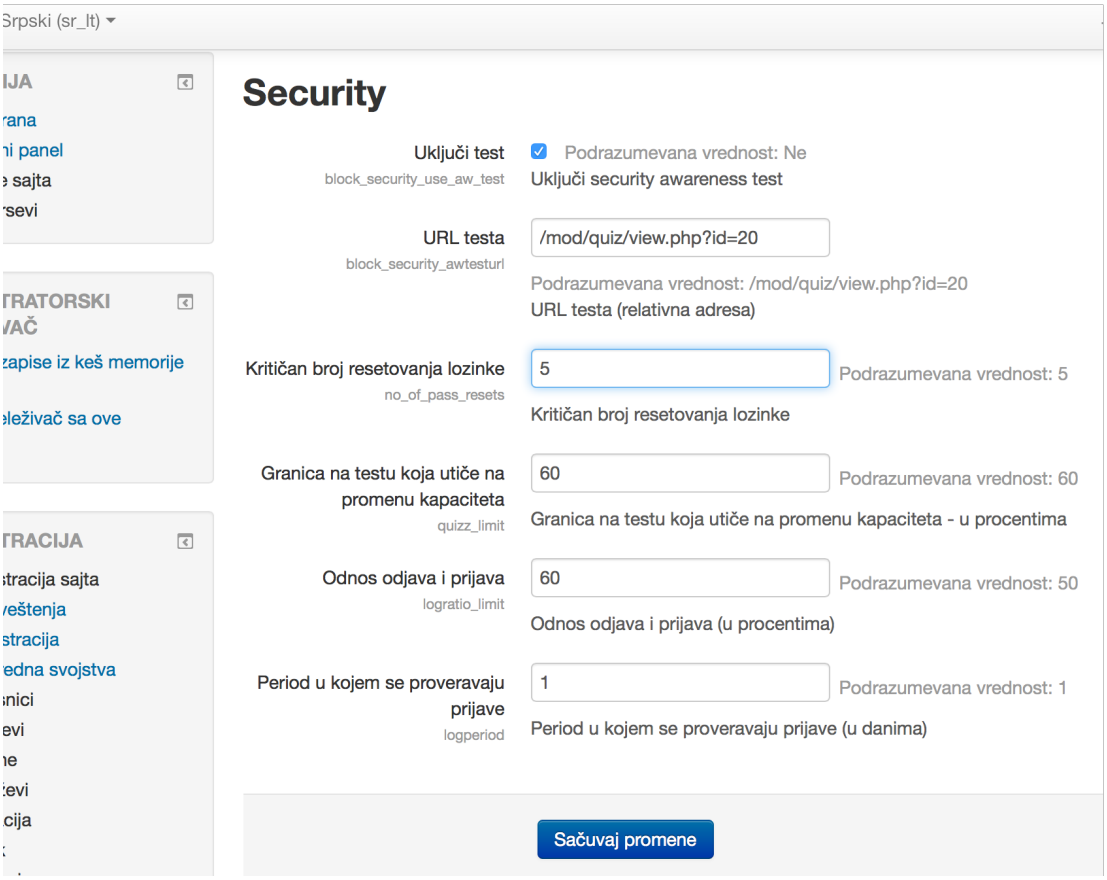
Поља имају вредности од 1-3 (privacy 5), а при креирању налога, поставља се подразумевана вредност (2), односно за вредност privacy корисник може поставити жељену вредност.

Приступ интерфејсу за конфигурацију модула врши се кроз мени за конфигурацију блокова (слика 44).



Слика 44 - Приступ конфигурацији модула

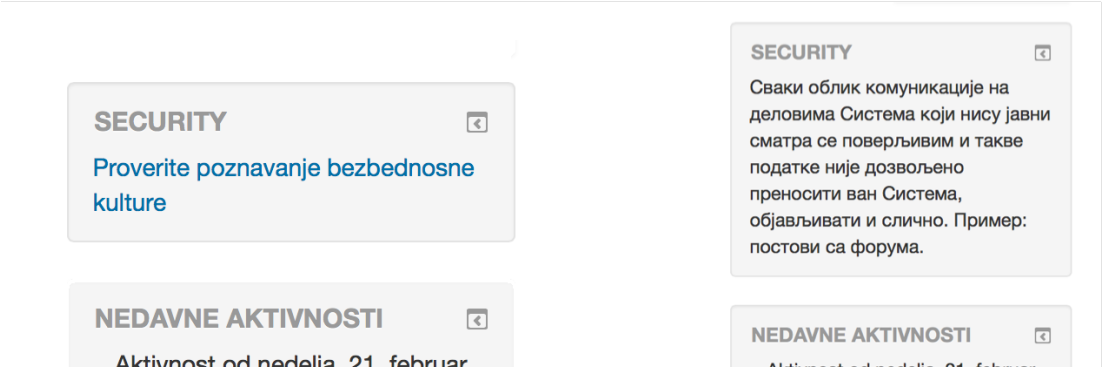
Конфигурација модула своди се на дефинисање параметара које модул интерно користи у свом раду (слика 45). Временом администратор може да стекне увид у то које су вредности оптималне за дато окружење и дефинише их. Ове вредности могу зависити од различитих фактора, као што је на пример природа курса, број корисника итд.



Слика 45 - Конфигурација модула

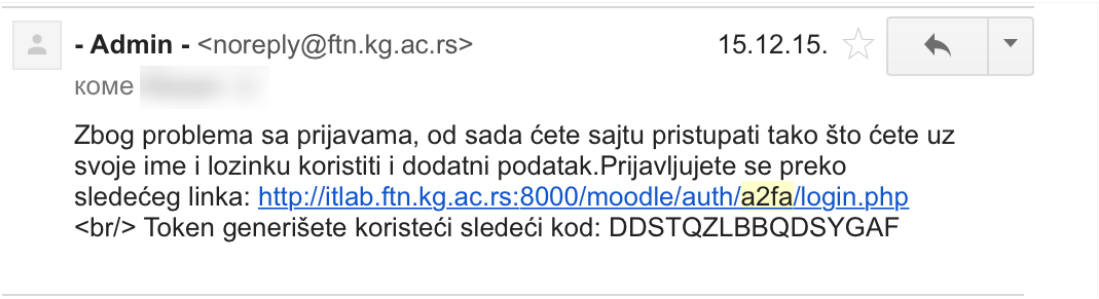
Корисникова интеракција са самим модулом је минимална. Корисник (е-ученик) може да контролише само вредност privacy, док се остале вредности *security* сегмента профила контролишу од стране модула или од стране администратора.

Корисник пре свега види садржај блока на самом курсу (слика 46).



Слика 46 - Приказ блока са различитим садржајима

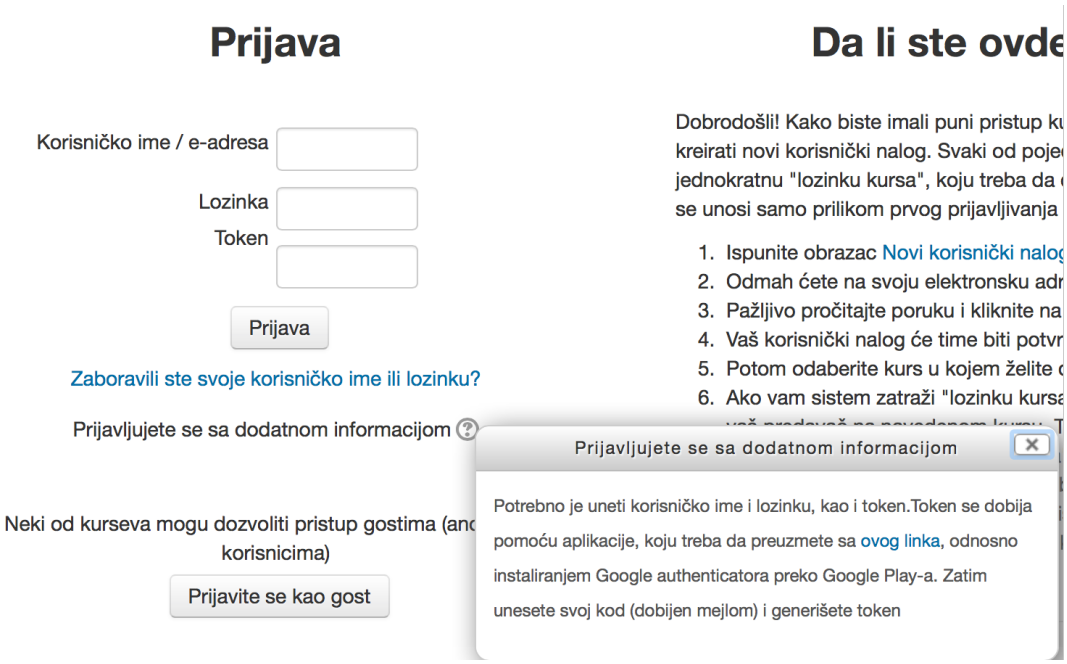
Поред информација из блока, корисник добија и личне поруке и мејлове. На пример, уколико дође до промене типа аутентификације, добија мејл са подацима неопходним за приступ (слика 47).



Слика 47 - Пример мејла послатог од стране модула

Поред мејла, користи се и систем личних порука, које непосредно стижу корисницима када су пријављени на систем.

Корисник добија и допунске информације које имају задатак да му помогну у операцијама које су везане за управљање сопственом безбедношћу: додатни систем помоћи (слика 48), усмеравање на ресурсе везане за конкретан ризик итд.



Слика 48 - Додатни систем помоћи за 2-факторску аутентификацију

Последњи сегмент у којем се огледа интерактивност модула у ширем смислу је управо безбедносни тест, који корисници решавају и који директно утиче на њихов безбедносни профил.

Пројектовање модула је ослоњено на стандарде, превасходно на серију 27000. Ток изградње самог модула (PDCA), као и препоруке у виду тзв. пракси директно су преузети из одговарајућих стандарда. Такође, сам модул се може видети као екстензија архитектуре LTSA, тј. стандарда IEEE1484, као и стандарда IMS LIP. Тиме се може закључити да је прва хипотеза доказана: модул је пројектован кроз стандардизовану методологију управљања безбедношћу и е-образовне стандарде.

Задаци модула су дефинисани на основу изабраних критеријума за обезбеђење квалитета. Ови критеријуми установљени су на основу шема квалитета, као и на основу анализе модела квалитета у е-образовању. Модул директно подржава следеће критеријуме:

- **Комуникација са корисницима о процедурама и начинима заштите садржаја**
- **Обавештавање о примењеним технологијама.**

С обзиром на то да модул директно реализује ова два задатка (између више својих задатака), може се констатовати да позитивно утиче на обезбеђење квалитета е-учења, чиме је подржана хипотеза 2.

10. Евалуација

Евалуација представља проверу рада модула у реалном окружењу и у складу је са PDCA циклусом који је апострофиран као методологија за пројектовање безбедносног информационог система (фаза ”Check"), у овом случају једног модула. У том смислу потребно је проверити перформансе и упоредити понашање са задатим захтевима и формирати одговарајући извештај.

У оквиру евалуације у овом раду потребно је проверити и хипотезе везане за поверење у коришћење система за е-учење и прихваћеност е-учења (H3 и H4). У том смислу извршено је одговарајуће истраживање.

10.1 Ток истраживања

За потребе истраживања коришћена је платформа наведена у претходном поглављу. Сајту је омогућен приступ преко адресе Лабораторије за информационе технологије на Факултету техничких наука у Чачку (itlab.ftn.kg.ac.rs:8000/moodle).

Модул није било могуће имплементирати код постојећег Moodle система, који броји око 2000 корисника, иако би за потребе евалуације то било најбоље. Разлози леже у томе што је у питању знатно старија верзија, као и у томе што је у питању тестирање, које са собом повлачи и евентуалне исправке, паузу у раду система и непредвиђена понашања, што би могло да има непредвидљив утицај на велики број курсева. Стога се аутор определио за приступ по којем је посебан, ажуран систем са уграђеним модулом постављен на посебан рачунар, а за потребе реалистичног тестирања, постављен је и курс и уписани полазници. Регистрација је отворена, а тестни курс је заштићен лозинком, којом је регулисан упис.

Истраживање је трајало од 20. новембра 2015. до 31. јануара 2016. На Moodle систему са имплементираним модулом постављен је курс ”Технологије и алати за оцењивање” и уписано 35 полазника. Формиране су 4 наставне теме са различитим облицима садржаја. Сваке седмице отварана је по једна нова тема, чиме се одржавала динамика. Наставни садржаји су изабрани тако да не буду превише тешки и да својом занимљивошћу мотивишу полазнике да посећују курс.

Полазницима није предочено шта се тачно испитује са циљем да се не утиче на њихов начин коришћења сајта и курса, како би се на крају добили што валиднији подаци за анализу. Све време трајања курса, полазници су од наставника (аутора) добијали задатке и информације као на класичном систему, без

наглашавања значаја безбедности. Није било сугерисања о начину коришћења сајта, о томе да ли треба решавати тест везан за безбедност итд. Да би се проверило како сам модул утиче на поверење у систем и прихваћеност е-учења, учињен је максималан напор да се оствари реално окружење, у којем би модул самостално презентовао одређене информације на курсу, слао поруке и обављао своје активности без уплива и додатних објашњавања од стране администратора или других лица. (На сваки захтев за корисничку подршку је одговорено, међутим није ни на који начин додатно скретана пажња на безбедносне контроле, нити индукована потражња за подршком - амбијент је максимално приближен реалном систему.)

По завршеном курсу, полазници су замољени да попуне два упитника. Циљ упитника био је испитивање: да ли и како модул утиче на прихваћеност система за е-учење и колико утиче на поверење корисника (полазника) у е-образовање.

Упитници су дати у прилогу (13.2, 13.3). Формирани су на основу модела представљених у самом раду, конкретно: [54] и [74] за поверење, а за прихватање модификовани TAM [79], [80] . Упитници су реализовани кроз модул Questionnaire на самом систему за е-учење.

Упитнике је попунило 30 полазника. Популацију која је похађала курс чинили су углавном студенти четврте године основних студија информационих технологија и пете године интегрисаних студија (техника и информатика). Осим њих, курс је похађало и неколико сарадника Факултета, од којих је четворо попунило упитнике.

Искази су сортирани по категоријама, а одговори су мапирани према Ликертовој скали са 5 степени слагања (”у потпуности се слажем”, ”углавном се слажем”, ”немам став”, ”углавном се слажем” и ”у потпуности се слажем”, са нумеричким вредностима 1-5). Постоје питања са отвореним одговорима, која су дата опционо, ради додатних квалитативних нализа и добијања општих повратних информација.

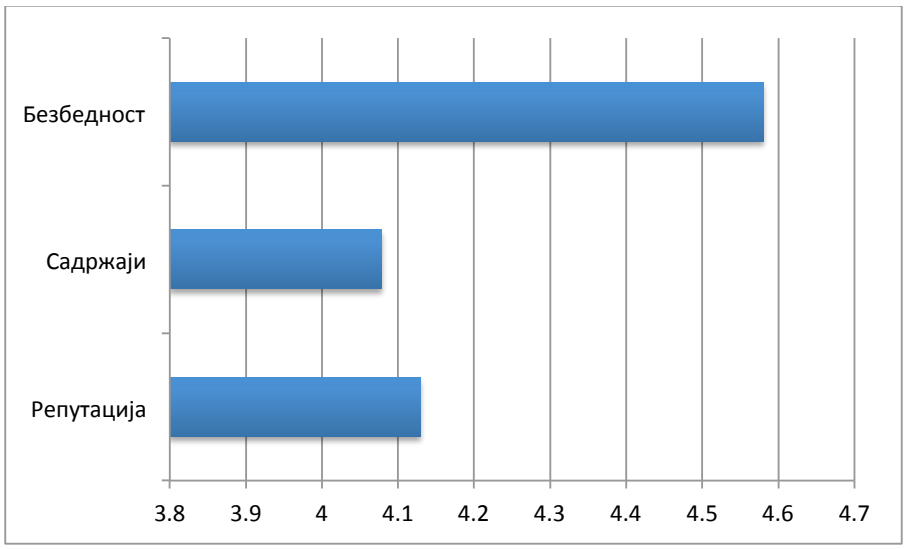
За анализу података коришћене су методе дескриптивне статистике и структурног моделирања (SEM). Коришћени су софтвери SPSS (евалуациона верзија) и SmartPLS.

За проверу хипотезе H3, која говори о томе да безбедносни модул позитивно утиче на поверење у систем за е-учење, коришћене су методе дескриптивне статистике. Упитник је састојао из три категорије ставова о томе шта утиче на поверење у систем за е-учење, представљених са различитим бројем питања.

Категорије су следеће:

- репутација - говори о томе како спољашњи показатељи система утичу на перцепцију о поверењу
- садржај - говори о томе колико квалитет садржаја утиче на поверење
- безбедност - говори о томе колико елементи безбедности (имплементирани у самом модулу) утичу на поверење

Резултати су приказани на слици 49.



Слика 49 - Перцепција утицаја фактора е-учења на ставове о поверењу

Према добијеним вредностима види се да је модул, односно прелиминарни фактори које он представља и реализује, значајан као утицајан фактор за перцепцију поверења у систем за е-учење. Чак је значајнији од друга два испитана фактора.

Овај однос треба узети са одређеном дозом резерве, јер је у питању релативно мали узорак. Такође, Ликертова скала, коришћена за испитивање, није интервална, већ ординална скала, па узимање просечних вредности може изазвати одређена одступања. Међутим, с обзиром на то да искази имају 5 подеока, као и да су вредности значајно у крајњем позитивном смеру (чак изнад 4), може се оправдано закључити да овакви резултати не одступају значајно од оних који би се добили другим методама (медијан, мод итд.).

Варијабле које су груписане у факторе надаље су подвргнуте статистичкој провери, кроз факторску анализу, како би се утврдило да ли је фактор ”Безбедност” (који представља модул) хомоген или и он сам садржи посебне компоненте.

Факторском анализом, дошло се до закључка да поједини од дата три фактора могу да се прерасподеле на основу Varimax методе груписања. Мануелно је подешена вредност 3 и добијени су следећи фактори у ротираној таблици (табела 8).

Табела 8 - Аутоматско рефакторисање

Component Matrix[a]

	Component		
	1	2	3
РЕП1	**,726**	,405	-,165
РЕП2	**,708**	-,233	-,003
САДР1	,042	,390	**,531**
САДР2	,161	**,452**	,395
САДР3	**,581**	-,260	,049
САДР4	,201	**,539**	-,072
САДР5	,487	-,436	,462
САДР6	**,549**	-,006	,460
САДР7	,575	-,304	,540
БЕЗБ1	,401	**-,634**	-,237
БЕЗБ2	**,659**	-,295	-,347
БЕЗБ3	**,682**	,053	-,488
БЕЗБ4.	,437	**,700**	-,079
БЕЗБ5.	**,587**	,547	-,128

Према подацима из таблице (болдирани су елементи који су доминантни за одређену групу), може се закључити да су безбедносни елементи груписани углавном као и елементи ”Репутација”. Тачније, сви фактори се могу релативно лако прегруписати у само два фактора. Један би се могао назвати: ”окружење за

е-учење”, а други ”садржаји”. У том смислу елементи подржани од стране модула (БЕЗБ) се могу груписати заједно у фактор који дефинише амбијент за е-учење.

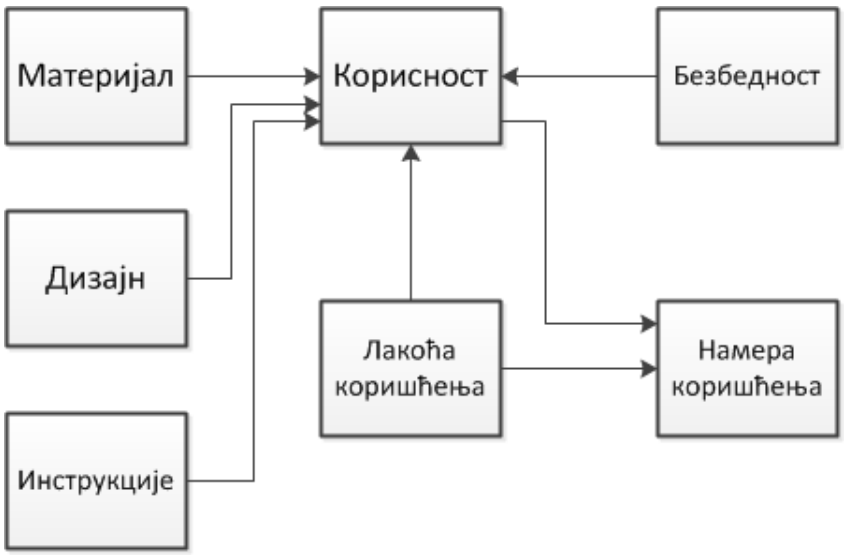
На основу наведеног се сумарно може закључити да фактор који представља безбедносни модул значајно утиче на поверење корисника у систем за е-учење, у склопу једног генералног фактора (названог ”окружење за е-учење”). Тиме је хипотеза Н3 потврђена.

За проверу хипотезе Н4, којом се претпоставља да модул позитивно утиче на прихваћеност, тестиране су две зависне променљиве: намера да се систем користи и лакоћа коришћења. Као независне, сложене променљиве узете су следеће:

- Карактеристика материјала
- Карактеристика инструкције
- Дизајн
- Безбедност

Фактор ”Безбедност” формиран је кроз 10 исказа везаних за активности модула. Ови искази су факторском анализом подељени на две групе (два фактора), од којих су узети искази 6-10, који су и логички непосредно везани за сам модул и перцепцију његовог дејства.

Независне променљиве које су провераване су: намера коришћења и лакоћа коришћења. Почетни модел је класични ТАМ, са додатим фактором ”Безбедност” и ”Инструкција”.



Слика 50 - Почетни теоријски модел

Модел (слика 50) је комбинација модела датих у [79], [80] и [140].

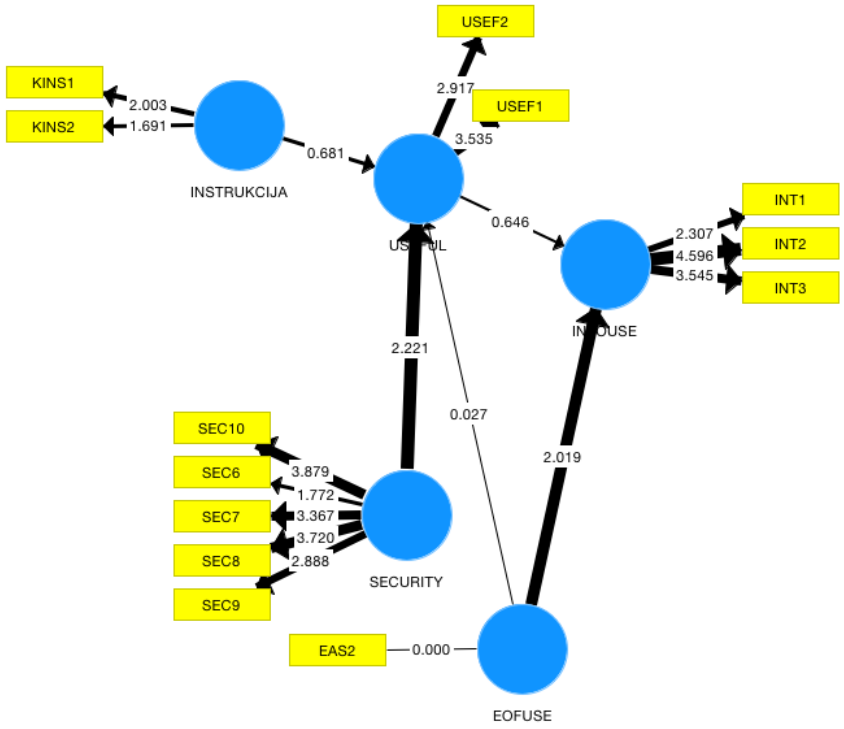
Иницијално су коришћени и фактори ”Квалитет материјала” и ”Дизајн”, али се они нису показали као статистички значајни, па су искључени (то је сугерисао и сам статистички софтвер током анализе).

Дескриптивна статистика дата је у прилогу (13.4).

За анализу је коришћен пакет SmartPLS [141]. Овај софтвер се користи код структурних модела (SEM - Structure Equation Model) и прорачуне заснива на методи најмањих квадрата. SmartPLS је коришћен из следећих разлога:

- узорак је мали
- постоји комплексна веза међу факторима у моделу
- основна верзија софтвера је бесплатна за некомерцијалну употребу

Променљиве које чине факторе су тестиране на Cronbach Alpha и Pearson у алату SPSS, затим је формиран модел у SmartPLS и уклоњене варијабле које имају слабу тежину (Loadings). Добијен је следећи статистички модел (слика 51).



Слика 51 - Резултат анализе у SmartPLS (t-вредности)

Са INTOFUSE означена је намера коришћења, а са EOFUSE лакоћа и са USEFUL (други фактор слева) корисност.

Вредности коефицијената представљени су таблицом (Табела 9).

Табела 9 - Статистички резултати тестирања модела

	Просек (Mean)	Стандардна девијација	t - вредност	p-вредност
EOFUSE->INTOUSE	0,400	0,205	2,019	0,044
EOFUSE->USEFUL	-0,046	0,354	0,027	0,978
INSTRUKCIJA->USEFUL	-0,087	0,234	0,681	0,496
SECURITY->USEFUL	0,550	0,265	2,221	0,027
USEFUL->INTOUSE	0,204	0,263	0,646	0,519

За пет фактора софтвер је генерисао одговарајуће статистичке параметре.

Прегледом p-вредности, може се установити да је њена значајност у погледу одбацивања нулте хипотезе присутна у 2 случаја, односно код два фактора:

EOFUSE (лакоћа коришћења) и SECURITY (безбедносни фактор), јер је у та два случаја мања од 0,05. Код првог је то 0,044, док је код другог 0,027. Праг (ниво значајности) од 0,05 је у истраживачкој пракси праг (ниво α) код којег се може одбацити нулта хипотеза [142].

Модел није у потпуности доказао почетне претпоставке самог TAM-а, међутим треба имати у виду да везе између лакоће коришћења и намере коришћења нису нужно присутне, тј. поједина истраживања их негирају, како је то наведено у [143].

Може се констатовати да је утицај фактора ”Безбедност” (SECURITY), који представља ставове непосредно везане за сам модул, значајан, судећи према p-вредностима и да је нулта хипотеза о утицају модула на корисност (перцепцију корисности) система оповргнута.

Узимајући у обзир непотпуну потврђеност самог модела, као и добијене резултате, може се констатовати да је хипотеза H4 делимично подржана.

Неопходно је оставити одређен простор и у будућим истраживањима размотрити различите варијанте TAM модела и потенцијалних утицаја на већем узорку, како би се добили тачнији и релевантнији резултати (такође, обезбедити расподелу што ближу нормалној), па је према томе оправдано прогласити хипотезу делимично потврђеном.

10.2 Остале повратне информације

Приликом коришћења сајта и самог курса, корисници су имали могућност да решавају тест којим се проверава безбедносна свест. Овај тест није обавезан, већ се појављује повремено у оквиру блока, као опција. Уколико корисник одлучи да решава тест, то ће утицати на његов капацитет, тј. ажурираће се безбедносни профил. Тест се може решавати неограничен број пута, уз задату минималну паузу између више покушаја. Тест су решавала 23 корисника и при том је остварен просечан успех **7,73** (од 10). Укупан број покушаја је 34. То показује да су корисници били заинтересовани да побољшају свој скор - самостално иницирајући поновне покушаје решавања.

Корисници су изнели различите позитивне утиске везане за сам сајт и курс, међутим није било посебних назнака да су студенти препознали да је сам сајт безбеднији од сајта који иначе користе за е-учење.

Поједини корисници имали су проблем са аутентификацијом, који је директно проузрокован радом модула. Проблем је настао тако што је њихов тип аутентификације промењен на 2-факторски, уз слање одговарајуће

информације како се пријавити уз додатну информацију (токен). Међутим, пошто је предвиђено да се токен генерише са Android уређаја, корисници који имају неки други систем, остали су ускраћени за ту информацију. На крају су самостално открили како се и преко PC-а може генерисати токен. Овај случај је још један индикатор о потреби олакшавања приступа безбедносним контролама.

Са друге стране, у отвореним одговорима корисника (нису били обавезни, али их је попунило неколико испитаника) готово да није поменут безбедносни аспект. Ова чињеница фактички је и очекивана, јер сам модул ради са веома мало интеракције, све додатне информације (на пример да је потребно да се корисник одјави или ”како креирати квалитетну лозинку”) остављене су на начин на који нису наметнуте. Са друге стране, без обзира на такав приступ, корисници су сами, без икакве сугестије, имали унутрашњи мотив да иницирају решавање теста о познавању безбедносних механизама.

10.3 Закључци евалуације

Евалуацијом се завршава ”Check" фаза пројектовања модула. У фази планирања дефинисан је делокруг и креиран модел, у другој фази је имплементиран као део Moodle система, док су кроз Евалуацију анализирани утицаји модула на два битна конструкта, а то су поверење и прихваћеност технологије.

Утврђено је да се безбедносни модул и његове функције не могу једноставно класификовати као независтан фактор, већ да је његово деловање тесно повезано са неким другим факторима који утичу и на поверење и на прихваћеност, као што је нпр. репутација, те да могу чинити нови сложен фактор (нпр. ”окружење за е-учење”). Може се закључити да у тим самим факторима безбедносни модул игра значајну улогу и да његове функције доприносе поверењу у систем и прихваћености. Са друге стране, неопходно је даље истражити моделе који би могли боље да опишу безбедносне аспекте сложених система, какав је нпр. систем за управљање е-учењем.

Техничка релизација самог модула такође може и мора бити предмет ревизије: почевши од имплементације нових функције, па до олакшавања приступу безбедносним контролама. Овим разматрањем дефинишу се и наредни кораци у фази "Act", који подразумевају унапређење постојећих функција и исправљање уочених грешака. Одређени елементи ове фазе наведени су и у наредном поглављу, у склопу идеја за будући рад.

11. Закључна разматрања и будући рад

Задатак који је стављен пред ову тезу испоставио се као озбиљан изазов превасходно из разлога мултидисциплинарности теме. Безбедност информација је већ научна област која је мултидисциплинарног карактера и ”укрштање” са другим сложеним концептом (е-образовање), па онда и са квалитетом изискивало је опсежну анализу литературе и обимно истраживање модела.

Постојање великог броја стандарда у е-образовању може се окарактерисати као ”мач са две оштрице”. Са једне стране отвара се низ могућности за примену, а са друге разноврсност спецификација и стандарда може унети конфузију и отежати имплементацију. Такође, општи међународни стандарди из области безбедности (серија ISO 27000) показали су се као изузетно корисни и приликом пројектовања овог модула. Не само што ISO стандарди прописују методологију развоја безбедносног информационог система (примењиву у различитим окружењима), већ постоји и скуп конкретних метода заштите, који су искоришћени за сам модул. Може се закључити да се општи стандарди и стандарди из области е-образовања могу искористити као оквир за пројектовање безбедносне подршке у процесима е-образовања. Да би то било могуће, неопходно је извршити анализу стандарда и њихову систематизацију, као и избор одговарајуће спецификације. Ова подршка реализована је у виду модула елемента који чини градивни део система за е-учење.

Осим анализе стандарда, у раду је дата и анализа модела квалитета у е-образовању, а посебна пажња је посвећена шемама које се баве обезбеђењем квалитета. Током пројектовања модула, у обзир су узети поједини критеријуми обезбеђења квалитета који су посебно издвојени. Ови критеријуми су имплементирани у самом модулу, чиме је он установљен као елемент који утиче на обезбеђење квалитета. Такође, закључено је да шеме квалитета изискују ревизију критеријума који се баве безбедношћу. Они који су тренутно присутни у већини шема нису комплетни, а и оправданост појединих критеријума је под знаком питања (на пример ”single sign on" аутентификација).

Све време идеја водиља у овој тези био је је ”холистички приступ”. Начињен је покушај да се што опсежније обухвате и презентују разноврсни фактори који утичу на безбедност у овој специфичној варијанти е-пословања. Анализом различитих безбедносних архитектура и применом у окружењу процеса е-образовања, формирана је безбедносна архитектура seLTSA. Поента ове надграђене архитектуре је да интегрише функције безбедности у процесе е-образовања и формулише место безбедносног модула као елемента који

оркестрира процесима безбедности. Ова архитектура (seLTSA) један је од кључних доприноса теме из следећих разлога:

- представља иновацију једног општеприхваћеног генеричког модела
- пружа везу ка наредном веома битном резултату тезе, а то је креирање самог безбедносног модула
- даје основу за изградњу сличних архитектура у окружењима других пословних процеса

Надоградња стандарда IMS LIP (модела ученика) је још један значајан резултат тезе. Ово проширење извршено је на основу више улазних параметара: на основу актуелних истраживања у пољу, на основу студије случаја и на основу анализе стандарда. Модел је проширен једноставном структуром, која је (на основу поменутих улазних параметара) усвојена као довољна за функционалност модула, чија функционалност се управо једним делом заснива на овом моделу.

За имплементацију модула изабран је Moodle. Показало се да природа модула изискује додатне елементе да би се потребне функционалности имплементирале и да није могуће направити модул потпуно модуларним, у пуном смислу те речи. Овај проблем је најбоље превазићи активним суделовањем у развоју самог основног Moodle система и стварањем основа за једноставнију имплементацију модула који захтевају одређене системске функције блиске језгру.

Модул је развијан кроз PDCA методологију. На овај начин јасно су разграничене активности у оквиру развоја модула и дефинисан кружни ток, који одговара континуалној природи саме безбедности. Показано је да се одговарајућим прилагођавањем PDCA може ефикасно применити на развој једног специфичног елемента, као што је безбедносни модул, чија финална реализација јесте у склопу система за е-учење.

Рад модула се показао као потпуно транспарентан за корисника. Тачније, приликом самог рада на систему, корисници нису имали фактички никаквих препрека узрокованих модулом, а са друге стране показали су значајно интересовање за елементе који су им доступни, нпр. за тест безбедности. Ова појединост иде у прилог претпоставци, која је од самог почетка уврштена у концепцију модула: унапређење безбедности кроз елемент који је добро интегрисан и хармонизован у функционалност самог система за учење. У овој ситуацији може значајан бити и елемент учења заснованог на игри, што није нов концепт у истраживањима о безбедности [144], [145].

Допринос тезе исказује се и кроз резултате истраживања о томе како безбедност утиче на поверење корисника у систем за е-учење и на прихваћеност технологија, што су конструкти који су повезани и са квалитетом. Кроз емпиријско истраживање и коришћењем прилагођених модела из литературе, уз одговарајуће статистичке процедуре установљено је да је безбедност, чији чиниоци фигуришу кроз модул интегрисан у систему за е-учење, значајан фактор. Показано је да се безбедност може уврстити у постојеће моделе, као што је TAM, али и да је потребно додатно истражити какав би то нови модел (или модификација постојећих) боље описао констелацију фактора који фигуришу у процесима е-учења.

Као резултати истраживања о утицајима безбедносног модула на поверење и прихваћеност технологија може се издвојити следеће:

- Установљено је да је утицај безбедносног модула на поверење значајан.
- Установљено је да фактор који представља безбедносни модул има своје место у сложенијем фактору, пошто значајно корелира са чиниоцима фактора ”репутација”
- Креиран је модификован TAM, после тестирања почетног модела и уклањањем појединих фактора након статистичне анализе.
- Дата је основа за даље теоријско и емпиријско истраживање нових модела (и поверења и прихватања технолофија) који би формулисали безбедност као посебан фактор или као део других комплекснијих фактора.

Иако је рад изнедрио доприносе у области мултидисциплинарних истраживања безбедности информација и расветлио како интеграција безбедности може утицати на е-учење, неопходно је скренути пажњу и на одређене ”слабе тачке” истраживања. Прва ”слабост” односи се на третирање самог е-образовања. У раду је разматран један типичан сценарио и веома популаран инфраструктурни и техничко/дидактички модус - е-учење коришћењем платформе и такав сценарио је обрађен специјализацијом кроз конкретан LMS Moodle. Међутим, е-образовање не мора нужно подразумевати примену оваквог сценарија. У најширем контексту, овај рад се може третирати као *proof of concept*, доказ да је разматрање безбедности могуће на модуларан начин, којем је корисник на првом месту. Конкретне имплементације у другим сценаријима могу се ослонити на основни концепт модула, који је дат у овом раду.

Модели квалитета, поверења и прихваћености технологија адаптирани су на основу примера из литературе. Међутим, чињеница да је одређени модел подржан у одређеном окружењу, не повлачи нужно да ће бити доказан и у неком другом. За то разлози могу лежати на најразноврснијим местима: од

културолошких до техничких специфичности. Уосталом, и студија случаја приказала је резултате из Србије, који се сигурно разликују од нпр. резултата из Норвешке или Јужне Кореје. За валидније резултате неопходан је и већи узорак, а идеално би било да је модул имплементиран у свакодневној, регуларној настави, тј. њеној е-компоненти, са више стотина студената. Онда би било могуће више експериментисати са различитим варијантама модела и пронаћи онај који најбоље описује дати контекст и уопште ширу природу феномена званог е-образовање.

Будући рад

Ова дисертација отворила је читаву раскрсницу путева за будућа истраживања: за самог аутора и све оне који су заинтересовани за ову област. Следе таксативно набројане неке од идеја:

- Формирање нових модела е-образовања који садрже безбедност као фактор (модел квалитета, задовољства...)
- Формирање и тестирање нових модификација TAM-а.
- Имплементација нових могућности (feature) у eLearnion-у.
- Примена напредних метода обраде података (рударење података, машинско учење) и метода вештачке интелигенције за рад модула.
- Увођење нових елемената учења заснованог на игри у сврху унапређења безбедности корисника и тестирање успешности оваквог приступа.
- Интеграција свих функција безбедности (постојећих и нових метода) ради управљања кроз један административни модул који би могао да генерише и одговарајуће извештаје.

Оно што би се могло издвојити као посебан изазов за будући рад је креирање сличног, општијег модела и одговарајуће архитектуре који би се могли применити у било ком информационом систему. Данас чак и најмање фирме користе неку варијанту пословног информационог система и интеграција безбедности кроз модул који би пратио активности корисника, надгледао и тестирао његову безбедносну свест, дисеминирао безбедносну политику и спроводио различите мере заштите, реална је опција за менаџмент и развојне тимове који се баве информационим системима

12. Литература

[1] S. Yahya, E. A. Ahmad, K. A. Jalil, and U. T. Mara, “The definition and characteristics of ubiquitous learning : A discussion,” *International Journal of Education and Development using Information and Communication Technology*, vol. 6, no. 1, pp. 1–12, 2010.

[2] “СТАНДАРД SRPS ISO / IEC 27001,” vol. 2014. Институт за стандардизацију Србије, Београд, 2014.

[3] G. E. Violettas, T. L. Theodorou, and G. C. Stephanides, “E-Learning Software Security: Tested for Security Vulnerabilities & Issues,” in *2013 Fourth International Conference on e-Learning “Best Practices in Management, Design and Development of e-Courses: Standards of Excellence and Creativity,”* 2013, pp. 233–240.

[4] S. Lineberry, “The Human Element: The Weakest Link in Information Security,” *Journal of Accountancy*, vol. 204, pp. 44–49, 2007.

[5] R. Woerner, “Fixing the weakest link in your security chain : People,” *Security Magazine*, no. December, pp. 60–62, 2012.

[6] J. T. Holden and P. J. L. Westfall, “AN INSTRUCTIONAL MEDIA SELECTION GUIDE FOR DISTANCE LEARNING,” 2009. [Online]. Available: http://www.calvin.edu/~dsc8/documents/IMSGDL-5thRev-NDLW.pdf. [Accessed: 08-Jul-2013].

[7] “Oxford Dictionary,” 2014. [Online]. Available: http://www.oxforddictionaries.com/.

[8] ITU-T, “Security Architectures for Open Systems Interconnection for CCITT Applications X.800,” 1991. [Online]. Available: http://www.itu.int/rec/T-REC-X.800-199103-I. [Accessed: 01-Jan-2013].

[9] I. Standard, “INTERNATIONAL STANDARD ISO / IEC techniques — Code of practice for,” vol. 2005, 2005.

[10] Microsoft, “The Stride Threat Model,” 2002. [Online]. Available: https://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx. [Accessed: 01-Jan-2015].

[11] B. Chen and A. Denoyelles, “Exploring Students’ Mobile Learning Practices in Higher Education,” *Educause Review Online*, pp. 1–9, 2013.

[12] Š. Hošková-Mayerová and Z. Rosická, “E-Learning Pros and Cons: Active Learning Culture?,” *Procedia - Social and Behavioral Sciences*, vol. 191, no. 0, pp. 958–962, 2015.

[13] S. Hrastinski, “Asynchronous and Synchronous E-Learning,” *Educause Quarterly*, vol. 31, pp. 51–55, 2008.

[14] M. Oztok, D. Zingaro, C. Brett, and J. Hewitt, “Exploring asynchronous and synchronous tool use in online courses,” *Computers & Education*, vol. 60, no. 1, pp. 87–94, Jan. 2013.

[15] C. R. Graham, “Introduction to Blended Learning,” *Handbook of blended learning Global perspectives local designs*, 2006. [Online]. Available: http://www.publicationshare.com/graham_intro.pdf. [Accessed: 01-Apr-2016].

[16] “The Open University Annual Report,” 2012. [Online]. Available: http://www.open.ac.uk/about/main/files/aboutmain/file/ecms/web-content/OU-Annual-Report-2011-12.pdf.

[17] R. Ellaway, “E-learning: Is the revolution over?,” *Medical Teacher*, vol. 33, no. 705, pp. 297–302, 2011.

[18] RATEL, “Pregled tržišta komunikacija u Republici Srbiji u 2013. godini,” 2014. [Online]. Available: http://www.ratel.rs/upload/documents/Pregled_trzista/Ratel Pregled trzista 2014.pdf.

[19] A. Mishra and D. Mishra, “E-LEARNING EXPERIENCE AT VARIOUS UNIVERSITIES: ACADEMICS PERSPECTIVE,” *Tehnički vjesnik*, vol. 1, no. 18, pp. 133–140, 2011.

[20] Á. F. Agudo-Peregrina, S. Iglesias-Pradas, M. Á. Conde-González, and Á. Hernández-García, “Can we predict success from log data in VLEs? Classification of interactions for learning analytics and their relation with performance in VLE-supported F2F and online learning,” *Computers in Human Behavior*, vol. 31, pp. 542–550, Feb. 2014.

[21] B. C. Czerkawski, “When Learning Analytics Meets E-Learning,” *Online Journal of Distance Learning Administration*, vol. XVIII, no. 2, 2015.

[22] M. Peeters, K. van den Bosch, J.-J. C. Meyer, and M. A. Neerincx, “The design and effect of automated directions during scenario-based training,” *Computers & Education*, vol. 70, pp. 173–183, Jan. 2014.

[23] I. Milošević, D. Živković, D. Manasijević, and D. Nikolić, “The effects of the intended behavior of students in the use of M-learning,” *Computers in Human Behavior*, vol. 51, pp. 207–215, Oct. 2015.

[24] A. Garcia-Cabot, L. de-Marcos, and E. Garcia-Lopez, “An empirical study on m-learning adaptation: Learning performance and learning contexts,” *Computers & Education*, vol. 82, pp. 450–459, Mar. 2015.

[25] J. Carmigniani, B. Furht, M. Anisetti, P. Ceravolo, E. Damiani, and M. Ivkovic, “Augmented reality technologies, systems and applications,” *Multimedia Tools and Applications*, vol. 51, no. 1, pp. 341–377, 2011.

[26] J. Martín-Gutiérrez, P. Fabiani, W. Benesova, M. D. Meneses, and C. E. Mora, “Augmented reality to promote collaborative and autonomous learning in higher education,” *Computers in Human Behavior*, vol. 51, pp. 752–761, Oct. 2015.

[27] J. DeNeen, “30 Myths About eLearning That Need To Die In 2013,” 2013. [Online]. Available: http://www.opencolleges.edu.au/informed/features/30-myths-about-elearning-that-need-to-die-in-2013/. [Accessed: 01-Jan-2015].

[28] T. Anderson, *The Theory and Practice of Online Learning*, 2nd ed., vol. 36, no. 1. Edmonton: AU Press, 2008.

[29] A. Al-adwan and J. Smedley, “Implementing e-learning in the Jordanian Higher Education System: Factors affecting impact.,” *International Journal of Education & Development using Information & Communication Technology*, vol. 8, no. 1, pp. 121–135, 2012.

[30] “DL@Web,” 2011. [Online]. Available: http://www.dlweb.kg.ac.rs/. [Accessed: 01-Jan-2015].

[31] V. Florjančić, R. Krneta, M. Milošević, R. Malčeski, S. Loškoska, V. Devedžić, L. Fedeli, P. Đ. Rosi, D. Bjekić, M. Bajčetić, M. Devedžić, M. Stanković, V. Caraguel, B. Krstajić, and A. Radulović, *Priručnik za učenje na daljinu sa primerima iz prakse*. Podgorica: Univerzitet Crne Gore, 2014.

[32] КАПК, “Упутства за припрему документације за акредитацију студијских програма који се реализују учењем на даљину,” 2013. [Online]. Available: http://www.kapk.org/images/stories/dokumentacija/Uputstvo za pripremu dokumentacije za akreditaciju programa za ucenje na daljinu.pdf. [Accessed: 01-Jan-2016].

[33] R. Krneta, B. Milovanović, and D. Milošević, “ANALIZA STANDARDA, PREPORUKA I UPUTSTAVA ZA AKREDITACIJU STUDIJA NA DALJINU U SRBIJI,” in *Informacione tehnologije - IT 2011*, 2011, pp. 54–58.

[34] B. von Solms and R. von Solms, “The 10 deadly sins of information security management,” *Computers & Security*, vol. 23, no. 5, pp. 371–376, Jul. 2004.

[35] E. R. Weippl, *Security in e-learning*. New York, NY: Springer, 2005.

[36] K. El-khatib, L. Korba, Y. Xu, and G. Yee, “Privacy and Security in E-Learning,” *International journal of Distance Education*, vol. 1, no. 4, 2003.

[37] D. C. Luminita, “Information security in E-learning Platforms,” *Procedia - Social and Behavioral Sciences*, vol. 15, pp. 2689–2693, 2011.

[38] S. R. Masadeh, N. Turab, and F. Obisat, “A secure model for building e-learning systems,” *Network Security*, vol. 2012, no. 1, pp. 17–20, Jan. 2012.

[39] C. Gil, M. Castro, and M. Wyne, “Computer Security Threats Towards the E-Learning System Assets,” in *Frontiers in Education Conference*, J. Mohamad

Zain, W. M. bt W. Mohd, and E. El-Qawasmeh, Eds. 2011, pp. 335–345.

[40] R. Raitman and N. Augar, “Security in the Online E-learning Environment,” no. Davis 2004, 2005.

[41] B. Jerman-Blažič and T. Klobučar, “Privacy provision in e-learning standardized systems: status and improvements,” *Computer Standards & Interfaces*, vol. 27, no. 6, pp. 561–578, Jun. 2005.

[42] C. G. Webber, M. D. F. W. P. Lima, M. E. Casa, and A. M. Ribeiro, “Towards Secure e-Learning Applications : a Multiagent Platform,” *Journal of Software*, vol. 2, no. 1, pp. 60–69, 2007.

[43] J. Yong, “Security and Privacy Preservation for Mobile E-Learning via Digital Identity Attributes,” vol. 17, no. 2, pp. 296–310, 2011.

[44] M. Tedre and B. Chachage, “University Students’ Attitudes Towards e-Security Issues: A Survey Study in Tumaini Universi ty, Tanzania,” in *TEDC 2008 Proceedings - Technology for Innovation and Education in Developing Countries:*, 2008.

[45] M. Milošević, D. Milošević, and R. Krneta, “Sigurnost i privatnost u online okruženju na Tehničkom fakultetu u Čačku,” in *TEHNIKA I INFORMATIKA U OBRAZOVANJU*, 2012.

[46] E. Marais, D. Argles, and B. von Solms, “Security Issues Specific to e-Assessments,” in *8th Annual Conference on WWW Applications*, 2006.

[47] C. Gil, M. Castro, and M. Wyne, “Identification in web evaluation in learning management system by fingerprint identification system,” in *2010 IEEE Frontiers in Education Conference (FIE)*, 2010, p. T4D–1–T4D–6.

[48] N. Chiranji, C. Depthi, and T. P. Shekhar, “A Novel Approach to Enhance Security for Online Exams,” *IJCST*, vol. 2, no. 3, pp. 84–89, 2011.

[49] C. J. Eibl, “Discussion of Information Security in E-Learning,” University of Siegen, 2010.

[50] C. Ghaoui, *Usability evaluation of online learning programs*. Hershey: Idea Group Inc, 2003.

[51] M. Anwar and J. Greer, “Facilitating Trust in Privacy-Preserving E-Learning Environments,” *IEEE Transactions on Learning Technologies*, vol. 5, no. 1, pp. 62–73, 2012.

[52] K. Borcea, H. Donker, E. Franz, A. Pfitzmann, and H. Wahrig, “Towards privacy-aware eLearning,” in *Privacy Enhancing Technologies*, vol. 3856, 2006, pp. 167–178.

[53] M. M. Ramim and Y. Levy, “Securing e-learning systems: A case of insider cyber attacks and novice IT management in a small University,” *Journal of Cases on Information Technology*, vol. 8, no. 4, pp. 24–34, 2006.

[54] B. Y. D. Wang, “Building Trust in,” *Athens Journal of Education*, no. February, pp. 9–18, 2014.

[55] N. Hayaati, M. Alwi, and I. Fan, “E-Learning and Information Security Management,” *International Journal of Digital Society*, vol. 1, no. 2, pp. 148–156, 2010.

[56] A. C. Punnoose, “Determinants of intention to use eLearning based on the technology acceptance model,” *Journal of Information Technology Education:Research*, vol. 11, no. 1, pp. 301–337, 2012.

[57] J. Sarsa and R. Soler, “E-Learning Quality,” *International Journal of Information and Communication Technology Education*, vol. 8, no. 2, pp. 46–60, 2012.

[58] A. Donabedian, *Explorations in Quality Assessment and Monitoring*. Chicago: Health Administration Press, 1980.

[59] S. Marshall, “Improving the quality of e-learning: Lessons from the eMM,” *Journal of Computer Assisted Learning*, vol. 28, no. 1, pp. 65–78, 2012.

[60] ISO, “ISO 9000: Quality Management Systems - Fundamentals and Vocabulary.” 2005.

[61] C. Holsapple and a Lee-Post, “Defining, Assessing, and Promoting E-Learning Success: An Information Systems Perspective*,” *Decision Sciences Journal of …*, vol. 4, no. 1, pp. 67–85, 2006.

[62] H. Li and R. Suomi, “A Proposed Scale for Measuring E-service Quality,” *International Journal of u- and e-Service, Science and Technology*, vol. 2, no. 1, pp. 1–10, 2009.

[63] D. Masoumi and B. Lindström, “Quality in e-learning: a framework for promoting and assuring quality in virtual institutions,” *Journal of Computer Assisted Learning*, vol. 28, no. 1, pp. 27–41, 2012.

[64] Josua Tarigan, “Factors Influencing Users Satisfaction on E-Learning Systems,” *Jurnal Manajemen dan Kewirausahaan*, vol. 13, pp. 177–188, 2011.

[65] J. Ojasalo, “E-Service Quality : A Conceptual Model 2 . The Concept and Characteristics of E-Services,” *International journal of Arts and Sciences*, vol. 3, no. 7, pp. 127–143, 2010.

[66] EFQUEL, “UNIQUE Information Package,” 2011. [Online]. Available: http://unique.efquel.org/files/2012/09/UNIQUe_guidelines_2011.pdf. [Accessed: 01-Jan-2013].

[67] K. El Emam, *Spice: The Theory and Practice of Software Process Improvement and Capability Determination*, 1st ed. Los Alamitos, CA, USA: IEEE Computer Society Press, 1997.

[68] S. Marshall and G. Mitchell, “AN E-LEARNING MATURITY MODEL ?,” *InProceedings of the 19th Annual Conference of the Australian Society for Computers in Learning in Tertiary Education, Auckland, New Zealand*, 2002.

[69] Y. Kats, *Learning Management Systems and Instructional Design*. Hershey: IGI Global, 2013.

[70] C. L. Corritore, B. Kracher, and S. Wiedenbeck, “On-line trust: concepts, evolving themes, a model,” *International Journal of Human-Computer Studies*, vol. 58, no. 6, pp. 737–758, Jun. 2003.

[71] H. Mohammadi, “Investigating users’ perspectives on e-learning: An integration of TAM and IS success model,” *Computers in Human Behavior*, vol. 45, pp. 359–374, 2015.

[72] T. Grandison and M. Sloman, “A survey of trust in internet applications,” *IEEE Communications Surveys & Tutorials*, vol. 3, no. 4, pp. 1–30, 2000.

[73] A. Longheu, V. Carchiolo, M. Malgeri, and G. Mangioni, “Trust into e-Learning,” in *Encyclopedia of the Sciences of Learning SE - 1829*, N. Seel, Ed. Springer US, 2012, pp. 3350–3353.

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

[75] M. Ziaullah, Y. Feng, S. N. Akhter, and M. F. Khan, “An Empirical Study on Exploring Relationship among Information Quality, E-satisfaction, E-trust and Young Generation’s Commitment to Chinese Online Retailing,” *Journal of Competitiveness*, vol. 6, no. 4, pp. 3–18, 2014.

[76] V. Venkatesh, M. G. Morris, G. B. Davis, and F. D. Davis, “USER ACCEPTANCE OF INFORMATION TECHNOLOGY: TOWARD A UNIFIED VIEW.,” *MIS Quarterly*, vol. 27, no. 3, pp. 425–478, 2003.

[77] F. D. Davis, R. P. Bagozzi, and P. R. Warshaw, “User Acceptance of Computer Technology: a Comparison of Two Theoretical Models,” *Management Science*, vol. 35, no. 8, pp. 982–1003, 1989.

[78] F. Umrani-Khan and S. Iyer, “ELAM: A Model for Acceptance and Use of E-learning by Teachers and Students,” in *International Conference on eLearning*, 2008, pp. 475–485.

[79] B.-C. Lee, J.-O. Yoon, and I. Lee, “Learners’ acceptance of e-learning in South Korea: Theories and results,” *Computers & Education*, vol. 53, no. 4, pp. 1320–1329, 2009.

[80] 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*, vol. 12, no. 3, pp. 1–26, 2007.

[81] “ISO 27000,” 2013. [Online]. Available: http://www.27000.org. [Accessed: 01-Jan-2015].

[82] ISO, “СТАНДАРД SRPS ISO / IEC 27001.” Институт за стндардизацију Србије, Београд, 2014.

[83] BSI, “PD ISO / IEC TR 27008 : 2011 BSI Standards Publication Information Technology — Security techniques — Guidlines for auditors on information security controls,” 2011.

[84] “ITU-T Recommendations.” [Online]. Available: http://www.itu.int/ITU-T/recommendations/index.aspx?ser=X. [Accessed: 10-Jun-2015].

[85] C. Schultz, “Information Security Trends and Issues in the Moodle E-Learning Platform: An Ethnographic Content Analysis,” *Journal of Information Systems Education*, vol. 23, no. 4, pp. 359–371, 2012.

[86] L. E. Anido-Rifón, M. J. Fernández-Iglesias, M. Caeiro-Rodríguez, J. M. Santos-Gago, M. Llamas-Nistal, L. Álvarez Sabucedo, and R. Míguez Pérez, “Standardization in computer-based education,” *Computer Standards & Interfaces*, vol. 36, no. 3, pp. 604–625, Mar. 2014.

[87] IEEE, “IEEE Standards IEEE Standard for Learning TEchnology - Learning TEchnology Systems Architecture (LTSA),” *IEEE Standards*, vol. 9, no. December. IEEE, pp. 5–8, 2003.

[88] L. Technology and S. Architecture, “LTSA Specification,” pp. 1–176, 1998.

[89] F. Farance, F. Farance, J. Tonkel, and J. Tonkel, “IEEE P1484.1/D9, 2001-11-30 Draft Standard for Learning Technology - Learning Technology Systems Architecture (LTSA),” pp. 1–120, 2001.

[90] IMS, “Find out more about IMS.” [Online]. Available: https://www.imsglobal.org/aboutims.html. [Accessed: 01-Jan-2016].

[91] V. F. Specification, “IMS Learner Information Package Summary of Changes,” *Learning*, no. January, pp. 1–29, 2005.

[92] C. Smythe, F. Tansey, and R. Robson, “IMS learner information package information model specification,” *Final Specification Version*, 2001.

[93] D. W. Group, “EduPerson Specification (200312) EduPerson Object Class Specification (200312) Status of this document,” pp. 1–34, 2003.

[94] T. K. Shih and J. C. Hung, *Future directions in distance learning and communications technologies*. Hershey, PA: Idea Group Pub, 2007.

[95] D. Šćepanović, U. Marjanović, and J. Radišić, “Digitalno i onlajn učenje u Srbiji: Visoko obrazovanje,” in *XXII Skup Trendovi razvoja: Nove tehnologije u nastavi*, 2016, pp. 15–18.

[96] “Registered Moodle sites,” 2012. [Online]. Available: https://moodle.net/sites/. [Accessed: 01-Dec-2012].

[97] M. Dougiamas, “Moodle,” 2011. [Online]. Available: https://download.moodle.org/releases/legacy/.

[98] J. H. P. Eloff and M. M. Eloff, “Information security architecture,” *Computer Fraud & Security*, no. November, pp. 10–16, 2005.

[99] J. K. Tudor, *Information security architecture: an integrated approach to security in the organization*, 2nd ed. Boca Raton, FL: Auerbach Publications, 2006.

[100] Bsi, “ISO/IEC 27001 - Information Security Management - Transition guide,” 2013.

[101] “ЗАКОН О ИНФОРМАЦИОНОЈ БЕЗБЕДНОСТИ,” 2016. [Online]. Available: http://www.parlament.gov.rs/upload/archive/files/cir/pdf/zakoni/2016/3515-15.pdf.

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

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

[104] J. Rees, S. Bandyopadhyay, and E. Spafford, “PFIRES: a policy framework for information security,” *Communications of the ACM*, vol. 46, pp. 101–106, 2003.

[105] J. Rees, S. Bandyopadhyay, and E. Spafford, “PFIRES: a policy framework for information security,” *Communications of the ACM*, vol. 46, no. 7, pp. 101–106, 2003.

[106] J. McCumber, *Assessing and managing security risk in IT systems: a structured methodology*. Boca Raton, FL: Auerbach Publications, 2005.

[107] J. Sherwood, C. Andrew, and D. Lynas, “A roadmap to develop enterprise security architecture.” SABSA, 2009.

[108] M. Wilson, J. Hash, and C. S. Division, “Building an Information Technology Security Awareness and Trainig Program,” no. October, 2003.

[109] M. Milošević and D. Milošević, “INFORMATION SECURITY IN E-LEARNING : THE MATTER OF QUALITY,” in *Preceedings, eLearning Conference 2013*, 2013, no. September, pp. 26–27.

[110] X. Z. X. Zhao, X. W. X. Wan, and T. Okamoto, “Adaptive Content Delivery in Ubiquitous Learning Environment,” *Wireless, Mobile and Ubiquitous Technologies in Education (WMUTE), 2010 6th IEEE International Conference on*, 2010.

[111] “Закон о високом образовању.” Службени гласник, Београд, 2015.

[112] S. Ribarić, B. Dalbelo Bašić, Z. Kalafatić, T. Hrkać, and I. Fratrić, “System for Biometric Authorization of Internet Users Based on Fusion of Face and Palmprint Features,” 2005. [Online]. Available: http://www.zemris.fer.hr/projects/Biometrics/english/results.shtml. [Accessed: 12-Dec-2014].

[113] A. Armando, R. Carbone, L. Compagna, J. Cuéllar, G. Pellegrino, and A. Sorniotti, “An authentication flaw in browser-based Single Sign-On protocols: Impact and remediations,” *Computers & Security*, vol. 33, pp. 41–58, Mar. 2013.

[114] W. Capone, “SCORM Sharable Content Object Reference Model,” *Info*, 2004.

[115] T. Buzan and B. Buzan, “The Mind Map Book,” in *The Mind Map Book How to Use Radiant Thinking to Maximize Your Brains Untapped Potential*, 1994, p. Buzan Organization.

[116] E. Aimeur, H. Hage, F. Serge, and M. Onana, “A Framework for Privacy-Preserving E- learning,” vol. 238, pp. 223–238, 2007.

[117] N. C. Rowe, “Cheating in Online Student Assessment : Beyond Plagiarism,” *Online Journal of Distance Learning Administration*, vol. 7, pp. 1–10, 2004.

[118] J. Bailie and M. Jortberg, “Online learner authentication: Verifying the identity of online users,” *Journal of Online Learning and Teaching*, vol. 5, no. 2, p. 25, 2009.

[119] M. E. Whitman, “Security Policy: From Design to Maintenance,” *Advances in Management Information Systems*, vol. 11, pp. 123–151, 2008.

[120] J. Dominick, “Information Security Policy,” 2015. [Online]. Available: https://www.princeton.edu/oit/it-policies/it-security-policy/Documents/Information_Security_Policy.pdf. [Accessed: 20-Jan-2016].

[121] A. W. Compliance, “Washington University in St . Louis About WUSTL Compliance & Policies Information Security Policy.”

[122] M. Bruhn and R. Petersen, *Policy Development for Information Security*. 2003.

[123] M. Milošević and D. Milošević, “Defining the e-learner’s security profile: Towards awareness improvement,” *Sadhana*, pp. 1–10, 2016.

[124] A. R. Baker, B. Caswell, M. Poor, S. Northcutt, R. Alder, J. Babbin, J. Beale, A. Doxtater, J. C. Foster, T. Kohlenberg, and M. Rash, *Snort 2.1 Intrusion Detection*. 2004.

[125] A. a. Cardenas, P. K. Manadhata, and S. P. Rajan, “Big Data Analytics for Security,” *IEEE Security & Privacy*, vol. 11, no. 6, pp. 74–76, 2013.

[126] C. Sanders and J. Smith, “The Practice of Applied Network Security Monitoring,” *Applied Network Security Monitoring*, no. October, pp. 1–24, 2014.

[127] M. Milošević and D. Milošević, “Praćenje kao element bezbednosne arhitekture sistema za e-učenje,” in *Zbornik radova naučno-stručnog skupa sa međunarodnim učešćem Tehnika i informatika u obrazovanju – TIO 2014*, 2014.

[128] A. Brown and G. Wilson, *The Architecture of Open Source Applications, Volume II*. 2012.

[129] M. Dougiamas, “Moodle Plugin Types,” 2015. [Online]. Available: https://docs.moodle.org/dev/Plugin_types. [Accessed: 01-Jan-2015].

[130] D. Miletić, *Moodle security: learn how to install and configure {Moodle} in the most secure way possible*. Birmingham: Packt Publ, 2011.

[131] M. Milošević, D. Pleskonjić, and D. Milošević, “Sigurnost sistema za upravljanje učenjem,” in *Zbornik radova XVI Naučno-stručnog skupa Informacione tehnologije - sadašnjost i budućnost*, 2011, pp. 49–54.

[132] S. Battat, “A2FA,” 2014. [Online]. Available: https://moodle.org/plugins/pluginversions.php?plugin=auth_a2fa.

[133] D. Hardt, “The OAuth 2.0 Authorization Framework,” *Internet Requests for Comments*, 2012. .

[134] R. Wang, S. Chen, and X. Wang, “Signing Me onto Your Accounts through Facebook and Google: A Traffic-Guided Security Study of Commercially Deployed Single-Sign-On Web Services,” *2012 IEEE Symposium on Security and Privacy*, pp. 365–379, May 2012.

[135] S. Franklin and A. Graesser, “Is It an agent, or just a program?: A taxonomy for autonomous agents,” in *Intelligent Agents III Agent Theories, Architectures, and Languages SE - 2*, vol. 1193, J. Müller, M. Wooldridge, and N. Jennings, Eds. Springer Berlin Heidelberg, 1997, pp. 21–35.

[136] S. Furnell, “Usability versus complexity – striking the balance in end-user security,” *Network Security*, vol. 2010, no. 12, pp. 13–17, Dec. 2010.

[137] M. Milošević and D. Milošević, “SECURITY IN E-LEARNING : INTEGRATED USER-CENTRIC APPROACH,” in *eLearning Conference 2015*, 2015, pp. 126–130.

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

[139] “NetBeans,” 2015. [Online]. Available: https://netbeans.org.

[140] B. M. H. M. P. G. P. Sumak, “Factor affecting acceptance and use of moodle: An Empirical Study Based on ATM,” *Informatica*, vol. 35, pp. 91–100, 2009.

[141] K. K. Wong, “28/05 - Partial Least Squares Structural Equation Modeling (PLS-SEM) Techniques Using SmartPLS,” *Marketing Bulletin*, vol. 24, pp. 1–32, 2013.

[142] J.-B. du Prel, G. Hommel, B. Röhrig, and M. Blettner, “Confidence Interval or P-Value?: Part 4 of a Series on Evaluation of Scientific Publications,” *Deutsches Ärzteblatt International*, vol. 106, no. 19, pp. 335–339, May 2009.

[143] A. Tarhini, K. Hone, and X. Liu, “Factors Affecting Students’ Acceptance of e-Learning Environments in Developing Countries: A Structural Equation Modeling Approach,” *International Journal of Information and Education Technology*, vol. 3, no. 1, pp. 54–59, 2013.

[144] J. Abawajy, “User preference of cyber security awareness delivery methods.,” *Behaviour & Information Technology*, vol. 33, no. 3, pp. 236–247, 2014.

[145] S. Sheng and B. Magnien, “Anti-phishing phil: the design and evaluation of a game that teaches people not to fall for phish,” *In Proceedings of SOUPS 2007*, pp. 88–99, 2007.

13. Прилози

13.1 Политика коришћења система

Право приступа

Право приступа Систему за е-учење имају студенти и наставници Факултета техничких наука у Чачку. Право приступа има и овлашћено административно особље, као и трећа лица, по одобрењу администратора и лица одговорног за Систем.

Права и обавезе корисника система

Корисник Система има право на:

- приступ курсевима који одговарају предметима студијског програма који похађа

- активно учешће у креирању он-лајн садржаја према захтевима

предмета (уређивање вики-страна, решавање тестова, постављање радова и сл.)

- комуникацију са другим учесницима курсева, односно корисницима Система путем механизама самог Система (сервиси личних порука, причаонице, форуми)

- техничку подршку од стране администрације Система

- очување поверљивости личних података.

Корисник Система у обавези је да:

- чува у тајности своје приступне параметре (корисничко име и лозинку)

- поставља искључиво своје личне фотографије у профилу

- поштује ауторска права (нпр. забрањено је постављање линкова на дигиталне садржаје или саме садржаје који нису легални: пиратске, крековане софтвере и сл.)

- пријави администрацији Система било какве недостатке Система или инциденте који нарушавају регуларан рад

Кориснички налог

Сваки корисник поседује корисничко име и лозинку. Лозинка мора испуњавати услове сложености који су имплементирани у самом Систему. Корисник је одговоран за чување своје лозинке. Уколико је лозинка компромитована (директно изложена другим лицима, запамћена на јавном рачунару и слично), корисник је дужан да изврши њену промену или да о проблему извести администратора система како би лозинка била промењена.

Лозинку не треба чувати у веб-читачима јавних рачунара (интернет кафе, факултетски терминали и слично), нити држати записану на видном месту.

Лозинку не треба саопштавати другим корисницима , без обзира на њихов статус (нпр. Наставницима) . Није дозвољено коришћење туђег налога за приступ Систему.

Приватност личних података

Лични подаци налазе се у профилу који попуњава сам корисник, односно аутоматски је попуњен из спољне базе података о корисницима. Корисник треба да самостално одлучи које опционе податке ће унети у профил, на основу видљивости тих података у Систему. Одређени подаци су видљиви само за наставника, док су други јавно видљиви за било ког другог корисника. Овакве информације су експлицитно наведене у самом Систему.

Администратор и лица одговорна за рад Система имају право да користе личне податке корисника искључиво у сврху комуникације са самим корисницима и не смеју их објављивати и бележити у друге сврхе.

Дневници догађаја (логови) у којима се бележе активности корисника смеју се користити искључиво у административне и научно –истраживачке сврхе и ради добијања статистичих показатеља. Дневници се могу предавати на коришћење на основу одобрења одговорних лица и искључиво у санитизованом облику: лишени личних информација, нпр. имена, презимена, IP адресе.

Поверљивост наставних садржаја и комуникације на Систему и ауторска права

Наставни садржаји су сви ресурси који се користе за учење, а постављени су на Систему. На пример: pdf фајлови, презентације, текстови у различитим форматима, SCORM пакети, е-књиге и др. Копирање и дељење оваквих ресурса дозвољено је само за случајеве у којима је то експлицитно одобрено , што је

наглашено у типу лиценце датог ресурса. Нпр. ”Сва права задржана” значи да корисник може употребити дати садржај (преузети, читати), али није дозвољено његово даље ширење, објављивање, слање трећим лицима итд.

Факултет није одговоран за садржај који се поставља на Систем, већ је одговорност на кориснику који је поставио материјал.

Сваки облик комуникације на деловима Система који нису јавни сматра се поверљивим и такве податке није дозвољено преносити ван Система, објављивати и слично. Пример: постови са форума.

Дозвољени типови садржаја

Корисници имају могућност постављања различитих садржаја на Систем, углавном према захтеву одређеног курса.

Није дозвољено постављање нелегалних апликација, вируса, као ни линкова ка овим и сличним садржајима.

Пријављивање нерегуларности у раду система

Корисник је обавезан да примећене нерегуларности пријави администрацији Система у најкраћем року. У овакве појаве спадају:

- немогућност приступа Систему

- сумња у компромитованост налога

- појава слања веће количине порука (спам а) преко Система

- појава злонамерних програма на самом сајту: у виду заражених фајлова за преузимање или скриптова самог сајта који се детектују као злонамерни програм

- уочавање постављених линкова ка пиратским и сличним садржајима

Сајбер-етика

При коришћењу Система важе основна правила сајбер-етике, односно понашања у виртуелном простору. Корисници треба да уважавају једни друге и обраћају се на одговарјућем нивоу комуникације.

Објављивање садржаја који су недолични, слање великог броја порука (спамовање) и комерцијално оглашавање нису дозвољени.

Непридржавање правила коришћења Система могу довести до привремене блокаде налога или потпуног искључења, а теже повреде које

задиру у повреду интерних правилника установе предвиђају и санкције предвиђене Статутом и правилником.

Поједине активности, као што је нпр. постављање нелегалних садржаја спадају у рачунарски криминал и подлежу одговарајућем Закону РС.

13.2 Упитник - ставови о поверењу у е-образовање

Оцените следеће ставове оценама од 1-5, при чему је 1 - у потпуности се не слажем, 2 - углавном се не слажем, 3 - немам став (нити се слажем, нити не слажем), 4 - углавном се слажем и 5 - у потпуности се слажем	
1. За моје поверење у овај сајт, од значаја је што је на факултетском домену.	12345
2. Значајно за моје поверење у овај систем за е-учење је што га користе и друге колеге.	12345
Оцените следеће ставове о коришћењу овог сајта (и курса) оценама од 1-5, при чему је 1 - у потпуности се не слажем, 2 - углавном се не слажем, 3 - немам став (нити се слажем, нити не слажем), 4 - углавном се слажем и 5 - у потпуности се слажем	
1. Тачност садржаја за е-учење (нпр. број словних грешака) утиче на моје поверење у сајт за е-учење.	12345
2. Доступност самог сајта утиче на моје поверење у сајт.	12345
3. Доступност техничке подршке утиче на моје поверење у сајт.	12345
4. Квалитет наставног материјала доприноси мом поверењу у систем за е-учење.	12345
5. Комуникација са другим учесницима на курсевима доприноси мом поверењу у систем за е-учење.	12345
6. Дизајн система (изглед, боје) утиче на моје поверење у систем за е-учење.	12345
7. Осећај заједништва са другим корисницима система утиче на моје поверење у систем за е-учење.	12345
Оцените следеће ставове везане за коришћење овог Моодле-а оценама од 1-5, при чему је 1 - у потпуности се не слажем, 2 - углавном се не слажем, 3 - немам став (нити се слажем, нити не слажем), 4 - углавном се слажем и 5 - у потпуности се слажем	
1. Од значаја за моје поверење у сајт за е-учење је да будем добро упознат/а са правилима коришћења.	12345
2. Од значаја за моје поверење у сајт за е-учење је да ми систем помаже у случају проблема са пријавом.	12345
3. Од значаја за моје поверење у сајт за е-учење је да су постављени фајлови на систему проверени.	12345
4. Од значаја за моје поверење у сајт је забрана посећивања сајта потенцијалним нападачима.	12345
5. Од значаја за моје поверење у сајт је очување приватности мојих података.	12345

13.3 Упитник - ставови о прихваћености система за управљање е-учењем

Оцените следеће ставове у вези инструкције оценама од 1-5, при чему је 1 - у потпуности се не слажем, 2 - углавном се не слажем, 3 - немам став (нити се слажем, нити не слажем), 4 - углавном се слажем и 5 - у потпуности се слажем	
Наставник је пружио одговарајућа упутства.	12345
Наставник је обезбедио информације о процесу учења.	12345
Наставникова процењења знања је правична.	12345
Оцените следеће ставове о наставном материјалу оценама од 1-5, при чему је 1 - у потпуности се не слажем, 2 - углавном се не слажем, 3 - немам став (нити се слажем, нити не слажем), 4 - углавном се слажем и 5 - у потпуности се слажем	
Обезбеђено је довољно наставног материјала	
Наставни материјал је у складу са циљевима учења.	
Оцените следеће ставове везане за дизајн оценама од 1-5, при чему је 1 - у потпуности се не слажем, 2 - углавном се не слажем, 3 - немам став (нити се слажем, нити не слажем), 4 - углавном се слажем и 5 - у потпуности се слажем.	
Ниво тежине наставног материјала је одговарајући.	12345
Динамика испоруке материјала је одговарајућа.	12345
Оцените следеће ставове о забавности (плауфуллнесс) од 1-5, при чему је 1 - у потпуности се не слажем, 2 - углавном се не слажем, 3 - немам став (нити се слажем, нити не слажем), 4 - углавном се слажем и 5 - у потпуности се слажем	
Делује ми да е-учење повећава моју креативност.	12345
Е-учење је веома корисно за мене.	12345
Оцените следеће ставове оценама од 1-5, при чему је 1 - у потпуности се не слажем, 2 - углавном се не слажем, 3 - немам став (нити се слажем, нити не слажем), 4 - углавном се слажем и 5 - у потпуности се слажем	
Методе е-учења су ми јасне за разумевање.	12345
Е-учење је једноставно.	12345
Оцените следеће ставове оценама од 1-5, при чему је 1 - у потпуности се не слажем, 2 - углавном се не слажем, 3 - немам став (нити се слажем, нити не слажем), 4 - углавном се слажем и 5 - у потпуности се слажем	
Радо бих учествовао/ла у другим е-курсевима.	12345
Мислим да би е-учење требало да буде имплементирано код других предмета.	12345
Препоручићу е-учење другим колегама.	12345
Радије бих да користим овај систем за е-учење, него постојећи (itlab.ftn.kg.ac.rs/moodle)	12345
Оцените следеће ставове везане за безбедност оценама од 1-5, при чему је 1 - у потпуности се не слажем, 2 - углавном се не слажем, 3 - немам став (нити се слажем, нити не слажем), 4 - углавном се слажем и 5 - у потпуности се слажем	
Безбедност личних података ми је битна када користим систем за онлајн-учење.	12345

Важно ми је да фајлови који се налазе на курсевима које похађам онлајн, буду проверени.	12345
Важно ми је да познајем своја права и обавезе код коришћења платформе за е-учење.	12345
Важно ми је да добијам информације које ми помажу да унапредим своју безбедност док користим платформу за е-учење.	12345
Током коришћења овог сајта, имао/ла сам прилике да унапредим своје познавање безбедности података.	12345
Добијао/ла сам одговарајуће информације потребне да безбедно користим сајт.	12345
На овом сајту сам имао/ла одговарајућу подршку у случајевима проблема са пријавом.	12345
Информације у вези безбедности података, које сам добио/ла на сајту нису ометале мој процес учења и обављања задатака на курсу "Технологије и алати за оцењивање".	12345
Моја безбедносна култура (управљање лозинком, одјава са система, коришћење садржаја и сл.) се побољшала коришћењем овог сајта.	12345
Информације везане за безбедност (поруке и оне на самом курсу) биле су ми од користи.	12345

13.4 Статистички подаци уз поглавље ”Евалуација”

Дескриптивна статистика - Упитник о поверењу

	N	Minimum	Maximum	Mean	Std. Deviation
Репутација 1	30	2	5	4,43	,728
Репутација 2	30	1	5	3,97	1,159
Садржаји 1	30	1	5	3,53	1,074
Садржаји 2	30	2	5	4,37	,718
Садржаји 3	30	3	5	4,40	,621
Садржаји 4	30	3	5	4,60	,563
Садржаји 5	30	2	5	3,90	,995
Садржаји 6	30	2	5	3,70	1,022
Садржаји 7	30	2	5	3,77	,817
Безбедност 1	30	2	5	4,13	,937
Безбедност 2	30	3	5	4,53	,681
Безбедност 3	30	4	5	4,63	,490
Безбедност 4	30	4	5	4,87	,346
Безбедност 5	30	3	5	4,87	,434
Valid N (listwise)	30				

Pearson коефицијенти (фактор ”безбедност”, упитник о поверењу)						
		БЕЗБ1	БЕЗБ2	БЕЗБ3	БЕЗБ4	БЕЗБ5
БЕЗБ1	Pearson Correlation	1	,587**	-,156	-,040**	,335
	Sig. (2-tailed)		,001	,410	,836	,070
	N	30	30	30	30	30
БЕЗБ2	Pearson Correlation	,587**	1	,020**	,365	,502**
	Sig. (2-tailed)	,001		,918	,047	,005
	N	30	30	30	30	30
БЕЗБ3	Pearson Correlation	,335	,502**	,312	,411**	1
	Sig. (2-tailed)	,070	,005	,093	,024	
	N	30	30	30	30	30
БЕЗБ4	Pearson Correlation	-,156	,020	1	,567	,312
	Sig. (2-tailed)	,410	,918		,001	,093
	N	30	30	30	30	30
БЕЗБ5	Pearson Correlation	-,040	,365*	,567	1*	,411*
	Sig. (2-tailed)	,836	,047	,001		,024
	N	30	30	30	30	30

Дескриптивна статистика - Упитник о прихваћености технологије

	N	Minimum	Maximum	Mean	Std. Deviation
KINS1	30	4	5	4,60	,498
KINS2	30	3	5	4,53	,730
KINS3	30	3	5	4,23	,774
KMAT1	30	3	5	4,13	,776
KMAT2	30	3	5	4,40	,621
DIZ1	30	2	5	4,13	,776
DIZ2	30	3	5	4,23	,626
USEF1	30	1	5	4,13	1,074
USEF2	30	3	5	4,57	,568
EAS1	30	3	5	4,60	,563
EAS2	30	2	5	4,30	,750
INT1	30	3	5	4,43	,626
INT2	30	3	5	4,50	,777
INT3	30	3	5	4,50	,682
INT4	30	1	5	3,63	,999
SEC1	30	4	5	4,87	,346
SEC2	30	4	5	4,77	,430
SEC3	30	3	5	4,63	,615
SEC4	30	2	5	4,47	,900
SEC5	30	2	5	3,77	,817
SEC6	30	2	5	4,23	,858
SEC7	30	3	5	4,50	,682
SEC8	30	3	5	4,30	,750
SEC9	30	1	5	3,77	1,006
SEC10	30	3	5	4,03	,765
Valid N (listwise)	30				

13.5 Списак слика и дијаграма

13.6 Списак табела