ՀՀ ԳԱԱ ԻՆՖՈՐՄԱՏԻԿԱՅԻ ԵՎ ԱՎՏՈՄԱՏԱՑՄԱՆ ՊՐՈԲԼԵՄՆԵՐԻ ԻՆՍՏԻՏՈՒՏ
Վահե Առաքելի Առաքելյան

Ինֆորմացիայի պաշտպանության հիմնահարցերի հետազոտում էլեկտրոնային կրթական համակարգերում

Ե13.04 – «Հաշվողական մեքենաների, համալիրների, համակարգերի և ցանցերի մաթեմատիկական և ծրագրային ապահովում» մասնագիտությամբ տեխնիկական գիտությունների թեկնածուի գիտական աստիճանի հայցման ատենախոսության

ՍԵՂՄԱԳԻՐ

Երևան – 2014

ИНСТИТУТ ИНФОРМАТИКИ И ПРОБЛЕМ АВТОМАТИЗАЦИИ НАН РА
Ваге Аракелович Аракелян

Исследование проблем информационной безопасности в системах электронного обучения

АВТОРЕФЕРАТ

диссертации на соискание ученой степени кандидата технических наук по специальности 05.13.04 –“Математическое и программное обеспечение вычислительных машин, комплексов, систем и сетей”

Ереван – 2014

Ատենախոսության թեման հաստատվել է ՀՀ ԳԱԱ Ինֆորմատիկայի և ավտոմատացման պրոբլեմների ինստիտուտում:

Գիտական ղեկավար՝ ֆիզ.մաթ.գիտ.դոկտոր Մ. Ե. Հարությունյան
Պաշտոնական ընդդիմախոսներ՝ տեխ.գիտ.դոկտոր Ա.Ս.Նանասյան
տեխ.գիտ.թեկնածու Մ.Ղ.Գյուրջյան

Առաջատար կազմակերպություն՝ Երևանի պետական համալսարան

Պաշտպանությունը կայանալու է 2014թ. հունիսի 6-ին, ժ. 15:00-ին ՀՀ ԳԱԱ Ինֆորմատիկայի և ավտոմատացման պրոբլեմների ինստիտուտում գործող 037 «Ինֆորմատիկա և հաշվողական համակարգեր» մասնագիտական խորհրդի նիստում հետևյալ հասցեով՝ Երևան, 0014, Պ. Սևակի 1:

Ատենախոսությանը կարելի է ծանոթանալ ինստիտուտի գրադարանում:
Սեղմագիրն առաքված է 2014թ. մայիսի 6-ին:

Մասնագիտական խորհրդի
գիտական քարտուղար, ֆ.մ.գ.դ. Հ. Գ. Սարուխանյան

Тема диссертации утверждена в институте проблем информатики и автоматизации НАН РА

Научный руководитель: доктор физ.-мат. наук М.Е.Арутюнян
Оффициальные оппоненты: доктор тех. наук А.С.Нанасян
кандидат тех. наук М.К.Гюрджян
Ведущая организация: Ереванский государственний университет

Защита состоится 6-го июня 2014г. в 15:00 на заседании специализированного совета 037 “Информатика и вычислительные системы” в Институте проблем информатики и автоматизации НАН РА по адресу: 0014, г. Ереван, ул. П. Севака 1.
С диссертацией можно ознакомится в библиотеке ИПИА НАН РА.
Автореферат разослан 6-ого мая 2014г.

Ученый секретарь специализированного совета
доктор физ.мат.наук А. Г. Саруханян

Աշխատանքի հիմնական բնութագիրը

Թեմայի արդիականությունը:

Էլեկտրոնային ուսուցումը կրթություն ստանալու գերժամանակակից միջոց է, որտեղ կիրառված են ավանդական և ինովացիոն մեթոդներ, համակարգչային և տեղեկատվական տեխնոլոգիաների վրա հիմնված բազմաֆունկցիոնալ գործիքներ և ծրագրային ապահովումներ: Էլեկտրոնային ուսուցումը ենթադրում է ուսանողների և դասախոսների միջև կապը ժամանակի և տարածության մեջ: Էլեկտրոնային ուսուցման միջավայրեր ապահովող շատ ծրագրային ապահովումներ կան: Դրանց շարքում կան թե՛ կոմերցիոն նպատակով և թե՛ ազատ օգտագործման համար նախագծվածներ:

Էլեկտրոնային ուսուցման առավելություններից է կրթություն ստանալու համեմատաբար ցածր ինքնարժեքը, էլեկտրոնային գրականության, առաջադրանքների և այլ նյութերի արագ հասանելիությունը, փոխանակումը դասախոսների և ուսանողների միջև, ուսուցման մեթոդների ճկունությունը, դասընթացների մասնակիցների և դասախոսների աշխարհագրական դիրքից և ժամանակից անկախությունը, նրանց սոցիալական հավասարության տպավորությունը և այլն:

Գոյություն ունեն բազմաթիվ էլեկտրոնային ուսուցման համակարգեր, որոնցից առավել լայնորեն կիրառվում են՝ Docent, Quasar, Claroline, IWT, Running Platform, ATutor, ADA,Ilias3 Docebo, eCollge, Dokeos, Blackboard Learning System, KEWL, LMS Moodle, Sakai, ANGELe Learning Management Sute, Desire2Learn, Olat: Թվարկվածներից յուրաքանչյուրն ունի իրեն բնորոշ հատկանիշները, հնարավորությունները, առավելությունները, թերությունները և նախապատվությունը՝ կախված կիրառական նշանակությունից, ոլորտից և բնույթից:

Հայաստանի Հանրապետությունում էլեկտրոնային ուսուցումը նույնպես արագ զարգանում է, կիրառման վառ օրինակներ են «Հայկական վիրտուալ համալսարան»–ը, ՀՀ ԳԱԱ Գիտակրթական միջազգային կենտրոնի կողմից առաջարկվող էլեկտրոնային ուսուցումը և Երևանի պետական համալսարանի կողմից առաջարկվող հեռուսուցումը: Մասնավորապես, Հայկական վիրտուալ համալսարանի ծրագիրը նախագծվել է 2004 թվականին՝ ՀԲԸՄ Սիլիկոն Վելի մասնաճյուղի կողմից, որը դեռ վաղուց էր նշում սփյուռքում և հայրենիքում հայ ժողովրդի ներկա պահանջները բավարարող կրթական մի ծրագրի անհրաժեշտության մասին: Ծրագրի տեխնոլոգիան բազմակողմանիորեն մշակվել է Հայաստանում՝ Երևանի պետական համալսարանի տեղեկատվական տեխնոլոգիաների կրթական և հետազոտական կենտրոնի գիտնականների և ծրագրավորողների համագործակցությամբ:

ՀՀ–ում գործող վերը նշված էլեկտրոնային ուսուցման բոլոր համակարգերը կառուցված են LMS Moodle համակարգի հենքի վրա, ինչը հիմնավորված է հետևյալ հատկանիշների առկայությամբ՝ համակարգը բաց ծրագրային կոդով է, անվճար է նույնիսկ կոմերցիոն

նպատակներով կիրառելու դեպքում, հնարավորություն է տալիս նախագծել և ներդնել անհրաժեշտ ծրագրային հավելումներ, ունի հայալեզու միջերես և այլն։

Հետազոտությունների արդյունքում պարզվել է, որ չնայած բազմաթիվ առավելությունների, այս համակարգն ունի անվտանգության և ամբողջականության ապահովման խնդիրներ։ LMS Moodle համակարգը խոցելի է տարբեր տեսակի գրոհների նկատմամբ։ Խոցելիության թերությունները համակարգը դարձնում են անպաշտպան, արդյունքում կարող է տեղի ունենալ համակարգի աշխատանքի խափանում, առցանց քննությունների արդյունքների կեղծում, անօրեն օգտագործում հարցաշարերի և տարբեր տեսակի էլեկտրոնային տվյալների կորուստ կամ արտահոսք և այլն։

Աշխատանքի նպատակը

Հաշվի առնելով, որ ՀՀ–ում կիրառվող էլեկտրոնային ուսուցման համակարգերի գերակշիռ մասը հիմնված է LMS Moodle–ի հենքի վրա, կարևոր է հետազոտել և առաջարկել այնպիսի լուծումներ, որոնք LMS Moodle համակարգը կդարձնեն ավելի պաշտպանված, հուսալի և հասանելի։ Ստեղծել հնարավորություն ուսանողների համակարգիչների կիրառմամբ անց կացնել առցանց անվտանգ քննություններ՝ խուսափելով հատուկ սարքավորումներով կահավորված քննասենյակներ կառուցելու ծախսատար գործընթացից։

Հետազոտման օբյեկտը

Ուսումնասիրության օբյեկտներն են LMS Moodle էլեկտրոնային ուսուցման համակարգը, նրա UML մոդելը, նույնականացման և վավերականացման մեխանիզմները։

Հետազոտման մեթոդները

Ատենախոսության մեջ օգտագործվում են WEB հենքով էլեկտրոնային ուսուցման համակարգերի անվտանգության ապահովման ծածկագրական HTTPS և SSL արձանագրությունները, PHP ծրագրավորման լեզվի միջոցով HTTP նույնականացման, մուտքի իրավունքների թույլտվության մեթոդները։ Օգտագործվում են համակարգիչների արգելափակման, օպերացիոն համակարգերի իրավասությունների բաշխման և ցանցային միջմիացումների կառավարման մեթոդները։

Արդյունքների գիտական նորությունը

Հայտնաբերվել է LMS Moodle համակարգի խոցելիությունը սեանսի առևանգում, սեանսի ամրագրում, ուղղակի գրոհով օգտատիրոջ մուտքանվան և գաղտնաբառի գուշակում հարձակումների նկատմամբ։ Մշակվել և առաջարկվել են մեխանիզմներ, որոնք ապահովում են պաշտպանությունը և հուսալիությունը նշված հարձակումների նկատմամբ։

Ստեղծվել է «առցանց թեստավորման միջավայր» (ԱԹՄ) համակարգ, որը հնարավորություն է տալիս անվտանգ առցանց քննությունների անցկացումը ուսանողների համակարգիչների միջոցով: Այն գործարկվում է անկախ համակարգչի օպերացիոն համակարգից, արգելափակում է ուսանողի համակարգիչը՝ առանց որևէ ծրագրային փոփոխություն կատարելու:

Ստացված արդյունքների կիրառական նշանակությունը

Առաջարկված անվտանգության ապահովման մեխանիզմները կարող են կիրառվել LMS Moodle համակարգը կիրառող էլեկտրոնային ուսուցման միջավայրերում՝ արդյունավետ և որոշակի հարձակման տիպերից պաշտպանված էլեկտրոնային ուսուցում ապահովելու նպատակով:

LMS Moodle-ում ներդրվել են կոնֆերանս և հայալեզու էլեկտրոնային դեկանատ մոդուլները, որոնք ապահովում են ուսանողների և դասախոսների փոխադարձ շփումը, դասախոսի կողմից ուսանողներին տեսնելը և իսկությունը ստուգելը, ուսանողների՝ հեռակա կարգով ինտերակտիվ դասընթացներին մասնակցելը, համակարգում առկա մուլտիմեդիա կրթական նյութերից օգտվելը:

Ստեղծված ԱԹՄ համակարգի կիրառմամբ հնարավոր է ուսանողների համակարգիչներով իրականացնել առցանց անվտանգ քննություններ՝ հատուկ սարքավորումներով կահավորված քննասենյակների քանակության չբավարարման դեպքում:

Ներդրումներ

Ստացված արդյունքները քննարկվել են ՀՀ ԳԱԱ Գիտակրթական միջազգային կենտրոնի համապատասխան մասնագետների հետ և ներդրվել են ուսումնական հաստատության կողմից իրականացվող էլեկտրոնային ուսուցման գործընթացի մեջ: LMS Moodle էլեկտրոնային ուսուցման համակարգում ներդրվել են անվտանգությունը բարելավող ծրագրային մոդուլներ, որոնք ապահովում են համակարգի անվտանգությունը որոշակի հարձակումներից:

Ներդրվել է «Առցանց թեստավորման միջավայրը», որը հնարավորություն է տալիս առցանց քննություններն անց կացնել ուսանողների համակարգիչների միջոցով՝ անբավարար քանակությամբ համակարգիչների դեպքում:

Պաշտպանությանը ներկայացվում են հետևյալ դրույթները

- առաջարկվել են LMS Moodle համակարգի անվտանգությունը բարելավող ծրագրային մեխանիզմներ, որոնք կառուցված են reCapcha–ի, սեանսի ID–ի վերստեղծման, համակարգ մուտք գործելիս թույլտվությունների բեռնման փոփոխության և SSL արձանագրության ինտեգրման հիման վրա,

- մշակվել է անվտանգ թեստավորման համակարգ, որի միջոցով հնարավոր է կիրառել ուսանողների համակարգիչները առցանց քննություններ հանձնելու համար,
- մշակվել է LMS Moodle համակարգում էլեկտրոնային դեկանատ մոդուլի հայալեզու միջերես,
- իրականացվել է LMS Moodle համակարգում BigBlueButton կոնֆերանս համակարգի ինտեգրումը։

Ապրոբացիա

Ատենախոսության արդյունքները զեկուցվել են՝

9–րդ Համակարգչային գիտություններ և տեղեկատվական տեխնոլոգիաներ գիտաժողովում, Երևան, 2013,

ITA 2013 – ITHEA ISS Joint International Events on Informatics Winter Session, December 18–19, Sofia, Bulgaria 2013, ինչպես նաև ՀՀ ԳԱԱ ԻԱՊԻ ընդհանուր սեմինարներում։

Հրապարակումներ

Ատենախոսության հիմնական արդյունքները հրապարակվել են [1-4] ում։

Ատենախոսության կառուցվածքը և ծավալը

Ատենախոսությունն իր մեջ ներառում է ներածություն, 4 գլուխներ՝ իրենց ամփոփումներով, գրականության ցանկ՝ իր 83 հղումներով և երկու հավելվածներով։ Ատենախոսության ընդհանուր ծավալը 102 էջ՝ 4 աղյուսակներով և 17 պատկերներով։

Աշխատանքի բովանդակությունը

Գլուխ 1-ը նվիրված է Էլեկտրոնային ուսուցման համակարգերի առավելություններին և թերություններին։ Ուսումնասիրվել և համեմատվել են առավել հայտնի էլեկտրոնային ուսուցման համակարգերը։ Էլեկտրոնային ուսուցման ոլորտում հանդիպող անվտանգության արդիական խնդիրները առաջ քաշելու նպատակով ուսումնասիրվել են վեբ հենքով ուսուցման համակարգերի պաշտպանության մեխանիզմները և սկզբունքները։

Բաժին 1.1-ում քննարկվում են օգտատիրոջը ճանաչելու և մուտքի արտոնություններն որոշելու նույնականացման գործընթացը։

Այս մեխանիզմը կանխում է հարձակվողների մուտքը այլ օգտատիրոջ էլեկտրոնային տարածք, զգայուն ինֆորմացիայի դիտումը և անթույլատրելի գործողությունների կատարումը։ **Բաժին 1.2-ը** դիտարկում է անվտանգության խնդիրները և հնարավոր

լուծումները: Էլեկտրոնային ուսուցման շրջանակներում գոյություն ունի կախվածություն դասախոսների, սովորողների և տվյալների միջև, որոնք գտնվում են աշխարհագրական տարբեր տարածաշրջաններում և կապվում են համացանցի միջոցով: Ինչպես երևում է նկ.1-ում, սովորողների գնահատումը նույնպես կատարվում է համացանցի միջոցով: Այս կախվածությունը նպաստում է ինֆորմացիոն անվտանգության ամենամեծ ռիսկին: **Բաժին 1.3-ը** նկարագրում է Էլեկտրոնային ուսուցման համակարգերի պաշտպանությունը որպես ՎԵԲ սերվեր: Ինչպես հայտնի է էլեկտրոնային ուսուցման համակարգերը հիմնականում իրենցից ներկայացնում են վեբ հենքով ծրագրային ապահովումներ: Ուստի Էլեկտրոնային ուսուցման համակարգը սպասարկող ՎԵԲ սերվերի անվտանգության ապահովումը անմիջականորեն կապված է ուսուցման համակարգի անվտանգության հետ[1]:

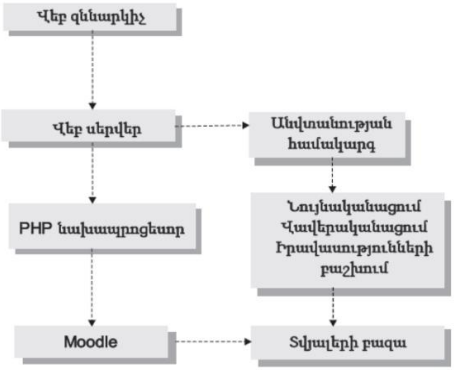
Նկ. 1: Էլեկտրոնային ուսուցման միջավայր

Բաժին 1.4-ում ներկայացված է LMS Moodle–ի նկարագրությունը և համեմատական ուսումնասիրությունն այլ էլեկտրոնային ուսուցման համակարգերի նկատմամբ: Moodle բառը հապավում է, որը թարգմանաբար նշանակում է մոդուլային օբյեկտ–կողմնորոշված դինամիկ ուսուցման միջավայր: Այն բաց կոդով էլեկտրոնային ուսուցման միջավայր է, հայտնի է որպես ուսուցման կառավարման համակարգ(Learning Management Systems), վիրտուալ ուսուցման միջավայր(Virtual Learning Environment): Հասանելի է 2002 թ–ից, օգտագործվում է ավելի է քան 210 երկրներում և ունի 4,700,000-ից ավել օգտագործողներ:Իրականացվել է 10 հայտնի էլեկտրոնային համակարգերի համեմատական վերլուծություն ըստ ուսումնական գործիքների, սպասարկման

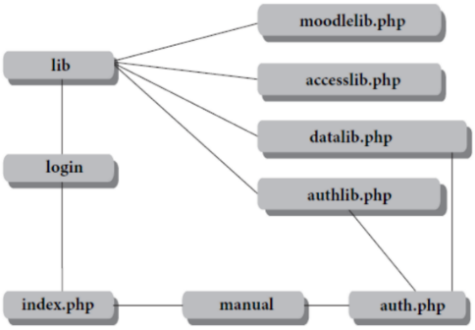
[1] Geetha V., Pranesh. V. Kallapur, “Web Security: Research Challenges and Open Issues”,SprAdvances in Computer, Communication, Control and Automation, Volume 121, pp 397-404, 2012

գործիքների և տեխնիկական հասանելիության: Համեմատվել են 41 հատկանիշներ, որոնցից 39–ը հասանելի են LMS Moodle համակարգում:
Այսպիսով, ըստ թվարկված վերլուծությունների՝ LMS Moodle–ը չի զիջում այլ համակարգերին, որոշ դեպքերում ունի առավելություններ, որոնցից ՀՀ–ում առավել կիրառական նշանակություն ունի հայալեզու միջերեսի առկայությունը:

Գլուխ 2-ում ներկայացված է LMS Moodle-ի օբյեկտ–կողմնորոշված մոդելը, որն օգտագործում է միասնական մոդելավորման լեզուն, դրա անվտանգության ծառայությունների վերլուծությունը, ինչպես նաև անվտանգության թերությունները վերացնելու առաջարկված լուծումները: **Բաժին 2.1-ում** ներկայացվում է LMS Moodle-ի



Նկ. 2 LMS Moodle-ի անվտանգության ծառայության կլասս-դիագրամի հատված



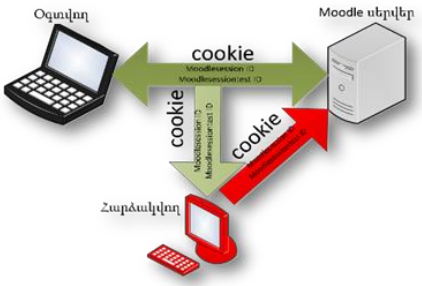
Նկ.3 LMS Moodle- ի բաղադրիչների դիագրամը

անվտանգության մոդելը և պարզաբանվում են անվտանգության ծառայությունները, ցույց է տրվում խոցելի տեղերը: Ներկայացված UML մոդելը բաժանված է 3 մոդելների՝

վերլուծության, նախագծման և բաղադրիչների: Նախագծման մոդելը բաղկացած է կլասսների դիագրամներից: LMS Moodle-ը իրականացնում է հետևյալ անվտանգության ծառայություններ՝ վավերականացում, մուտքի ղեկավարում և ոչ-ժխտում: Նկ.2–ում պատկերված է անվտանգության ծառայության մեջ օգտագործվող կլասսների դիագրամը:

Ինչպես բոլոր վեբ համակարգերում, որոշ անվտանգության ծառայություններ չեն իրականացվում ուղղակիորեն, այլ կախված են վեբ-սերվերի կառուցվածքից[2]: Այսպիսի ծառայություններ հաստատելու համար անհրաժեշտ է որոշել LMS Moodle–ի իրականացման բաղադրիչները: Ամենակարևոր բաղադրիչները պատկերված են նկ.3-ում:

Բաժին 2.2-ում տրված են հայտնաբերված արդյունավետ գրոհները ընդդեմ LMS Moodle համակարգի: Այդպիսի գրոհները կարող են բաժանվել 2 խմբի՝ սեանսի գրոհներ և



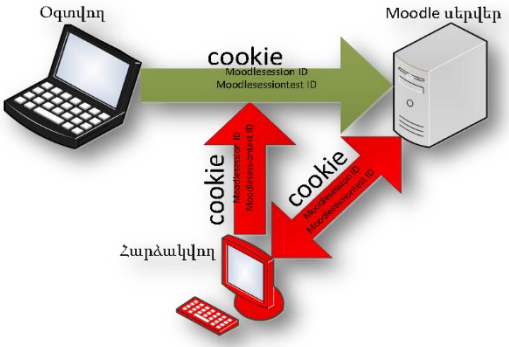
Նկ. 4 Սեանսի առևանգման դիագրամ

կառուցվածքային գրոհներ: Երկու սեանսի գրոհներ արդյունավետ են LMS Moodle-ի դեմ՝ սեանսի առևանգում և սեանսի ամրագրում:

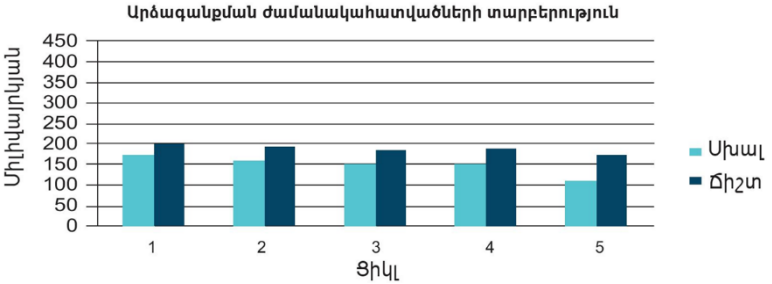
Սեանսի առևանգումը գաղտնալսման գրոհների մի մաս է, որտեղ գրոհողը լսում է օգտատիրոջ և սերվերի միջև խոսակցությունը և աշխատում է գտնել այնպիսի ինֆորմացիա, որը կարող է օգտագործվել օգտատիրոջը վերահսկելու նպատակով (Նկ.4): Սեանսի ամրագրում գրոհի թիրախը նույնպես օգտատիրոջ սեանսի տվյալներն են: Ինչևէ, այս գրոհը դասակարգվում է որպես ակտիվ գրոհ կամ խափանող գրոհ: Օգտատիրոջ և սերվերի միջև խոսակցությունը լսելու փոխարեն գրոհողը ընդհատում է օգտատիրոջ HTTP հարցումը: Երբ անանուն օգտատերը փորձում է մուտք գործել LMS Moodle, moodlesession և moodlesessiontest պարամետրերը հատկացվում են օգտատիրոջը: Օգտվելով այդ հանգամանքից՝ գրոհողը կարող է ստանալ արժեքներ որպես անանուն

[2] Jana Fruth, Carsten Schulze, Marleen Rohde, Jana Dittmann, “E-Learning of IT Security Threats: A Game Prototype for Children”, Communications and Multimedia Security Lecture Notes in Computer Science, Volume 8099, pp 162-172, 2013

օգտագործող և կասեցնել դեռ չվավերականացված օգտատիրոջ հարցումը: Երբ օգտատերը փորձում է մուտք գործել համակարգ, գրոհողը փոխարինում է օգտատիրոջը տրված moodlesession և moodlesessiontest արժեքները նախկինում իր կողմից ստացված արժեքներով: Երբ թիրախային օգտատերը նույնականացվում է, սեանսը թույլատրվում է օգտատիրոջ իրավասություններով, ինչը հնարավորություն է տալիս գրոհողին ստանալ նույն իրավասությունները, քանի որ նա արդեն ունի moodlesession և moodlesessiontest ստացված արժեքներ, որը որոշում է ֆիքսված սեանսը: Նկ.5-ում ցույց է տալիս սեանսի ամրագրման գրոհը:



Նկ.5 Սեանսի ամրագրման դիագրամ



Նկ. 6 Ճիշտ և սխալ մուտքանունների ներմուծման դեպքում LMS Moodle–ի արձագանքների ժամանակների համեմատումը

Գաղտնաբառի գուշակում գրոհն իրականցվում է դատարկ cookie դաշտով LMS Moodle-ի սերվերին բազմաթիվ հարցումներ ուղարկելով: LMS Moodle-ում առկա բացթողումների պատճառով մուտք գործելու անհաջող փորձերը զրոյացվում են, երբ հարցման ներսում cookie-ների դաշտը ոչ մի արժեք չունի կամ ընդհանրապես cookie գոյություն չունի:

Այս բացթողումը հնարավորություն է տալիս գրոհողին կանխագուշակել գաղտնաբառը: Ուղղակի գրոհի (brute force) մեթոդը իրականացվում է նույն կերպ, ինչպես գաղտնաբառի գուշակման դեպքում: Ինչևիցէ, բազմաթիվ գաղտնաբառեր ուղարկելու փոխարեն մի քանի մուտքանուններ ուղարկվում են պատահական սկզբունքով ընտրված գաղտնաբառի հետ: LMS Moodle–ի արձագանքը ճիշտ մուտքանունների դեպքում ավելի երկար է տևում, քան սխալ մուտքանվան դեպքում: Դա օգտագործվում է գրոհները իրականացնելիս համակարգի արձանգանքման ժամանակների միջև տարբերությունը գրանցելիս: Նկ.6-ում ցույց է տրված ճիշտ և սխալ մուտքանունների դեպքում LMS Moodle-ի արձագանքման միջին ժամանակները:

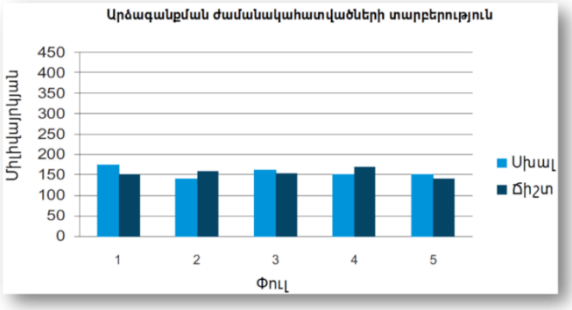
Բաժին 2.3-ում ներկայացված են LMS Moodle–ում հայտնաբերված խոցելիությունների վերացման և որոշակի գրոհներից պաշտպանվելու առաջարկված լուծումները: LMS Moodle-ը խոցելի է հետևյալ գրոհների նկատմամբ՝ սեանսի առևանգում, սեանսի ամրագրում, օգտատիրոջ մուտքանվան և գաղտնաբառի ուղղակի գուշակում: Այս խոցելիությունը շրջանցելու նպատակով ՀՀ ԳԱԱ ԳԿՄԿ–ում ներդրված LMS Moodle–ի սկզբնական կոդում կատարվել են որոշակի փոփոխություններ և ավելացվել են նոր մոդուլներ [1]:

2.3.1 ենթաբաժնում ներկայացված է սեանսի առևանգման կանխման լուծումը: LMS Moodle-ը ունի որոշակի գործողությունների համար SSL օգտագործելու հնարավորություն: Ինչևէ այդ հնարավորությունը չի կարող կանխել սեանսի առևանգումը, սեանսի ամրագրումը և օգտատիրոջ մուտքանվան գուշակումը: Այս գրոհը կասեցնելու նպատակով անհրաժեշտ է ամբողջ կայքը օգտագործողների հետ HTTPS արձանագրության միացումներով իրականացնել: Դա իրականացվել է ծրագրային մոդուլի մշակմամբ և ինտեգրմամբ, որը ավտոմատ կերպով կատարում է SSL սերտիֆիկատի գեներացում, տեղադրում և բոլոր HTTP արձանագրությամբ հարցումների հարկադրաբար փոխակերպում HTTPS հարցումներով: **2.3.2 ենթաբաժնում** ներկայացված է սեանսի ամրագրման կանխման լուծումը: Սեանսի ամրագրման կանխումն իրականացված է նոր սեանսի ID-ի վերստեղծմամբ, երբ օգտատեը վավերականացվում է մուտքանուն/գաղտնաբառ համապատասխանեցմամբ: Բարեհաջող մուտքանուն/գաղտնաբառ համապատասխանեցման դեպքում LMS Moodle համակարգը օգտատիրոջը փոխանցվող cookie–ում սկզբնականից տարբեր moodlesession և moodlesessiontest արժեքներ է տեղադրում: Արդյունքում հարձակվողի կողմից ներմուծված cookie–ն դառնում է անվավեր հարձակումը ձախողվում է: Սեանսի ID-ի վերստեղծման և նոր cookie–ի փոխանցման գործընթացն իրականցվում է ատենախոսության շրջանակներում մշակված ծրագրային մոդուլի միջոցով, որն ինտեգրվել LMS Moodle համակարգի accesslib.php և authlib.php մոդուլներում: **2.3.3 ենթաբաժնում** ներկայացված է գաղտնաբառի գուշակման կանխման լուծումը: Վավերականացման ծառայությունը, որն իրականացվում է մուտքի էջի տեսքով, կարող է ավտոմատացված ուղղակի հարձակման

թիրախ լինել: Մուտք գործելու էջը կարող է պաշտպանվել CAPTCHA-ի միջոցով: Նկ. 7–ում պատկերված է մուտքի էջում ներդրված CAPTCHA համակարգի կողմից իրականացված reCaptcha հավելումը: Վերջինս վավերականացման ծառայությունը ավելի կայուն է դարձնում ծրագրային միջոցների կողմից իրականացվող ուղղակի գրոհների նկատմամբ: Հետազոտության ընթացքում նախագծվել է նոր մոդուլ, որը ինտեգրվել է LMS Moodle համակարգի կարգաբերման moodle.php ֆայլում: Արդյունքում հնարավոր դարձել էլեկտրոնային ուսուցման համակարգի մուտքային էջում տեղադրել reCaptcha հավելումը: Համվելման նպատակն է կանխել թե՛ մուտքանվան, թե՛ գաղտնաբառի ուղղակի գրոհով հարձակումները:

Նկ 7. LMS Moodle համակարգի մուտքի էջը reCaptcha–ի ինտեգրմամբ:

2.3.4 ենթաբաժնում ներկայացված է մուտքանվան գուշակման կանխման լուծումը: Ուղղակի գրոհն իրականացվում է հետևյալ սկզբունքով՝բազմաթիվ մուտքանուններ ուղարկվում են դեպի ուսուցման համակարգ՝ պատահական սկզբունքով ընտրված գաղտնաբառի հետ, LMS Moodle–ի արձագանքը ճիշտ մուտքանունների դեպքում ավելի երկար է տևում քան սխալ մուտքանվան դեպքում: Պատճառը Moodle համակարգի իրավասությունների բաշխման մեխանիզմն է, վերջինս իրավասությունները հատկացնում է օգտագործողին, միայն մուտքանվան իսկությունը ստուգելով: Գրոհի ժամանակ չափելով Moodle համակարգի արձագանքման ժամանակը, կարելի է կռահել, արդյոք տվյալ մուտքանունը ճիշտ է թե սխալ: Այս խնդիրը լուծելու նպատակով մշակվել է նոր ալգորիթմ, որը իրականացվել է moodlelib.php մոդուլում ինտեգրված authlib.php մոդուլի կողմից օգտատիրոջը տրված իրավասությունների և նույնականացման հաստատման հերթականություն փոփոխմամբ՝ նկ.9 [1]:



Նկ.9 Ճիշտ և սխալ մուտքանունների ներմուծման դեպքում LMS Moodle–ի արձագանքների ժամանակների համեմատումը թույլտվությունների փոփոխված բեռնման դեպքում:

Գլուխ 3-ում ներկայացված է մշակված «առցանց թեստավորման միջավայր» համակարգը: ՀՀ ԳԱԱ ԳԿՄԿ–ում ուսանողների քանակի աճին զուգընթաց ավելի ու ավելի արդիական խնդիր է դառնում հատուկ համակարգչային սարքավորումներով կահավորված քննասենյակների կառուցումը: Հաշվի առնելով ՀՀ–ում սոցիալտնտեսական դժվարին պայմանները՝ խոշոր ծախսերից խուսափելը ցանկացած հաստատության ամենաարդիական խնդիրներից մեկն է: Հատուկ համակարգչային սարքավորումներով կահավորված քննասենյակների կառուցումը ՀՀ ԳԱԱ ԳԿՄԿ–ի համար հանդիսանում է նշանակալի ծախս: Նմանատիպ ծախսերից խուսափելու համար խնդիր առաջացավ մշակել այնպիսի համակարգ, որը հնարավորություն կտա հատուկ սարքավորումներով կահավորված քննասենյակներում անց կացնելուն զուգահեռ առցանց քննություններ կազմակերպել նաև ուսանողների համակարգիչների միջոցով: Նկարագրված է մի համակարգ, որի օգնությամբ հնարավոր է օգտագործել քննություն հանձնողների համակարգիչները, սահմանափակելով դրանց հնարավորությունները, քննության ընթացքում օգտվել արտաքին ինֆորմացիայի աղբյուրներից, ինչպիսիք են օրինակ հիշողության ֆլեշ կրիչներ, համացանց և այլն: Մշակված համակարգը անվանվել է «Առցանց թեստավորման միջավայր» (ԱԹՄ) [3][4], որի մանրամասն նկարագիրը տրված է 3.4 բաժնում: Մասնակիցների համակարգիչների օգտագործումը քննության ընթացքում հանգեցում է մի շարք խնդիրների, ինչպիսիք են տվյալների բացահայտում, համակարգչում պահվող տեղեկությունների օգտագործման հնարավորություն, համացանցից օգտվելու հնարավորություն և այլն: Սույն հետազոտության նպատակն է ստեղծել անվտանգ միջավայր, որը քննություն հանձնողներին կտա, դեպի էլեկտրոնային քննական հարթակ մուտքի հնարավորություն՝ քննության ընթացքում օգտագործելով անհրաժեշտ ծրագրային ապահովումներ, միևնույն ժամանակ արգելափակելով

ցանկացած այլ ծրագրային ապահովումից, տեղեկատվական աղբյուրներից, համացանցից և այլն միջոցներից օգտվելու հնարավորությունը: **Բաժին 3.1-ում** թվարկվախ են առցանց առցանց թեստերի անվտանգության ռիսկերի գնահատման ընթացքում ի հայտ եկող հիմնական վտանգները [3]: Առցանց քննության ընթացում մասնակիցների համակարգիչների կիրառումը բերում է մի շարք խնդիրների, ինչպիսիք են տվյալների արտահոսքը, համակարգչում պահված ինֆորմացիայից օգտվելու հնարավորությունը, համացանցից օգտվելու հնարավորությունը և այլն: **Բաժին 3.2-ում** առաջարկված են կազմակերպմամ ընթացակարգ, քանի որ առցանց քննությունների անցկացման ընթացքում կարող են ի հայտ են գալ մի շարք խնդիրներ, որունց լուծման համար անհրաժեշտ է նախքան քննությունը սկսելը նախապատրաստվել: **Բաժին 3.3-ում** ներկայացված է մշակված «Առցանց թեստավորման միջավայր» համակարգը: Ուսումնասիրվել են գոյություն ունեցող լուծումները, որոնք կարող են համակարգիչը արգելափակել այնպես, որպեսզի նրա միջոցով հնարավոր լինի օգտվել միայն որոշակի ծրագրերից կամ վեբ կայքերից [4]: Այսպիսի լուծումները կիրառելու դեպքում անհրաժեշտություն է առաջանում որոշակի ծրագրային ապահովումներ տեղադրել ուսանողի անձնական համակարգչի վրա, ինչը կարող է ընդունելի չլինել ուսանողի կողմից: Մշակված ինքնագործարկվող ԱԹՄ համակարգը կարող է գործարկվել USB կրիչից, DVD սկավառակից կամ PXE սերվերից: Ինքնագործարկվող ԱԹՄ համակարգը կառուցված է Debian Linux օպերացիոն համակարգի հենքի վրա: ԱԹՄ համակարգը իրենից ներկայացնում է ծրագրային ապահովումների համալիր համատեղություն, որտեղ ներառված են Windows XP օպերացիոն համակարգը, XEN վիրտուալ մեքենան, SEB զննարկիչը, Debian Linux օպերացիոն համակարգը: ԱԹՄ համակարգի աշխատանքի մանրամասն նկարագրությունը ներկայացված է ստորև: Քննությունը սկսելու համար ուսանողը պետք է համակարգիչը համակցի քննասենյակի տեղական համկարգչային ցանցին և գործարկի ԱԹՄ–ն USB կրիչից, DVD սկավառակից կամ PXE սերվերից:

- Գործարկման առաջին փուլում միանում է Debian Live օպերացիոն համակարգը,
- երկրորդ փուլում կատարվում է համակարգչի բաղադրամասերի և ցանցային կապի հաստատման ստուգում,
- երրորդ փուլում, եթե խափանումներ չեն հայտնաբերվել, ինքնագործարկվում է ինտեգրված XEN վիրտուալ մեքենան, որն էլ իր հերթին գործարկում է վիրտուալ Windows Xp օպերացիոն համակարգը,

[3] Frank A. J., "Dependable Distributed Testing - Can the Online Proctor be Reliably Computerized?," ICETE 2010 Intl. Conf. on e-Business and Telecommunications, ICE-B Track, 22-31, July 2010.

[4] Shackleford D., "Managing Operating System (OS) Lock Down: Trusted Computer Solutions' Security Blanket Review", A SANS Whitepaper, March, 2010

- չորրորդ փուլում Windows Xp-ն գործարկում է SEB-ը և համակցում կրթական LMS Moodle սերվերին:

Ուսանողը ներմուծում է իրեն հատկացված մուտքանունը և գաղտնաբառը, այնուհետև ընտրում համապատասխան քննությունը:

Բաժին 3.4-ում և 3.5–ում թվարկված են ԱԹՄ համակարգում առկա սահմանափակումները և անվտանգության ապահովման լուծումները: Քննության ընթացքում ուսանողների միջև անմիջական շփումը պետք է կանխվի կազմակերպիչների միջոցով, իսկ համակարգչում նախօրոք տեղադրված ինֆորմացիայից, USB կրիչներից օգտվելը պետք է կանխվի տեխնիկական միջոցների կիրառմամբ: Բացի առցանց քննությունից, LMS Moodle-ը զրուցարանի և ակնթարթային հաղորդագրությունների հնարավորություն ունի, սակայն դրանք արգելափակում են SEB զննարկիչի միջոցով: Եթե որևէ մեկը, խաբեության նպատակով փորձի մուտք գործել LMS Moodle-ի թեստավորման միջավայր SEB զննարկիչից բացի մի ուրիշ զննարկիչի միջոցով, մուտքը չի թույլատրվի: մշակված ԱԹՄ համակարգը ունի անվտանգություն ապահովող հետևյալ հատկությունները՝

- Հարմարեցված Debian LiveCD-ն ապահովում է գրեթե բոլոր համակարգիչների ճանաչելիությունը և համակարգչում առկա տվյալներից օգտվելիս արգելափակումը:
- Debian LiveCD-ում առկա firewall–ի միջոցով արգելափակված է ուսանողի մուտքը դեպի համացանց և միևնույն ցանցում գտնվող այլ համակրգիչներ, բացառությամբ դեպի LMS Moodle համակարգ:
- LMS Moodle-ում ինտեգրված է SEB զննարկիչի կիրառումը, որը սահմանափակում է LMS Moodle-ի տրամադրած ծառայություններից օգտվելը:
- ԱԹՄ համակարգում ներդրված է սերտիֆիկացման համակարգ, որի շնորհիվ մուտքը դեպի քննական միջավայր հնարավոր է միայն ԱԹՄ համակարգից:

ԱԹՄ համակարգում կիրառվել են տարբեր գործիքներ, որոնք հնարավորություն են տալիս արգելափակել համակարգչի աշխատանքային սեղանը, օպերացիոն համակարգը, և վեբ զննարկիչը: ԱԹՄ համակարգի ներսում արգելափակված են հետևյալ գործողությունները՝

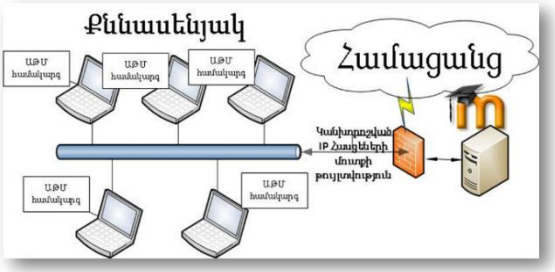
- ✓ տվյալների կտրում, պատճենում, արտատպում դեպի ԱԹՄ համակարգ և ԱԹՄ համակարգից,
- ✓ աշխտանքային էկրանի սևեռում, տպում, ղեկավարման վահանակի և օպերացիոն համակարգում առկա ծրագրերի գործարկում, մկնիկի աջ կոճակի գործարկում,
- ✓ նամակագրություն, աշխտանքային էկրանի փոխանցում, ցանցի հասկում,
- ✓ վեբ կայքերի դիտում,
- ✓ զննարկիչի մենյուի, կոճակների և գործիքների գործարկում՝ բացառութամբ հետ/առաջ/թարմացում/կանգ կոչակնորը,
- ✓ HTML ակունքային կոդի դիտում ,

- ✓ վեբ կայքերի պահպանումը զննարկիչի հիշողության մեջ,
- ✓ ամբողջական էկրանով բացված թեստային պատուհանի փոքրացում,
- ✓ cookie-ների, ժամանակավոր հիշողության և ժամանակավոր հիշված ֆայլերի դիտում:

Բաժին 3.6–ում ներկայացված են ԱԹՄ և քննական համակարգերի միջև ցանցային միացումների ցանկալի կառուցվածքը: Լարային ինֆրակառուցվածքի դեպքում հնարավոր է արգելափակել բոլոր IP հասցեների խմբերին, որոնք թույլատրված չեն քննական համակարգին միանալու համար: Քննությանը կարող են մասնակցել միայն այն համակարգերը, որոնք գտնվում են քննասենյակում, համակցված են լարային ցանցին, և որոնցում տեղադրված է SEB ծրագիրը

Ինչպես պատկերված է նկ.10-ում, մուտքը դեպի քննություն հնարավոր է, եթե բավարարված են հետևյալ պահանջները՝

- ➢ համակարգիչները աշխատում են ԱԹՄ համակարգում, որում առկա է SEB զննարկիչը
- ➢ համակարգիչները ֆիզիկապես համակցված են քննասենյակի լարային ցանցին:



Նկ. 10 Քննասենյակի և քննական համակարգի միջցանցային կառուցվածքը:

Գլուխ 4-ում ներկայացված են LMS Moodle համակարգում ներդրված կոնֆերանս և էլեկտրոնային դեկանատ համակարգերը: Աշխատանքում նկարագրվում է մի համակարգ, որը հնարավորություն է տալիս ուսանողներին հեռակա կարգով մասնակցել ինտերակտիվ դասընթացներին, միաժամանակ հնարավորություն տալով դասընթացների ընթացքում մասնակցել էլեկտրոնային ուսուցմանը ներդրված կոնֆերանս համակարգի միջոցով:

Բաժին 4.1-ը նկարագրում է ներդրված կոնֆերանս համակարգը: Ուսանուղների և դասախոսների անմիջական փոխադարձ շփումը, դասախոսի կողմից ուսանողներին տեսնելու և իսկությունը ստուգելու նպատակով էլեկտրոնային ուսուցման համակարգերում անհրաժեշտություն է առաջանում կիրառել կոնֆերանս համակարգեր: Այսպիսի խնդիրների լուծման նպատակով LMS Moodle համակարգում ներդրվել է

BigBluButton կոնֆերանս համակարգը: BigBlueButton–ը իրական ժամանակում սլայդերի, պատկերների, համակարգչների աշխատանքային էկրանների, ընդհանուր և անձնական զրուցարանների փոխդիտման, տվյալների և ձայնի փոխանակման, ինչպես նաև ուսանողների և դասախոսի միջև ինտերակտիվ շփման հնարավորություն է տալի: Այս համակարգի միջոցով հնարարավոր է կատարել դասախոսությունների տեսաձայնագրում: **Բաժին 4.2–ում** դիտարկվում են Էլեկտրոնային դեկանատի ֆունկցիոնալ հնարավորություններն ու առավելությունները: Էլեկտրոնային դեկանատը հանդիսանում է "բլոկ" տիպի մոդուլ LMS Moodle ծրագրի համար: Վերոհիշյալ մոդուլը հնարավորություն է տալիս ստեղծել մի ինֆրակառուցվածք, որը պարզեցնում է թե՛ ուսումնական բաժնի աշխատակիցների, թե՛ ուսանողների տեղեկացված լինելը կրթական համակարգում տեղի ունեցող փոփոխություններին:

Աշխատանքի հիմնական արդյունքները

- Մշակվել և ներդրվել են մեխանիզմներ, որոնք ապահովում են LMS Moodle համակարգի պաշտպանությունը և հուսալիությունը սեանսի առևանգում, սեանսի ամրագրում, օգտատիրոջ մուտքանվան և գաղտնաբառի գուշակում ուղղակի գրոհով հարձակումներից [1]:
- Մշակվել է ԱԹՄ համակարգը, որի միջոցով հնարավոր է ուսանողների համակարգիչների միջոցով անց կացնել անվտանգ առցանց քննություններ [3, 4]:
- Մշակվել է LMS Moodle համակարգում էլեկտրոնային դեկանատ մոդուլի հայալեզու միջերես [2]:
- իրականացվել է LMS Moodle համակարգում BigBlueButton կոնֆերանս համակարգի ինտեգրումը [2]:

Հրատարակված աշխատությունների ցանկ

[1] Arakelyan V., "Vulnerable Security Problems in Learning Management System (LMS) Moodle", Transactions of IIAP NAS RA, Mathematical Problems of Computer Science, vol. 39, pp. 129-134, 2013

[2] Arakelyan V., "Organizing of a Virtual Learning Environment at the International Scientific Educational Center of NAS RA", In Proc. of the 9 th International Conference on Computer Science and Information Technologies, Yerevan, Armenia, September 26-30, pp.437-440, 2013

[3] Arakelyan V., "New Solutions for Secure Online Testing", ITA 2013 – ITHEA ISS Joint International Events on Informatics Winter Session, December 18–19, Sofia, Bulgaria, 2013

[4] Arakelyan V., "Secure Online Testing System for LMS Moodle", Transactions of IIAP NAS RA, Mathematical Problems of Computer Science, vol. 41, pp 38-46, 2014

В. А. Аракелян

Исследование проблем информационной безопасности в системах электронного обучения

РЕЗЮМЕ

Диссертация посвящена исследованию задач безопастности и целостности электронных систем обучения LMS Moodle, по скольку подавляющее их число, использующихся на территории Республики Армения, реализованы на этой платформе.

Преимуществами электронного обучения в сфере образования являются относительно низкая стоимость, возможность обращения ко многим источникам учебной информации (электронным библиотекам, банкам данных, базам знаний и т.д.), равные возможности получения образования независимо от места проживания, состояния здоровья, элитарности и материальной обеспеченности обучаемых, использование в образовательном процессе новейших достижений информационных и телекоммуникационных технологий.

В результате исследований было выявлено, что, не смотря на многочисленные преимущества, в данной система имеются недостатки в сфере безопасности и целостности. Система LMS Moodle уязвима к различным типам атак. А это, в свою очередь, может привести к сбою работы системы, фальсификации результатов экзаменов, потери или утечки вопросников и других данных.

Целью данной работы является исследование и предложение таких решений, которые позволят сделать эту систему более защищённой, надежной и доступной. А так же создать возможность для проведения онлайн безопасных экзаменов с компьютеров студентов, избегая процесса создания дорогостоящих специально оборудованных классов. В отличие от существующих систем, разработанная «Среда онлайн тестирование» система работает независимо от операционной системы ПК, без каких-либо программных изменений в компьютере студента, что приводит к экономии времени и человеческих ресурсов.

В рамках диссертации были получены следующие результаты:

- Разработаны и внедрены механизмы, обеспечивающие защиту и надежность системы LMS Moodle от атак перехвата сессии, ее фиксации и определение входных данных (логин, пароль) пользователя [1].
- Разработана система, позволяющая проводить онлайн безопастные экзамены с использованием студенческих компьютеров [3, 4].
- Разработан армяноязычный интерфейс модуля электронного деканата в системе LMS Moodle [2].
- В системе LMS Moodle реализована интеграция BigBlueButton конференс-системы [2].

Предложенные механизмы защиты могут быть применены в системах, работующих на платформе LMS Moodle, для обеспечения эффективного и защищенного, от определенных типов атак, онлайн обучения.

Благодаря созданной среде онлайн тестирования, возможно проводить безопастные экзамены, с использованием студенческих компьютеров, в случае недостатка мест в экзаменационных помещения.

В систему LMS Moodle внедрены армяноязычный электронный деканат и конференс система, которая обеспечивает общение между преподавателями и студентами, дает возможность преподавателям видеть и идентифицировать студентов.

V. A. Arakelyan

Investigation of information security issues in e-learning systems

Summary

The thesis is devoted to the study of issues of security and integrity of e-learning systems, particularly to LMS Moodle system, as the vast majority of e-learning systems used in the Republic of Armenia are based on LMS Moodle system. Advantages of e-learning in education is relatively low cost, access to many sources of academic information (digital libraries, databases, knowledge bases, etc.), equal educational opportunities regardless of place of residence, health status, elitism and material status of the trainee, the use of the newest achievements in the educational process information and telecommunication technologies.

Studies have found that despite the numerous advantages, there are weaknesses in the area of security and integrity in this system. The LMS System Moodle is vulnerable to various types of attacks. This, in turn, can lead to failure of the system, the falsification of exam results, loss or diversion of questionnaires and other data.

The aim of this work is to investigate and propose solutions that will make the system more protected, secure and available. As well as to create a safe online exams with student computer, avoiding the costly process of creating specially equipped classrooms. Unlike existing systems, created “Online Testing Environment” system works independently of operating system PCs, without any software changes in the student's computer, which saves time and human resources.

Within the framework of the thesis the following results were obtained:

- The mechanisms were developed and implemented to ensure system security and reliability in LMS Moodle from direct attacks of session hijacking, session fixation, user login and password prediction [1].
- A system was developed through which it is possible to conduct secure online exams using the students’ computers [3, 4].

- Armenian interface was developed for electronic deanary in the LMS Moodle system [2].
- The integration of conference system BigBlueButton is realized in the LMS Moodle [2].

The proposed security mechanisms can be applied to e-learning environments using the LMS Moodle system to ensure efficient e-learning and protection from certain types of attack.

With the use of the created “Online Testing Environment” system it is possible to conduct secure online exams using the students' computers in case of specially equipped insufficient examination rooms.

Armenian-language electronic deanery and conference systems are embedded in the LMS Moodle, which provide communication between teachers and students, help teachers to see and identify the students.

Ծավալը՝ 20 էջ: Տպաքանակը՝ 100:
ՀՀ ԳԱԱ ԻԱՊԻ կոմպյուտերային պոլիգրաֆիայի լաբորատորիա:
Երևան, Պ. Սևակի 1