GOCE DELCEV UNIVERSITY, SHTIP, NORTH MACEDONIA

FACULTY OF ELECTRICAL ENGINEERING

ETIMA 2021

FIRST INTERNATIONAL CONFERENCE

19-21 OCTOBER, 2021

TECHNICAL SCIENCES APPLIED IN ECONOMY, EDUCATION AND INDUSTRY

УНИВЕРЗИТЕТ „ГОЦЕ ДЕЛЧЕВ” - ШТИП
ЕЛЕКТРОТЕХНИЧКИ ФАКУЛТЕТ

UNIVERSITY „GOCE DELCHEV” - SHTIP
FACULTY OF ELECTRICAL ENGINEERING

ПРВА МЕЃУНАРОДНА КОНФЕРЕНЦИЈА
FIRST INTERNATIONAL CONFERENCE

ЕТИМА / ETIMA 2021

ЗБОРНИК НА ТРУДОВИ
CONFERENCE PROCEEDINGS

19-21 Октомври 2021| 19-21 October 2021

Главен и одговорен уредник / Editor in Chief
Проф.д-р Сашо Гелев
Prof.d-r Saso Gelev

Јазично уредување / Language Editor
Весна Ристова (Македонски) / Vesna Ristova (Macedonian)

Техничко уредување / Technical Editing
Доц.д-р Далибор Серафимовски / d-r Dalibor Serafimovski

Издавач / Publisher
Универзитет „Гоце Делчев" - Штип / University Goce Delchev - Stip
Електротехнички факултет / Faculty of Electrical Engineering

Адреса на организационен комитет / Adress of the organizational committee
Универзитет „Гоце Делчев" – Штип / University Goce Delchev - Stip
Електротехнички факултет / Faculty of Electrical Engineering
Адреса: ул. „Крсте Мисирков" бр. 10-А / Adress: Krste Misirkov, 10 - A
Пош. фах 201, Штип - 2000, С.Македонија / PO BOX 201, Stip 2000, North Macedonia
E-mail: conf.etf@ugd.edu.mk

CIP - Каталогизација во публикација
Национална и универзитетска библиотека "Св. Климент Охридски", Скопје

62-049.8(062)
004-049.8(062)

МЕЃУНАРОДНА конференција ЕТИМА (1 ; 2021)
Зборник на трудови [Електронски извор] / Прва меѓународна конференција ЕТИМА 2021, 19-21 Октомври 2021 = Conference proceedings / First international conferece ETIMA 2021, 19-21 October 2021 ; [главен и одговорен уредник Сашо Гелев]. - Штип: Универзитет "Гоце Делчев", Електротехнички факултет = Shtip: University "Goce Delchev", Faculty of Electrical Engineering, 2021

Начин на пристапување (URL): https://js.ugd.edu.mk/index.php/etima. - Текст во PDF формат, содржи 358 стр.илустр. - Наслов преземен од екранот. - Опис на изворот на ден 15.10.2021. - Трудови на мак. и англ. јазик. - Библиографија кон трудовите

ISBN 978-608-244-823-7

1. Напор. ств. насл.
а) Електротехника -- Примена -- Собири б) Машинство -- Примена -- Собири
в) Автоматика -- Примена -- Собири г) Информатика -- Примена -- Собири

COBISS.MK-ID 55209989

Прва меѓународна конференција ЕТИМА
19-21 Октомври 2021
First International Conference ETIMA
19-21 October 2021

ОРГАНИЗАЦИОНЕН ОДБОР
ORGANIZING COMMITTEE

Василија Шарац / Vasilija Sarac
Електротехнички факултет,
Универзитет „Гоце Делчев" - Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delchev University - Stip, North Macedonia

Сашо Гелев / Saso Gelev
Електротехнички факултет,
Универзитет „Гоце Делчев" - Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delchev University - Stip, North Macedonia

Тодор Чекеровски / Todor Cekerovski
Електротехнички факултет,
Универзитет „Гоце Делчев" - Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delchev University - Stip, North Macedonia

Далибор Серафимовски / Dalibor Serafimovski
Електротехнички факултет,
Универзитет „Гоце Делчев" - Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delchev University - Stip, North Macedonia

Маја Кукушева Панева / Maja Kukuseva Paneva
Електротехнички факултет,
Универзитет „Гоце Делчев" - Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delchev University - Stip, North Macedonia

Билјана Читкушева Димитровска / Biljana Citkuseva Dimitrovska
Електротехнички факултет,
Универзитет „Гоце Делчев" - Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delchev University - Stip, North Macedonia

Весна Конзулова / Vesna Konzulova
Електротехнички факултет,
Универзитет „Гоце Делчев" - Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delchev University - Stip, North Macedonia

Прва меѓународна конференција ЕТИМА
19-21 Октомври 2021
First International Conference ETIMA
19-21 October 2021

ПРОГРАМСКИ И НАУЧЕН ОДБОР
SCIENTIFIC COMMITTEE

Со Ногучи / So Noguchi
Висока школа за информатички науки и технологии
Универзитет Хокаидо, Јапонија
Graduate School of Information Science and Technology
Hokkaido University, Japan

Дионис Гашпаровски / Dionýz Gašparovský
Факултет за електротехника и информациони технологии,
Словачки Технички Универзитет во Братислава, Словачка
Faculty of Electrical Engineering and Information Technology
Slovak Technical University in Bratislava, Slovakia

Антон Белан / Anton Beláň
Факултет за електротехника и информациони технологии
Словачки Технички Универзитет во Братислава, Словачка
Faculty of Electrical Engineering and Information Technology
Slovak Technical University in Bratislava, Slovakia

Георги Иванов Георгиев / Georgi Ivanov Georgiev,
Технички Универзитет во Габрово, Бугарија
Technical University in Gabrovo, Bulgaria

Ивелина Стефанова Балабанова / Ivelina Stefanova Balabanova,
Технички Универзитет во Габрово, Бугарија
Technical University in Gabrovo, Bulgaria

Бојан Димитров Карапенев / Boyan Dimitrov Karapenev
Технички Универзитет во Габрово, Бугарија
Technical University in Gabrovo, Bulgaria

Сашо Гелев / Saso Gelev
Електротехнички факултет,
Универзитет „Гоце Делчев” - Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delchev University - Stip, North Macedonia

Влатко Чингоски / Vlatko Cingoski
Електротехнички факултет,
Универзитет „Гоце Делчев” - Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delchev University - Stip, North Macedonia

Божо Крстајиќ / Bozo Krstajic
Електротехнички факултет
Универзитет во Црна Гора, Црна Гора
Faculty of Electrical Engineering,
University in Montenegro, Montenegro

Милован Радуловиќ / Milovan Radulovic
Електротехнички факултет
Универзитет во Црна Гора, Црна Гора
Faculty of Electrical Engineering,
University in Montenegro, Montenegro

Гоце Стефанов / Goce Stefanov
Електротехнички факултет,
Универзитет „Гоце Делчев” - Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delchev University - Stip, North Macedonia

Мирјана Периќ / Mirjana Peric
Електронски факултет
Универзитет во Ниш, Србија
Faculty of Electronic Engineerig,
University of Nis, Serbia

Ана Вучковиќ / Ana Vuckovic
Електронски факултет
Универзитет во Ниш, Србија
Faculty of Electronic Engineerig,
University of Nis, Serbia

Тодор Чекеровски / Todor Cekerovski
Електротехнички факултет,
Универзитет „Гоце Делчев” - Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delchev University - Stip, North Macedonia

Далибор Серафимовски / Dalibor Serafimovski
Електротехнички факултет,
Универзитет „Гоце Делчев” - Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delchev University - Stip, North Macedonia

Мирослава Фаркаш Смиткова / Miroslava Farkas Smitková
Факултет за електротехника и информациони технологии
Словачки Технички Универзитет во Братислава, Словачка
Faculty of Electrical Engineering and Information Technology
Slovak Technical University in Bratislava, Slovakia

Петер Јанига / Peter Janiga
Факултет за електротехника и информациони технологии
Словачки Технички Универзитет во Братислава, Словачка
Faculty of Electrical Engineering and Information Technology
Slovak Technical University in Bratislava, Slovakia

Јана Радичова / Jana Raditschová,
Факултет за електротехника и информациони технологии
Словачки Технички Универзитет во Братислава, Словачка
Faculty of Electrical Engineering and Information Technology
Slovak Technical University in Bratislava, Slovakia

Драган Миновски / Dragan Minovski
Електротехнички факултет,
Универзитет „Гоце Делчев" - Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delchev University - Stip, North Macedonia

Василија Шарац / Vasilija Sarac
Електротехнички факултет,
Универзитет „Гоце Делчев" - Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delchev University - Stip, North Macedonia

Александар Туџаров / Aleksandar Tudzarov
Електротехнички факултет,
Универзитет „Гоце Делчев" - Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delchev University - Stip, North Macedonia

Владимир Талевски / Vladimir Talevski
Електротехнички факултет,
Универзитет „Гоце Делчев" - Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delchev University - Stip, North Macedonia

PREFACE

The Faculty of Electrical Engineering at University Goce Delcev (UGD), has organized the International Conference ***Electrical Engineering, Informatics, Machinery and Automation - Technical Sciences applied in Economy, Education and Industry-ETIMA*.**
ETIMA has a goal to gather the scientists, professors, experts and professionals from the field of technical sciences in one place as a forum for exchange of ideas, to strengthen the multidisciplinary research and cooperation and to promote the achievements of technology and its impact on every aspect of living. We hope that this conference will continue to be a venue for presenting the latest research results and developments on the field of technology.
Conference ETIMA was held as online conference where contributed more than sixty colleagues, from six different countries with forty papers.
We would like to express our gratitude to all the colleagues, who contributed to the success of ETIMA'21 by presenting the results of their current research activities and by launching the new ideas through many fruitful discussions.
We invite you and your colleagues also to attend ETIMA Conference in the future. One should believe that next time we will have opportunity to meet each other and exchange ideas, scientific knowledge and useful information in direct contact, as well as to enjoy the social events together.

The Organizing Committee of the Conference

ПРЕДГОВОР

Меѓународната конференција ***Електротехника, Технологија, Информатика, Машинство и Автоматика-технички науки во служба на економија, образование и индустрија-ЕТИМА*** е организирана од страна на Електротехничкиот факултет при Универзитетот Гоце Делчев.
ЕТИМА има за цел да ги собере на едно место научниците, професорите, експертите и професионалците од полето на техничките науки и да представува форум за размена на идеи, да го зајканува мултидисциплинарното истражување и соработка и да ги промовира технолошките достигнувања и нивното влијание врз секој аспект од живеењето. Се надеваме дека оваа конференција ќе продолжи да биде настан на кој ќе се презентираат најновите резултати од истражувањата и развојот на полето на технологијата.
Конференцијата ЕТИМА се одржа online и на неа дадоа свој допринос повеќе од шеесет автори од шест различни земји со четириесет труда.
Сакаме да ја искажеме нашата благодарност до сите колеги кои допринесоа за успехот на ЕТИМА'21 со презентирање на резултати од нивните тековни истражувања и со лансирање на нови идеи преку многу плодни дискусии.

Ве покануваме Вие и Вашите колеги да земете учество на ЕТИМА и во иднина. Веруваме дека следниот пат ќе имаме можност да се сретнеме, да разменime идеи, знаење и корисни информации во директен контакт, но исто така да уживаме заедно и во друштвените настани.

Организационен одбор на конференцијата

Содржина / Table of Contents

UDC: 004.738.5:37]:004.457.056.5

E-LEARNING – CYBER SECURITY CHALLENGES AND PROTECTION MECHANISMS

Dimitar Bogatinov[3] Goce Stevanoski,[2] Monika Kachurova[1]

[1]Military academy "General MihailoApostolski" – Skopje, University "GoceDelcev" - Stip, N.Macedonia, monikakacurova@hotmail.com
[2]Military academy "General MihailoApostolski" – Skopje, University "GoceDelcev" - Stip, N.Macedonia, goce.stevanoski@ugd.edu.mk
[3]Military academy "General MihailoApostolski" – Skopje, University "GoceDelcev" - Stip, N.Macedonia, dimitar.bogatinov@ugd.edu.mk

Abstract
In the successful functioning of modern society, the traditional educational methods are not enough, and new methods must be introduced. Given the constant development of technology today, a high-quality workforce is needed as much as possible. The fast changes in the modern way of living are forcing a life in virtual spaces, in which smart devices are an essential part.
The e-learning concept offers several advantages to educational organizations that use this technology, including short and effective training, flexibility, and modulation. The Internet is increasingly used for a variety of online courses, so one of the essential tasks is understanding the e-learning security issues. The security aspect is very important for the companies creating e-learning platforms, which should consider the safety of the instructors, the students, as well as the companies / educational institutions that use the services. In this paper, we will look at the threats to the security and privacy of the most popular e-learning systems and suggest methods for overcoming those challenges.

Keywords: e-learning, threats, security and privacy.

Вовед и преглед на литература

Денес, кога станува збор за образованието, напредувањето во дигиталната технологија станува суштинска ставка во нашето секојдневие. Бидејќи сè повеќе начинот на пренесување на знаења се сведува преку интернет, треба да ги разбереме безбедносните проблеми на електронското учење. Безбедносниот аспект е уште поважен за компаниите кои користат системи за е-учење за да испорачуваат курсеви за обука на своите вработени. Е-учењето е нов метод на учење кој зависи од Интернет при неговото извршување и е добро познато дека интернетот стана место за нов пакет на незаконски активности, така што околината за е-учење е изложена на многу ризици и закани. Ризикот се појавува при електронски пренос на информациите, додека заканата подразбира предвидена опасност. Вообичаени закани за компјутерите се вируси, мрежни продирања, кражби и неовластено модифицирање на податоците, прислушување и недостапност на сервери и персонални компјутери.

За време на преносот, оригиналните документи можат да бидат изменети, поправени или уништени од активните и пасивни напади на хакерите. Како поизложена технологија на вообичаени закани и ризици е електронското учење.

Електронското учење

Е-учење е обединувачки термин за да се опише учењето преку Интернет, обука базирана на веб-страници и упатства засновани на технологија. Обично, поимот е - учење подразбира курсеви, настава или обуки преку Интернет [1].

Подолу се дадени некои карактеристики на системите за е-учење:

- Процесот на учење се врши во виртуелна училница;
- Едукативниот материјал е достапен на Интернет и вклучува текст, слики, врска до други мрежни ресурси, слики, аудио и видео презентации;
- Виртуелната училница е координирана од инструктор кој ја планира активноста на учесниците во работните групи, дискутира за аспектите на курсот со помош на форум за разговор или разговор, обезбедува помошни ресурси, итн.;
- учењето станува социјален процес;
- поголемиот дел од системите за е-учење овозможуваат следење на активностите на учесниците, а некои од нив, исто така, вклучува и симулации и работа на подгрупи.

Концептот на е-учење нуди неколку предности на образовните организации што ја користат оваа технологија, вклучувајќи кратка и ефикасна обука, флексибилност и модулизација. Повеќето иновации за е-учење се фокусираат на развојот на курсот и начинот на презентирање, со малку или воопшто посветување на внимание на приватноста и безбедноста како потребни елементи. Сепак, од горенаведените трендови, јасно е дека ќе има поголема потреба од високи нивоа на доверливост и приватност во апликациите за е-учење и дека мора да се воспостават безбедносни технологии за да се задоволат овие потреби. Исполнувањето на безбедносните барања во системот за е-учење е исклучително комплексен проблем затоа што е неопходно да се заштитат содржината, услугите и личните податоци, не само за надворешните корисници, туку и за внатрешните корисници, вклучително и администраторите на системот.

Закани и ризици

Загубата на средството е предизвикана од реализација на закани или ризици. Сите закани се реализираат преку медиум на ранливост [2].

Главните закани се:

- Прекршување на доверливоста;
- Повреда на интегритетот;
- Одбивање на услугата: Спречување на легитимни права за пристап со нарушување на сообраќајот за време на комуникацијата меѓу корисниците на системот за е-учење.
- Нелегитимна употреба: Експлоатација на привилегии од легитимни корисници;
- Злонамерна програма: Код за оштетување на програми;
- Одрекување: Лица што негираат учество во пренос на документи;
- Анализа на сообраќајот: протекување на информации со злоупотреба на комуникацискиот канал;

- Brute force attack: Обид со сите можни комбинации да се открие лозинката.

<u>Можни ризици на креаторите на содржини</u>

Современата технологија им овозможи на креаторите на содржини да обезбедат пристап до материјали како книги, списанија, итн. Креаторите на содржини се одговорни да ја развиваат и имплементираат содржината. Причината зошто многу креатори на содржини се воздржуваат од обезбедување е стравот дека нивниот составуван материјал може да биде предаден и обработен без нивно знаење. Должноста на креаторот на содржини е да се заштити од неовластена употреба, модификација и повторна употреба на податоците во различни контексти поврзани со е-учење.

Белешките на креаторите на содржини може да бидат модифицирани / уништени од хакерите преку напади. Затоа, во интерес на креаторот на содржини е да се осигура дека корисниците ја добиваат содржината непроменета и дека корисниците можат да го проверат интегритетот на текстот.

<u>Можни ризици на професорите</u>

Професорите се одговорни за обезбедување на секоја можна поддршка на студентите во врска со академската материја. Професорите можат да ја следат или да купат содржината на курсот, презентации од трето лице според барањата на курсот. Сите ризици од е-учењето не треба да бидат ограничени на техничкиот систем. Неопходно е да се опфатат целокупните методи на предавање, испитување и оценување. Методологиите на наставата се менуваат од еден наставник на друг, но ќе има вообичаени ризици во настаните како што се предавање, испраќање белешки и задачи, прифаќање и обележување листови со одговори, подготвување и дистрибуирање на тестови. Дискусиите се основна компонента на наставата на кој било курс. Една форма на дискусија може да биде преку онлајн форумот.

Предност на дискусиите на форумите преку Интернет во однос на усните дискусии е тоа што сите пишани документи се чуваат електронски на серверот, но дигиталното складирање на материјали претставува голем ризик за приватноста на студентите, како и на Професорите.

Покрај тоа, постои ризик во системот за испити што вклучува стандардизација на прашањата за испит и список на прашања што може да ја ограничат академската слобода на одделни наставници. Мора да постои тим што ќе се грижи за сите овие ризици. Ризикот поврзан со испитување е директно поврзан со мамење. Освен мамењето, Професорите мора да бидат загрижени за достапноста на оценките. Исто така, за време на испитувањето студентите се повеќе сакаат да соберат материјали за проучувањето на содржината. Сите наставници мора да бидат свесни за ризикот студентите да добијат непроменет прашалник пред почетокот на испитите и сите одговори да се чуваат на непроменет начин. Иако предавањето е наједноставна и природна форма на комуникација, останува секогаш ризикот од модификација на предавањето на час (говор) за време на предавањето.

Можни ризици кај студентите

Максимален број на корисници во системот Е-Учење се студентите кои учат и го споделуваат своето знаење со други во системот. Студентската група може да се класифицира на различни нивоа од низок степен, дипломски, постдипломски, до ниво на докторски студии. Но, секој корисник мора да биде свесен за секој материјал добиен од институтот, Професорите или другите студенти. Од друга страна, доколку натрапниците ги уредувале документите со прашања или други важни документи, потоа студентите ќе треба да се соочат со проблеми во моментот на испитувањето.

Покрај тоа, постои ризик од зачувување на информации за најава (корисничко име и лозинки). Сите студенти мора да бидат свесни за злоупотреба на информации за најава, во спротивно напаѓачот може да се обиде да го спречи овластениот ученик да пристапува до серверот за Е-учење со горенаведените напади. Професорите не се секогаш достапни за да им помогнат на студентите, така што тие треба да бидат дисциплинирани да работат самостојно без помош на наставникот.

Студентите треба да имаат добри вештини за пишување и комуникација. Кога Професорите и другите студенти не се состануваат лице в лице, можно е да не се разберат, т.е. погрешно да се протолкуваат. Како механизам за повратна информација од постои ризик од страна на студентите да ги испратат истите повратни информации до раководството на институтот за е-учење. На крај, сите ученици треба да бидат свесни за фишингот каде напаѓачот поставува лажни веб-страници кои изгледаат како вистинска веб-страница за е-учење, така што тешко може да прави се разлика помеѓу вистинската и страната на напаѓачот. Овде често од студентите се бара да внесат некои доверливи информации.

Други закани и ризици при е-учење

Покрај горенаведените ризици, постојат и разни други закани присутни во системот на е-учење, како:

Природни закани – може да бидат предизвикани од природни непогоди, како што се пожар, невреме, вулканска ерупција, земјотрес, поплави и др. Системот за електронско учење може да биде под влијание на овие закани.

Промислени– Заканите може да бидат од измама, уцена, кражба итн.

Ненамерни – Може да има некои неизбежни закани како компјутерска грешка, прекинување на електрична енергија, грешка во ракување итн.

Начини за справување со ризици

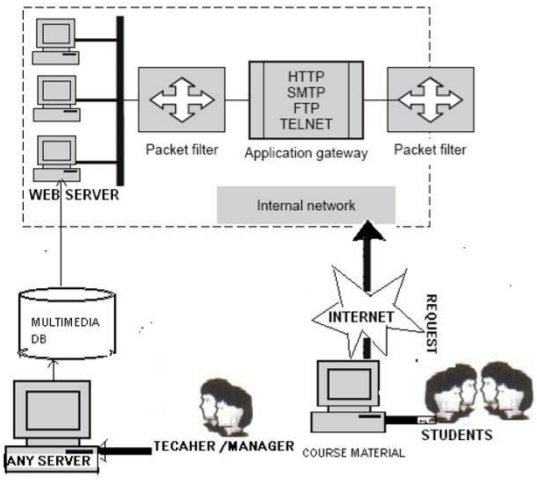
Учесниците на системот за е-учење се соочуваат со различни ризици или закани, како што беше дискутирано во претходниот дел. Следниве алатки или техники може да бидат наметнати за да се минимизираат овие ризици[3].

Контрола на пристап со помош на "Firewall"

Заштитен ѕид (Firewall) е комбинација на хардверски и софтверски систем за безбедност, воспоставен за да се спречи неовластен пристап до корпоративната мрежа од надвор во организацијата. Технички, заштитниот ѕид е специјализирана верзија на рутерот. Покрај

основните функции за рутирање и правила, рутерот може да се конфигурира за да ја изврши функционалноста на заштитниот sид, со помош на дополнителни софтверски ресурси.

Главниот принцип заснован на правилото е дека целиот сообраќај од внатре кон надвор и обратно, мора да помине низ заштитниот sид. За да се постигне ова, целиот пристап до локалната мрежа мора прво физички да се блокира, а пристапот само преку заштитниот sид треба да биде дозволен. Само сообраќајот овластен според локалната политика за безбедност треба да се дозволи да помине. Самиот заштитен sид мора да биде доволно силен, за да ги направи сите напади извршени врз него бескорисни. Во практични имплементации, заштитниот sид обично е комбинација на филтри и апликации. Еден таков заштитен sид е прикажан на сликата подолу. Пософистицираните заштитни sидови можат да блокираат извесен сообраќај од надвор, но да им дозволи на корисниците на Е-Учење (може да бидат студенти, наставници, итн.) да комуницираат слободно.



Слика 1: Организација на безбедносен sид базиран во е-учење

Значи, должноста на сите администратори на системот е да имаат знаење и вештини за спроведување на заштитниот sид, да го конфигурираат заштитниот sид и да ги следат и решаваат проблемите со заштитните sидови.

<u>Криптографија</u>

Целта на доверливоста е да се осигура дека информациите и податоците не се откриваат на кое било неовластено лице или субјект. Исто така, читателите мора да се потпрат на точноста на курсот. Една од техниките во овој аспект е криптографијата. Различни криптографски алатки и техники се потребни за примена на безбедноста во трансакциите базирани на интернет. Постојат два вида на алгоритми во криптографијата:

- Алгоритми на таен клуч
- Алгоритми со јавен клуч
- Алгоритми на таен клуч

Во алгоритмите со таен клуч, клучот за криптирање и декрипција е ист, тој бара испраќачот и примачот да се договорат за клучот пред комуникацијата, главната функција на овој алгоритам е криптирање на податоците. Примери на вакви алгоритми

се Стандард за криптирање на податоци (DES), Меѓународни алгоритми за криптирање на податоци (IDEA) и Напреден стандард за криптирање (AES).

Алгоритми со јавен клуч

Крипто-системите на јавниот клуч, од друга страна, користат еден клуч (јавниот клуч) за криптирање на пораки или податоци и втор клуч (тајниот клуч) за декриптирање на тие пораки или податоци. Тука главно се користат три математички модели – Факторизација, дискретни логаритми и елипсовидна крива. Различни алгоритми со јавен клуч се RSA, El-Gamal, DiffieHellman. Можеме да ги користиме овие техники за време на испраќање на хартија за прашања и примање на листови со одговори. За автентикација на учесник, можеме да ги користиме следниве технологии користејќи алгоритам за јавен клуч:

- Дигитален потпис
- Дигитален сертификат

Криптографија базирана на невронски мрежи

Криптографија базирана на невронски мрежи е нов пристап заснован на вештачки невронски мрежи (АНН) за безбедност на податоците во електронската комуникација. Претставува крипто-систем, кој се заснова на биолошки идеи, вклучително и мрежна архитектура, биолошки операции и процес на учење. Значи, сложеноста на генерирање на обезбедениот канал е линеарна со големината на мрежата. Овој биолошки механизам може да се користи за изградба на ефикасен систем за криптирање со употреба на клучеви кои се менуваат. Многу е едноставен и брзо може да се спроведе во случај на можен напад во моментот на пренесување на документ за е-учење.

Биометриска автентикација

Меѓу сите техники за автентикација како лозинки, паметна картичка, дигитален потпис и дигитален сертификат, не постои гаранција дека студентите ќе ја чуваат својата лозинка во тајност. Лозинката може да биде злоупотребена за време на поднесување на задача, примање на трудови, преземање на материјали од курсот и сл, каде што биометриската автентичност би давала поголема безбедност. Но, за ова треба малку повеќе инвестиции.

Заклучок

За успешно функционирање на современото општество и следење на трендовите на пазарот веќе не се доволни традиционални методи на образование, туку веќе има потреба од нови форми на стекнување со знаење. Со оглед на постојаниот развој на технологијата во денешно време, потребата за високообразована работна сила е се поголема. Постојаното забрзување на темпото на живот нè насочува кон виртуелниот свет и компјутерот станува дел од нашиот секојдневен живот. Важна карактеристика на учење од далечина е употреба на информациска и комуникациска технологија и од ден на ден се повеќе влијае на животот на поединецот, но и на целото општество и на тој начин и на нивниот образовен процес.

Развојот на системите за е-учење треба да се направи со користење на меѓународно признати методи и стандарди за безбедност. Системот треба да спроведе безбедносни механизми како што се автентикација, криптирање, контрола на пристап, управување со корисници и нивни дозволи. Безбедната платформа за учење треба да ги вклучи сите аспекти на безбедноста и да ги направи повеќето процеси потранспарентни за наставникот и ученикот.

Поради постојано забрзување на темпото на живот, кој оди заедно со технологијата, учењето на далечина се повеќе станува неопходност на денешното општество. Учењето од далечина станува препознатливо како многу важен и моќен начин за успешно управување со современото општество ширум светот, вклучително и кај нас.

Користена Литература

1. Creswell, J. W. „*Conducting Risk Assessments* 1 (2): 1-95. [10] Sugiyono. (2014) *MetodePenelitianManajemen"*[Title in English: *Research Method in Management*], Bandung, Alfabeta. (2016)
2. Dobre, I „The standard model of an e-learning platform". Bucharest, Romania, (2010). (Chapter 2)
3. Edgar, R. W. „Critical Study of the present e-learning systems", Academia Romana, Romania, (2005). (Chapter 2).
4. Jalal, A. & Ahmad, M. „Security in e-learning". Springer. Vienna University of Technology, Austria, (2008). (Chapter 1).
5. Kritzinger, E. &Solms S „Security Enhancement for E-Learning" Portal. Proceedinggs of International Journal of Computer Science and Network Security", Department of Computer Science City University, Peshawar, Pakistan, (2006). 41-45.
6. Kumar, S. & Kamlesh, D. "Information Security Management System Based on ISO/IEC 27001: 2005," E-learning: Incorporating Information Security Governance, Proceeding of Informing Science and IT Education Conference, Salford (Greater Manchester), England, (2011 Chazar, C. (2015), 319-325.
7. Norwood, Herry T., and P. Sandra. Catwell. *Cybersecurity, Cyber analysis and Warning*, New York, Nova Science Publisher, Inc (2009)
8. Pustaka Pelajar, *Research Design:„Quantitative, Qualitative Method*", 4th Ed., SAGE Publication, Yogyakarta.