E-COMMERCE SECURITY PROTOCOLS

Igor Kambovski
Faculty of Law, "Goce Delchev" University – Shtip, Republic of N. Macedonia
igor.kambovski@ugd.edu.mk

Abstract: Information technology is the fastest growing technology in the world. Countries that can not keep up with the pace of implementation of this technology are increasingly moving away from countries in the developed world and the gap between them is widening. With the relentless expansion of the Internet, all countries are increasingly introducing information technology in all areas of work and living. Globalization as an unstoppable process is perhaps most felt in commerce, especially Electronic commerce. E-commerce breaks down all boundaries and barriers. The terms "near" and "far" are lost in the virtual world of the Internet. Anyone who produces something through E-commerce can offer their product to millions and billions of potential buyers around the world. The term global market is becoming a reality. Also, banking in the world is experiencing a revival and has entered a new era with the advent of electronic banking. E-banks are already a reality today, they work 24 hours a day, 7 days a week. They are not crowded at the counters that do not really exist and they are ready to receive your payment order at any time. In an increasingly dynamic way of working and living, fast and reliable communication is the key to success. Electronic communication is becoming part of our daily lives. Electronic operation through modern and widely available information and telecommunication technology increases the efficiency and security of communications between entities in payments and in legal acts. The use of electronic technology enables the receipt, sending and storage of data in electronic form, as well as the creation of an electronic signature whose use in payment operations and transactions between other legal entities in payment operations becomes a necessary need. Due to all this, as well as for many other reasons, there is a need to check the authenticity and verification of electronic data, messages and texts. With proper application of security systems and protocols, everyday risks that are an integral part of E-commerce and online communications and transactions can be avoided. In terms of E-commerce, special attention is paid to the protection of confidential and personal data, which are the target of illegal activities of hackers who do it mostly for dishonest earnings, trading with them, but also for prestige and fame. For effective protection against such unauthorized access and use of information and data, E-commerce entities use cryptography as a data processing technique. Every system in which data is stored and processed belongs to the group of endangered systems and needs protection. In general, any person, object or event that could potentially endanger the data security in the system can be considered a threat. Therefore, these threats should be identified and prevented, and if they have already occurred, procedures should be implemented to eliminate them and minimize the damage.
Keywords: E-commerce, technology, security, cryptography

БЕЗБЕДНОСНИ ПРОТОКОЛИ КАЈ ЕЛЕКТРОНСКАТА ТРГОВИЈА

Игор Камбовски
Правен факултет, Универзитет „Гоце Делчев“ – Штип, Република С. Македонија
igor.kambovski@ugd.edu.mk

Резиме: Информатичката технологија е технологија со најбрз развој во светот. Земјите кои не можат да го следат темпото на имплементација на оваа технологија се повеќе се оддалечуваат од земјите во развиениот свет и се зголемува јазот меѓу нив. Но, со незапирливата експоанзија на Интернетот, сите земји се позасилено да ја воведуваат информатичката технологија во сите области на работење и живеење. Глобализацијата како несопирлив процес можеби најмногу се чувствува во трговијата, особено во електронската трговија. Е-трговијата ги руши сите граници и бариери. Поимите „блиску“ и „далеку“ се губат во виртуелниот свет на Интернетот. Секој кој произведува нешто преку Е-трговијата може да го понуди својот производ на милиони и милијарди потенцијални купувачи во целиот свет. Терминот глобален пазар станува реалност. Исто така, банкарството во светот доживува препород и навлезе во нова ера со појавата на електронското банкарство. Е-банките веќе денес се реалност, тие работат 24 часа, 7 дена во неделата. Кај нив нема гужва на шалтерите кои реално и не постојат и тие се подготвени во секое време да го примат вашиот налог за плаќање. Во се подинамичниот начин на работење и живеење, брзата и сигурна комуникација е клуч на успехот. Електронската комуникација станува дел од нашиот секојдневен живот. Електронското работење преку современата и широко достапна информатичка и телекомуникациска

технологија ја зголемува ефикасноста и сигурноста во комуникациите помеѓу субјектите во платниот и правниот сообраќај. Со употребата на електронската технологија се овозможува примање, праќање и чување на податоци во електронски облик, како и креирање на електронски потпис чие користење во платниот промет и прометот помеѓу другите правни субјекти во платниот промет станува нужна потреба . Поради сето ова, како и поради многу други причини, се наметнува потребата за проверка на автентичноста и верификација на електронските податоци, пораки и текстови. Со соодветна примена на безбедносни системи и протоколи можат да се избегнат секојдневните ризици кои се составен дел од електронската трговија и онлајн комуникациите и трансакциите. Во услови на Е-трговија особено внимание се посветува на заштитата на доверливите и тајните податоци, кои претставуваат цел на недозволените активности на хакерите кои тоа го прават најчесто заради нечесна заработка, тргување со истите, но и заради престиж и слава. Заради ефикасна заштита од таквите неовластени пристапи и користења на информациите и податоците, субјектите на Е-трговијата се служат со криптографијата како техника на процесирање на податоците. Секој систем во кој се чуваат и процесираат податоци спаѓа во групата на загрозени системи и потребна му е заштита. Генерално, како закана за секој систем можат да се сметаат секое лице, објект или настан кои потенцијално можат да доведат до загрозување на безбедноста на податоците во системот. Токму затоа, овие закани треба да се идентификуваат и да се спречат, а доколку веќе настапиле треба да се спроведат постапки за нивно отстранување и минимизирање на штетите.
Клучни зборови: Е-трговија, технологии, безбедност, криптографија

1. ВОВЕД

Во функција на остварување на безбедноста и сигурноста на корисниците на услугите на Електронската трговија е потребно да биде обезбедена соодветна правна рамка на условите за задоволување на потребите за комуникациските услуги, заштита на интересите на корисниците, условите за изградба, одржување, безбедност, надзор и користење на комуникациски мрежи и услуги и заштитата на тајноста и доверливоста на електронските комуникации. Во тој контекст, од особено значење е и употребата на информатичката и телекомуникациската технологија и употребата на електронските документи, електронската идентификација, креирањето доверливи услуги и податоци во електронски облик и електронски потпис. Исто така, прашањето на формата и валидноста на електронскиот документ е од особено значење за електронската трговија и онлајн трансакциите. Потребно е да се определат прецизни критериуми за да се гарантира неговата валидност и доказна моќ која е еднаква со дејството на пишаниот документ во постапката пред судовите, арбитражите и другите државни органи. Комерцијалната практика го употребува, а судовите го прифаќаат, пишаниот документ на хартија како сигурно и доверливо средство за чување информации. Информацијата пренесена од хартија на електронски медиум станува дематеријализирана и се претвара во електронски документ. Но, за тоа е потребно да бидат исполнети одредени услови за да таквите дематеријализирани документи имаат иста правна сила како и нивните верзии на хартија: да се обезбеди сигурноста во определување на идентитетот на страната која соопштува информација која се наоѓа во електронски документ; и да се обезбеди содржината на самиот електронски документ. Во секој случај, за изедначување на електронскиот документ со писмениот е неопходно да се осигура неговиот идентитет. Тоа подразбира: осигурување дека содржината на електронскиот документ нема да биде откриена на неовластено лице; осигурување на автентичноста на електронскиот документ, со што се штити од можно менување или бришење; гарантирање на доказната моќ на електронскиот документ во поглед на постоењето и содржината на трансакцијата, независно од правното опкружување во кое делуваат праќачот и примачот; обезбедување докази за определување одговорност на праќачот и примачот на електронскиот документ и евентуална одговорност на мрежниот провајдер на услуги на информатичкото општество.

2. КОН ЗАКОНОТ ЗА ЕЛЕКТРОНСКИТЕ КОМУНИКАЦИИ

Законот за електронските комуникации[50], меѓу другото, има за цел да обезбеди услови за задоволување на потребите за комуникациски услуги, забрзување на процесот на создавање на конкурентен пазар во областа на електронските комуникации, како и поттикнување на развојот на економијата во Р. Македонија. Законот

[50] Консолидиран текст на Законот е објавен во „Службен весник на РМ“ бр.39/14, 188/14, 44/15, 193/15, 11/18, 21/18, а со денот на влегување во сила на овој закон престана да важи Законот за електронските комуникации („Службен весник на РМ“ број 13/2005, 14/2007, 55/2007, 98/08, 83/10, 13/12, 59/12, 123/12 и 23/13).

е особено значаен од причина што дава објаснувања и дефиниции на некои основни инструменти на електронската трговија. Така, електронска комуникациска мрежа (чл. 3 точка 1.) е преносен систем и комутациска или насочувачка опрема и други средства вклучително мрежни елементи што не се активни, а коишто овозможуваат пренос на сигнали преку жичени, радиобранови, оптички или други електромагнетни средства, вклучувајќи сателитски мрежи, фиксни (со комутација на кола или комутација на пакети, вклучувајќи и Интернет) и мобилни земски мрежи, електроенергетски кабелски системи, доколку се користат за пренос на комуникациски сигнали, радиодифузни мрежи и кабелски телевизиски мрежи, независно од видот на информациите што се пренесуваат; Електронска комуникациска услуга (чл.3 точка 2) е услуга што вообичаено се нуди за надоместок, а која целосно или главно се состои од пренос на сигнали преку електронски комуникациски мрежи и ги вклучува телекомуникациските услуги и преносните услуги во мрежите наменети за емитување или реемитување на програмски содржини, но ги исклучува услугите кои овозможуваат или извршуваат уредувачка контрола врз содржините кои се пренесуваат со помош на електронските комуникациски мрежи или услуги, а не ги вклучува ниту услугите на информатичкото општество кои, целосно или делумно, не се состојат од пренос на сигнали преку електронски комуникациски мрежи. Услуги на информатичко општество (чл.3, т.14) се услуги што се обезбедуваат за надоместок на далечина преку електронски средства и на лично барање на примателот на услугата. "На далечина" означува дека услугата се обезбедува без истовремено присуство на две страни. "Преку електронски средства" значи дека услугата се испраќа од почетната/изворната точка и се добива на крајната дестинација преку електронска опрема за процесирање (вклучително и дигитална компресија) и чување на податоци и се испраќа, пренесува и добива во целост преку кабел, радиобранови, оптички средства или други електромагнетни средства. "На лично барање на примателот на услугата" значи дека услугите се обезбедуваат преку пренос на податоци на лично барање; Комуникација подразбира секоја информација што се разменува или пренесува меѓу ограничен број на страни преку јавни електронски комуникациски услуги, а не вклучува информации што се пренесуваат како дел од емитување на програмски содржини преку јавна електронска комуникациска мрежа, освен кога информацијата е наменета за одреден претплатник или корисник.

Електронскиот договор претставува договор склучен со користење на информациски технологии. Тој може во целост да биде склучен по електронски пат, или, пак, како комбинација на електронскиот метод и класичниот "хартиен" писмен метод. Како и традиционалниот договор, тој настанува во моментот на прифаќањето на понудата, односно во моментот на постигнувањето согласност на волјите на двете договорни страни. Склучувањето на електронскиот договор поставува неколку важни прашања во поглед на правниот аспект на тргувањето по електронски пат. Првото прашање е прашањето на валидност на таквиот договор, односно дали договорот склучен по електронски пат е полноважен и дали врз основа на таквиот одоговор може да се бара извршување на договорените обврски. Генерално, прифатен е ставот дека ваквиот тип договори се сметаат за полноважни, односно најголем број законодавства имаат донесено закони за електронската трговија, хармонизирани со меѓународните правни акти и правила, во кои е наведено дека на електронскиот договор не смее да му се оспорува полноважноста поради формата во која е склучен, односно поради отстапувањето од традиционалната писмена форма на договорите, но доколку исполнува определени услови кои постојат во светот на традиционалните пишани договори[51]. Таков пристап по ова прашање, или таканаречен функционално-еквивалентен пристап, има и УНЦИТРАЛ комисијата за меѓународно трговско право на Обединетите Нации. Имено, оваа комисија смета дека би бил преголем и неоправдан зафат да се пристапи кон менување на начелата на договорното право кои постоеле до појавата на електронските трансакции, и истите треба да се применат на новите технологии и теники на договарање, со дозволени неопходни прилагодувања. Во тој контекст, прашањето на полноважноста на електронските договори е решено со наведениот функционално-еквивалентен пристап, со соодветни прилагодувања на секој правен систем поединечно[52].

Второто битно прашање е прашањето на идентификација на договорните страни. Имено, како лицата кои комуницираат по електронски пат можат со сигурност да знаат дека понудата или прифаќањето на понудата го испраќа лице кое за тоа има овластување од страна на некоја фирма, преку службениот е-маил на фирмата, и дали не станува збор за лажно претставување заради измама (на пример, преку хакерски упад во компјутерскиот систем на фирмата заради извршување на недозволена и неовластена трансакција). Ова

[51] Le Tourneau Ph., (2003) *La Notion de Contrat Electronique,* Les deuxiemes journees internationals du droit du commerce electronique, Litex, Paris, стр.8

[52] Živković V., *Elektronska trgovina-Pravo Informacionih tehnologija*, Pravni fakutelt Univerzitet UNION, Službeni glasnik, Beograd, 2007, стр.132

прашање на почетокот на развојот на информациските технологии претставуваше голем проблем кој подоцна беше решен со развивањето и имплементацијата на системот за идентификација на учесниците во трансакциите со електронски потпис.

Електронскиот потпис претставува широк поим кој опфаќа различни начини на идентификација на лицата преку електронска верзија на своерачниот потпис, идентификација преку ПИН код (Personal Identification Number), биометрички потпис (идентификација на лицето преку неговите физички карактеристики, на пример, со скенирање на зеницата на окото, дланката, папиларните отисоци), дигиталниот потпис и друго. Во зависност од тоа каква е комуникацијата, договорните страни можат да се определат за повисок или понизок степен на сигурност на електронските потписи. Така, на пример, во случај на организирање состаноци, потврда на резервации, деловна кореспонденција, страните кои разменуваат пораки можат да се потпишат со скенирање на своерачниот потпис или со впишување на своето име и презиме и во дадениот случај тоа за нив претставува доволна сигурност и начин за идентификување на другата страна. Меѓутоа, кога станува збор за трансакции чија вредност е голема, или кога е во прашање трансфер на доверливи информации, страните најчесто избираат некој од посигурните и пософистицираните начини за идентификација односно валидација и конфирмација на потписот на другата страна (дигитален потпис).

Дигиталниот потпис претставува електронски потпис кој функционира по принципите на криптографијата, како посебна гранка на математиката. Овој вид потпис настанува со користење на криптографија на "јавен клуч". Така, компјутерот на испраќачот преку посебна програма ја трансформира пораката во збиена криптирана форма која подоцна може да се енкриптира или прочита со користење на приватниот клуч на испраќачот. Вака составената порака е единствена и уникатна и ниедна друга порака создадена со методот на криптирање не може да биде идентична со неа. Кај потпишувањето на документите со дигитален клуч се користат два клуча, и тоа приватниот кој се наоѓа кај потписникот и јавниот кој е достапен на широк круг заинтересирани лица. Со оглед на фактот што приватниот клуч не е директно поврзан со личните карактеристики на неговиот сопственик, тој може неовластено да биде употребен од страна на трети лица (на пример, може да биде украден и употребен од страна на трето лице), поради што при користењето на дигиталниот потпис мора да се посвети големо внимание и да се преземат сите мерки за заштита на клучевите кои се користат, како и заштита на компјутерскиот систем преку кој се врши трансакцијата и потпишувањето. Електронскиот потпис се смета за адекватен и како чин на потврда, прифаќање или одобрување на текстот или документот на кој се однесува, под услов постапувањето на лицето кое се потпишува недвосмислено да укажува на неговата намера тоа навистина да го стори.

Електронско потпишување е, во принцип, математичка операција, каде со помош на одреден алгоритам од електронски напишаниот текстот се добива единствена уникатна низа од карактери. Било каква промена во текстот доведува до промена во низата. Понатаму, со помош на друг алгоритам, од оваа низа и од приватниот клуч на корисникот кој дигитално го потпишува текстот се добива електронскиот потпис кој е единствен. И тука било каква промена во текстот или примената на друг приватен клуч доведува до промена во генерираниот електронскиот потпис. Проверката на автентичноста и верификација на електронскиот потпис исто така се врши со помош на алгоритам и од добиениот текст се добива една низа од карактери која е единствена, за да подоцна со употреба на јавниот клуч на потписникот кој се верифицира со помош на сертификат, од електронскиот потпис повторно се добива низа од карактери која е уникатна. Вака добиените низи се споредуваат. Доколку низите се потполно идентични, тоа значи дека и текстот и потписот се автентични. Од ова може да се види дека технологијата на електронско потпишување под одредени услови е доволно безбедна за секојдневно користење.

Битна карактеристика на податокот во електронски облик и на електронскиот потпис е што тој не може да се одбие или да не се прифати како доказ само затоа што е во електронски облик. Ова е од особена важност за правната валидност и издржаност на електронскиот потпис и електронскиот договор заверен со таквиот потпис, затоа што, во крајна линија, го изедначува дематеријализираниот потпис и документ со оној класичниот, пишан и своерачно потпишан документ. Општо прифатлив електронски потпис со квалификуван сертификат даден во врска со електронски податоци е изедначен со своерачен потпис и затоа има еднаква важност и сила на доказ како и своерачниот потпис даден во врска со хартиени документи. Од ваквото правило постои и исклучок, односно електронскиот потпис не важи таму каде што се бара своерачен потпис пред нотар или суд.

Како што е погоре наведено, утврдувањето и проверката на идентитетот на лицето испраќач се постигнува со употреба на електронски сертификат кој претставува електронска "лична карта" на испраќачот, односно документ за негова идентификација во електронската комуникација. Тој може електронски да се презентира за да се докаже идентитетот или правото на пристап до определена информација или онлајн услуги.

Електронскиот сертификат го издава овластен издавач на сертификати како трета неутрална и доверлива страна.

За време на процесот на проверка на општо прифатениот електронскиот потпис задолжително треба да се обезбеди и следното: податоците кои се употребуваат за проверка на електронскиот потпис да се исти со податоците кои корисникот ги гледа, потписот да се провери на сигурен начин, а резултатот од оваа проверка и идентититетот на носителот на сертификатот правилно да се прикажат на корисникот, за да може тој на сигурен начин да ја провери содржината на потпишаните податоци. Средствата за општо прифатливо електронско потпишување меѓу другото треба да го обезбедат и следното: податоците за електронско потпишување да се единствени, сигурни и доверливи и да може во разумно време и со разумни средства од податоците за проверка на електронскиот потпис да се добијат податоците за електронско потпишување, електронскиот потпис да биде заштитен од фалсификување со употреба на моментално достапната технологија и потписникот да може сигурно да ги сочува податоците за електронско потпишување од неовластен пристап. Овие средства не смее да ги променат податоците кои се потпишуваат или да го спречат потписникот да ги види податоците кои ги потпишува.

3. ОБЕЗБЕДУВАЊЕ НА ТРАНСАКЦИИТЕ И ЕЛЕКТРОНСКИОТ ПОТПИС СО КРИПТОГРАФИЈА

Податоците кои се користат кај Е-трговијата можат да имаат различен карактер. Така, јавни податоци се оние до кои секој има пристап и увид. Авторизирани податоци се оние податоци на кои сите имаат право на увид, но нивното користење е ограничено со авторското право на нивниот сопственик. Доверливи се оние податоци за кои се знае дека постојат, но пристапот до нив е оневозможен. На крајот, тајни податоци се оние за кои не се знае дека постојат, ниту се знае нивната содржина. Во услови на Е-трговија особено внимание се посветува на заштитата на доверливите и тајните податоци. Заради ефикасна заштита од неовластени пристапи и користења на информациите и податоците, субјектите на Е-трговијата се служат со криптографијата како техника на процесирање на податоците .

Криптографијата буквално значи претварање на информациите во мноштво неповрзани податоци кои никој освен примачот не може да ги прочита. Таа има за цел да ги заштити како пренесените, односно оние информации кои треба да бидат трансферирани до друг корисник, така и архивираните податоци кои треба да бидат заштитени од неовластен пристап[53]. Податоците се кодираат (фаза на енкрипција) по што се пренесуваат во форма на криптографска порака (криптограм), за да по пристигнувањето бидат декодирани (фаза на декрипција) од страна на примачот со употреба на клуч за декодирање или дешифрирање. За да може да се изврши трансферот на податоците и информациите, претходно испраќачот и промачот на пораката мораат да си разменат клучеви за кодирање и декодирање.

Постојат два начини на кодирање, симетрично и асиметрично, кои имаат свои специфичности и определени предности во зависност од ситуациите во кои се користат. Така, симетричното шифрирање се врши со таен клуч, при што клучевите за кодирање и декодирање се идентични. Овој систем е брз и едноставен, но е и несигурен бидејќи бара транспортирање и чување на клучевите преку сигурни канали заради избегнување на несакани упади и злоупотреби. Од друга страна, асиметричното кодирање претставува посложен и побавен процес, но се одликува со многу поголем степен на безбедност на трансферот на податоците и информациите. Тука, пред се, е надминат проблемот на трансфер на тајниот клуч до примачот и со тоа во голема мерка е зајакната сигурноста на податоците. Кај асиметричното шифрирање постојат два клуча, од кои едниот служи за шифрирање а другиот за дешифрирање. Клучевите не се исти, но се поврзани со определени трансформации, така што познавањето на едниот клуч и неговиот алгоритам не овозможува добивање на другиот клуч. Едниот клуч се нарекува јавен клуч и може слободно да се дистрибуира, а другиот е таен клуч и мора да му биде достапен исклучиво на неговиот сопственик. Технологијата на електронскиот или дигиталниот потпис е заснована токму на решенијата кои ги овозможува асиметричната криптографија и користењето на два криптографски клучеви; со првиот, тајниот или приватниот клуч, се врши потпишувањето на податоците и документите, а со вториот, јавниот клуч, се врши верификување на потписот.

Онлајн трансакциите кај Е-трговијата бараат исклучителни напори за заштита на трансферот на податоци и информации. Во такви услови како решение кое пружа високо ниво на заштита на електронските податоци се смета инфраструктурата на јавните клучеви, како сложен систем кој опфаќа криптографски технологии, протоколи, стандарди, политики, процедури, сервиси и апликации и е заснован на концептот на асиметрична

[53] Novaković J., Elektronsko poslovanje, drugo izmenjeno i dopunjeno izdanje, Megatrend Univerzitet, Beograd, 2008, стр.222

криптографија. Оваа инфраструктура обезбедува четири основни функции на заштита : тајност, со која се гарантира дека содржината на податоците може да ја дознае единствено корисникот кому е наменета пораката; автентикација, со која се верификува идентитетот на корисниците кои комуницираат преку Интернет; интегритет, со кој се гарантира непроменливоста на пораката во фазата на преносот, и неотповикливост, со која се оневозможува отповикување на извршената трансакција. Со кодирањето на пораките, преку примена на соодветен криптографски систем, се реализира заштитата на тајноста на пораката, како прва од четирите функции на заштита, додека останатите три функции се реализираат со примена на технологијата на дигиталниот потпис.

Кај онлајн трансакциите потребно е да се обезбеди дека информациите за плаќањата не можат да бидат изменети во тек на преносот. При тоа, корисникот сака да биде сигурен дека неговите лични информации и информациите за неговата кредитна картичка се безбедни, а трговецот сака да биде сигурен дека плаќањето ќе биде извршено без никакви пречки. Таквата сигурност на трансакциите и заштита од евентуални ризици ја овозможува токму SSL протоколот преку кодирање на податоците, идентификација на серверот, интегритетот на пораките и опциона идентификација на клиентот преку TCP/IP.

4. Е-БАНКАРСТВО

Електронското банкарство претставува современ канал за користење на банкарските производи и услуги. Предности на Е-банкарството се: максимално поедноставување на банкарското работење, заштеда на време и пари, намалување на обемот на шалтерското работење, олеснување на пристапот на потрошувачите до услугите и производите на банката, намалени трошоци за надоместоците кај електронските трансакции, безбедно и сигурно вршење на трансакциите по електронски пат преку веб-страницата на банката со овозможен пристап од било кој компјутер преку едноставна најава со корисничко име и лозинка и друго.

Сигурноста на банкарските трансакции на Интернет е она што претставува сегмент на посебно интересирање кај научната и стручната јавност. За да можат банките да ги задоволат барањата на своите корисници на услуги, тие мораат да пружат квалитетни и адекватни услуги и да задоволат пет основни начела: еднаквост, понуда на услуги, погодности, квалитет и цена. Електронското банкарство може да даде задоволителни резултати само ако се исполнат неколку услови: ниска цена на интерактивниот пристап на коминтентите од дома; развој на системите кои можат да поддржат малопродажни активности на е-трговијата врзани за онлајн плаќања; понуда на најквалитетни информации на корисниците на Е-банкарските услуги; развој на производи и услуги кои ќе бидат привлечни за корисниците и кои ќе бидат подобри и поразлични од оние што ги нудат конкурентите; и идентификација на нови маркетиншки сегменти во кои постои подготвеност за вложувања во електронско банкарство[54]. На одлуката за имплементација на Е-банкарството големо влијание има и цената, односно скапиот софтвер, цената на развојот, тестирања и комерцијализацијата на банкарските производи, цената на маркетиншките активности, како и цената на користењето и одржувањето. Сепак, најважна активност на Е-банкарството е да се заинтересираат корисниците за користење на новиот систем. Корисниците бараат одговори на многу прашања и банките мораат да бидат респонзивни за да ги привлечат, но и да ги задржат коминтентите во услови на силна конкуренција и инвазија на нови производи и услуги понудени од конкурентните банки.

Во Р. Македонија Е-банкарството е во експанзија. Речиси сите деловни банки нудат производи и услуги за вршење зделки по електронски пат, но само 5 од нив поддржуваат интернет (електронска) трговија кај онлајн трговци со седиште во Р. Македонија. Банките издаваат т.н. токени-специјални уреди кои служат за еднократно генерирање на лозинки за корисниците кои сакаат, освен обичните плаќања на сметки за комуналии, да вршат и трансфер на средства од девизна на денарска сметка и обратно, или други трансакции за кои е потребно повисоко ниво на заштита и безбедност. Сепак, останува впечатокот дека е потребна агресивна маркетиншка кампања за подигнување на нивото на свеста кај потрошувачите за бенефитите кои ги нуди електронското банкарство и електронската трговија во целост, како и подигнување на квалитетот на услугите од страна на деловните банки кои го имплементираат Електронското банкарство.

ЛИТЕРАТУРА

Chissick, M. (1999). Electronic Commerce – Law and Practice. London,

Ellison, K.E. (2016). *A cultural history of early modern English cryptography manuals*. Abingdon, Oxon: Taylor & Francis.

Le Tourneau, P. (2003). *La Notion de Contrat Electronique,* Les deuxiemes journees internationals du droit du commerce electronique, Litex, Paris

[54] Novaković, op. cit., стр.127

Novaković, J. (2008). Elektronsko poslovanje, drugo izmenjeno i dopunjeno izdanje, Megatrend Univerzitet, Beograd

Vilus, J. (2000). „Elektronsko trgovačko pravo“, Evropski centar za mir i razvoj (ECPD) Univerziteta za mir UN

Vulic, M. (2015). Elektronska trgovina, Visoka skola strukovih studija za informacione tehnologije, Beograd

Shadi, A. A. (2016). Online Banking Security Measures and Data Protection, Jordan University of Science and Technology, Jordan.

Živković, V. (2007). *Elektronska trgovina-Pravo Informacionih tehnologija*, Pravni fakutelt Univerzitet UNION, Službeni glasnik, Beograd