XV МАЈСКО САВЕТОВАЊЕ

# СЛОБОДА ПРУЖАЊА УСЛУГА И ПРАВНА СИГУРНОСТ

УРЕДНИК:
Миодраг Мићовић

УНИВЕРЗИТЕТ У КРАГУЈЕВЦУ
ПРАВНИ ФАКУЛТЕТ

Крагујевац
2019.

**ПРАВНИ ФАКУЛТЕТ УНИВЕРЗИТЕТА У КРАГУЈЕВЦУ**
**Институт за правне и друштвене науке**

# СЛОБОДА ПРУЖАЊА УСЛУГА И ПРАВНА СИГУРНОСТ

**Уредник**
**МИОДРАГ МИЋОВИЋ**

**Крагујевац**
**2019.**

# СЛОБОДА ПРУЖАЊА УСЛУГА И ПРАВНА СИГУРНОСТ

Зборник реферата по позиву са Међународног научног скупа одржаног 17. маја 2019. године, на Правном факултету у Крагујевцу у организацији Института за правне и друштвене науке Правног факултета Универзитета у Крагујевцу.



ИЗДАВАЧ: Правни факултет Универзитета у Крагујевцу
Институт за правне и друштвене науке
Јована Цвијића 1, 34000 Крагујевац
телефон: (034) 306 513, 306 504
телефакс: (034) 306 540
е-пошта: faculty@jura.kg.ac.rs
веб: http://.jura.kg.ac.rs

РЕЦЕНЗЕНТИ Проф. др Хрвоје Качер
Проф. др Снежана Миладиновић
Проф. др Миодраг Мићовић

ЗА ИЗДАВАЧА: Проф. др Драган Вујисић

УРЕДНИК: Проф. др Миодраг Мићовић

ШТАМПА: Графопромет д.о.о.

ТИРАЖ: 120

ISBN 978-86-7623-088-4

Штампање Зборника подржало Министарство просвете, науке и технолошког развоја Републике Србије

# САДРЖАЈ

## *Начелна разматрања о услугама*



## *Пословне и прометне услуге*



## *Финансијске и банкарске услуге*

## *Одговорност пружалаца и заштита корисника услуга*



## *Услуге и друга са њима повезана питања*

*Др Игор Камбовски, ванредни професор*
*Правног факултета, Универзитета „Гоце Делчев" у Штипу*

*УДК: 336.71:004*
*339:004*

# СИГУРНОСТ ЧУВАЊА И ПРЕНОСА ПОДАТАКА И ИНФОРМАЦИЈА КОД ЕЛЕКТРОНСКЕ ТРГОВИНЕ И ЕЛЕКТРОНСКОГ (ИНТЕРНЕТ) БАНКАРСТВА

## *Резиме*

*Заштита трансакција и обезбеђивање сигурности чувања и преноса информација код електронске трговине и електронског банкарства је изузетно сложен и скуп процес. Они се заснивају на успостављању заштићених система и протокола који ће моћи да идентификују могуће претње и анализирају могуће ризике и губитке који могу настати. Систем захтева инсталацију одређених механизама заштите као што су контрола приступа, аутентификација корисника, шифровање информација и увођење безбедносних протокола. Сваки систем у којем се подаци чувају и обрађују припада групи угрожених система и захтева заштиту. Генерално, свака особа, објект или догађај који потенцијално могу довести до угрожавања сигурности података у систему може се сматрати претњом. Такве претње могу бити случајне (нежељено брисање датотеке са подацима) или намерне (злонамерна модификација осетљивих података или хардвера система). Зато, те претње морају бити идентификоване и спречене, а ако су се већ догодиле, треба провести процедуре за њихово отклањање и минимизирање штете.*

***Кључне речи:*** *заштита, информације, е-трговина, е-банкарство.*

У свеприсутном дигиталном окружењу, у ери глобализације, све више информација и података преноси се и процесира путем интернета, у дигиталном облику, или преко других електронских средстава комуникације. Овај тренд је нарочито изражен код Електронске трговине и електронског пословања. Сједињене Америчке Државе још увек држе примат у обиму електронске трговине. Са већином потрошача који поседују паметне телефоне и мобилне уређаје (91 проценат у САД), а прате их лаптоп компјутери (83 процента), дигитално тржиште је постало реалност. Наравно, технологија подржава велики обим онлајн интеракција између трговаца и потрошача. Али права вредност дигиталне трговине је поверење. Онлајн активности међу

потрошачима одражавају распрострањено прихваћање електронске трговине као начина за куповину добара и услуга (90 посто) и вођење личног интернет банкарства (88 посто). Како компаније пролазе кроз дигиталне трансформације у својим предњим и позадинским пословима, оне препознају важност поверења и потребу за технологијом да то омогући. Када је у питању онлајн ангажман, највећи број компанија и банака је заинтересовано за напредније сигурносне мере и аутентификацијске процесе који имају мали или никакав утицај на клијента[1]. Наравно, сваки нови, успешан подухват, свака иновација на пољу Електронске трговине и интернет банкарства носи са собом и велики ризик од злоупотреба и превара, који могу проузроковати финансијске губитке, како за трговце и банке, тако и за потрошаче. У тим нелегалним процесима може доћи до неовлашћених употреба ресурса, губљења пословног угледа, губљења поверљивих и вредних информација и података, повећања правног ризика, као и повећања трошкова пословања изазваних неизвесним и несигурним условима пословања.

Банке, као пословни субјекти који пружају електронске услуге и платформу за плаћање путем интернета су такође изложени великим претњама. Интернет банкарство је све развијеније и све популарније, али корисници услуга интернет банкарства су под сталном претњом од злоупотребе њихових рачуна, финансијских података, упада у базе личних података, „фишинг“ напада и других облика криминалних активности[2]. Е-банкарство или интернет банкарство је модерна и савремена платформа за коришћење банкарских производа и услуга преко које потрошачи који имају рачун у одређеној банци имају могућност плаћања свакодневних обавеза и обављање разних трансакција: плаћање режијских трошкова и комуналија, плаћање доспелих обавеза везаних за картично пословање, плаћање кредитних обавеза, плаћање пореза, онлајн куповина, онлајн провера стања банковних рачуна и др.

Сигурност банкарских трансакција на Интернету је од посебног значаја и интереса у научној и стручној јавности. У оквиру савремених истраживања, посебна пажња се посвећује овим проблемима како би се пронашла прихватљива решења која ће омогућити безбедно вођење и спровођење онлајн процеса у домену финансија и банкарства, како би се банкама омогућило да задовоље захтеве својих корисника услуга, пружити квалитетне и адекватне услуге и задовољити неколико функционалних принципа: понуду услуга, погодности, квалитет и цену. Е-банкарство може дати задовољавајуће резултате само ако су испуњени следећи услови: ниски трошкови интерактивног приступа за потрошаче; развој система који могу да подрже активности у области малопродаје и плаћања у електронској трговини; пружање најквалитетнијих информација корисницима услуга електронског банкарства; развој производа и услуга који ће бити атрактивни за купце и који

[1] https://www.experian.com/assets/decision-analytics/reports/global-fraud-report-2018.pdf
[2] https://financialregnews.com/banking-industry-suffered-2-2-billion-fraud-losses-2016/

ће бити бољи и разноврснији од оних које нуде конкуренти; и идентификовање нових маркетиншких сегмената у којима постоји спремност за улагање у електронско банкарство.

У исто време, компаније схватају да су њихови клијенти задовољни са безбедносним мерама које већ имају у погледу чувања и обраде података и информација и дигиталних трансакција. Изградња поверења кроз технологију без ометања је све више циљ, али и одговорност компанија и трговаца који користе онлајн платформе за пословање и продају. Ентузијазам потрошача на дигиталном тржишту темељи се на поверењу. Потрошачи верују да компаније и банке постављају заштиту њихових личних информација на највиши пиједестал својих приоритета. Потрошачи очекују да ће их компаније штитити и осећају се сигурни. Они наводе да су визуелни знакови сигурности и препреке на које наилазе приликом приступа својим компјутерима и паметним телефонима - индикатори да је трансакција сигурнија. Најчешће, недостатак видљиве безбедности приликом приступа одређеној веб страници је главни разлог зашто купци напуштају трансакцију.

Насупрот томе, велики број компанија који послују на интернету наводе крађу података и превару као растућу забринутост, а није мали број оних који пријављују исти или већи ниво губитака. Код потрошача, скоро 80% верују да је заштита личних података главни приоритет у електронском банкарству и електронској трговини. Такође, већина потрошача верује у сигурносне протоколе приликом обављања онлајн трансакција јер им ствара позитиван утисак и улива поверење да се осећају заштићеним. Решења која комбинују информације о уређају са другим тачкама података као што су биометрија могу помоћи трговцима, банкама и компанијама у будућности да боље препознају своје клијенте. Трговци су свесни да постоје све веће претње од преваре на тржишту и степена до којег та криминална активност има утицај на њихово пословање. Зашто су преваре и крађе података постале тако свеприсутне и зашто се банке и компаније боре да иду у корак са новим изазовом? Иронија је у томе што је оружје против онлајн превара такође извор његове рањивости. Постојећи процес подешавања налога захтева од потрошача да пруже обимне личне информације и одговоре на тајна питања и лозинке, и фактички омогућује злонамерницима да дођу до тих рањивих и изузетно значајних података.

Када се једном украду, ове информације се могу користити како би се олакшала нелегална активност, дајући личним подацима истинску вредност на нелегалним тржиштима. Како се потенцијални неповољни резултат дигиталних превара повећава, тако расте и мотивација сајбер криминалаца да остану испред најновијих стратегија и технологија откривања. Сајбер криминалци увек унапређују софистицираност својих метода. Напади се сада крећу између канала као што су интернет, компјутер, мобилни телефон итд. - и нове шеме,

као што су синтетичке преваре[3] (где криминалци спајају стварне и лажне информације како би створили потпуно нови идентитет). Компаније нису веома сигурне у њихову способност да заштите себе и своје клијенте од преваре и признају да су све постојеће мере резултат реактивних, а не проактивних иницијатива. Технолошки изазови (интеграција нових и комбинација старих решења) такође представљају препреке. Компаније, банке и остали пословни субјекти на дигиталној платформи стреме се ка увођењу иновативних начина у настојању да клијенти отворе рачуне и обављају онлајн трансакције, али се они и даље суочавају са изазовима које треба превазићи. Традиционална решења су се ослањала на обрасце понашања који су помагали компанијама да открију злоупотребе и преваре. Нова решења подразумевају нове обрасце понашања на мрежи, а старе референтне вредности које се користе за откривање абнормалних активности које би могле да сигнализирају преваре и крађу података више нису поуздане. Сходно томе, како компаније промовишу своје дигитално искуство, оне се осећају све рањивије и нису веома сигурне у њихову способност да уоче преваре. Из тих разлога, многе фирме приоритетно дају предност безбедности трансакција и заштити података и прихватају одређене нивое финансијских губитака на основу трошкова које ове активности генеришу.

Главни циљеви предузимања мера безбедности за системе у трансакцијама у оквиру електронске трговине су[4]:

- поверљивост - обезбеђује недоступност информација неовлашћеним лицима;

- интегритет - осигурава конзистентност података, спречава неовлашћено генерисање, промену или уништавање података, односно даје потврду да су подаци остали непромењени;

- доступност - овлашћени корисници могу користити услуге и базе података у било ком тренутку;

- искључиво коришћење система од стране овлашћених корисника-ресурси се не могу користити од стране неовлашћених лица. Овдје се посебан нагласак ставља на спречавање лажног представљања успостављањем контролних механизама - идентификације извора и провере идентитета.

Заштита система, података и трансакција се обично врши кроз софистицирани систем механизама и процедура за заштиту. То укључује: идентификацију и аутентичност Е-записа (аутентификација), верификацију аутентичности потписаног Е-записа у случају спора, електронски запис и енкрипцију, идентификацију потписника, итд. Аутентификација је један од начина за онемогућавање лажног представљања. У условима Е-трговине, купац, продавац, посредник и институције преко којих се врши исплата (банке)

[3] https://www.idanalytics.com/solutions-services/fraud-risk-management/synthetic-identity-fraud/

[4] Новаковић, Ј., *Електронско пословање*, Београд, 2005, стр. 245,

треба да буду убеђени у идентитет странке са којом се трансакција обавља. Идентитет корисника одређује се преко неколико параметара: код, лозинка (нешто што само корисник зна); картица (нешто што само корисник има); потпис, глас, папиларни отисак, слика ока, геометрија длана и друге карактеристике (нешто што је корисник) које се утврђују биометријским контролама и инструментима. Ако се за аутентификацију користи само код, као најпоузданији сигурносни механизам који се може детектовати или пресрести током преноса преко система, у том случају систем безбедности може бити компромитован и то представља озбиљну претњу за цео систем. Зато, ове сигурносне технике и механизме треба користити у комбинацији, сводећи ризик неовлаштеног приступа и злоупотребе података и трансакција на рационалном минимуму.

Постоји неизвесност о томе колико треба инвестирати у напредна решења за откривање и аутентификацију преваре из забринутости за ометање корисничког искуства. Компаније и банке се често боре са тензијом између борбе са преварама и одржавања позитивног искуства са клијентима. Било да се ради о отварању новог налога, пријављивању на постојећи рачун или склапању трансакције, већина банака и компанија се и даље ослања на лозинке и једнократне кодове као примарни облик провере аутентичности, пре свега, зато што су добро схваћене и корисници су се навикли на њих. Међутим, велики број клијената и потрошача заборавља корисничко име или лозинку, или заборави да промени своју лозинку у препоручено време. То ствара непријатност и конфузију код корисника, из разлога што заборављају корисничко име или лозинку, или је приступ онемогућен због погрешног навођења лозинке превише пута, или морају да одговоре на тајна или лична питања пре него што приступе свом налогу или рачуну.

Многи потрошачи који желе купити одређену робу преко интернета не желе да њихов идентитет буде откривен. Они не желе да други знају шта су купили и воле да остану анонимни, као када плаћају готовином у традиционалној трговини. Како би се осигурала приватност и поверљивост одређених података, користи се одговарајући програм за њихову заштиту, која се спроводи кроз већ споменуто шифрирање података и њихово кодирање и декодирање, како у преносу тако и у архивирању и чувању података. Шифровањем, подаци се претварају у облик који је несхватљив и неразумљив ономе који не зна или који нема кључ за њихово декодирање и повратак у почетни облик. То, наравно, спречава приступ, употребу информација и њихову злоупотребу од стране неовлашћеног лица. Такође, у процесу преноса података и њиховог кодирања и декодирања може доћи до нежељеног нарушавања редоследа података и њихове измене, чиме се губи почетни облик и садржај. У циљу спречавања таквих нежељених догађаја и губитка података, неопходно је обезбедити компјутерски софтверски систем за интегритет података који ће обезбедити заштиту информација, сервера и других компоненти компјутерског система и мреже од неовлашћених модификација

информација. Овај систем провере може открити могуће промене у редоследу делова порука и информација, њихово брисање, додавање информација, итд. Овај програм не може у потпуности заштитити систем од неовлаштених измена, али је могуће открити такве измене, осим ако се информације не бришу и не изгубе.

Превара, крађа идентитета и личних података је све присутнији и све већи ризик. За дигитално оријентисане компаније, управљање мерама безбедности и сигурности је деликатно балансирање између откривања превара и дигиталног искуства корисника. Да би одржали корак, банке и компаније морају направити значајна улагања у хардвер и софтвер за препознавање клијената. Неким је компанијама тешко проактивно имплементирати напредне методе провере аутентичности које ће точно идентификирати своје клијенте, да не би тиме ушли у „комфорну зону“ корисника њихових услуга[5]. Банке су у том погледу више напредовале. Купци су навикли на тренутни ниво заштите и, иако би били задовољни са више удобности, као што је употреба отиска прста уместо лозинке, они нису увек спремни на промену. Напредне методе аутентикације, као што су употреба интелигентних уређаја за препознавање или биометрија, могу помоћи у обостраном приступу, без повећања нивоа непријатности. Када је у питању управљање ризиком од превара, не постоји глобално решење за све, али постоје опције које су већ проверене и које се све више прихватају у дигиталном окружењу. У том погледу, препознавање клијената путем напредних, вишеслојних решења прилагођених корисничком искуству је будућност превенције од превара, злоупотребе или крађе идентитета и личних података.

На одлуку о имплементацији електронског банкарства утиче и цена. Тако, за банке, почетни трошкови имплементације нових технологија и покретања е-банкарства могу бити веома високи. На цену утичу: скуп софтвер, цена финансијских производа са свим пратећим елементима - развој, тестирање и комерцијализација тих производа, цена маркетиншких активности, као и трошкови коришћења и одржавања. Међутим, најважнија активност електронског банкарства је да заинтересује кориснике за коришћење новог система. У почетку ће се од корисника тражити да одговоре на многа питања, а банке морају имати одговор за привлачење свих заинтересованих корисника, али и да одржавају у условима јаке конкуренције и инвазије нових производа и услуга које нуде конкурентске банке.

У свету електронско банкарство је широко прихваћено међу свим слојевима популације, нарочито у развијеним земљама. У Македонији Е-банкарство је у експанзији, већ десетак година. Готово све банке нуде производе и услуге за обављање послова електронским путем. АТМ Банкомати су распрострањени у целој земљи и омогућују аутоматизовану уплату, проверу

[5] Камбовски, И., *Електронска трговина и електронски уговор*, (Докторска дисертација), Правни факултет „Јустинијан Први“, УКИМ, Скопје, 2009, стр. 205.

рачуна и повлачење готовине у било које доба дана једноставним коришћењем кредитних и дебитних картица које издаје одговарајућа банка. Такође, све банке имају отворене ПОС терминале у трговини, што омогућава потрошачима да обављају безготовинске уплате, обично праћене додатним погодностима као што су безконтактно плаћање, плаћање на рате, попусти или учешће у наградним играма. Са своје стране, македонски корисници ових услуга обично одлучују да закључе онлајн уговоре са банкама за плаћање режијских трошкова (комуналије - рачуни за електричну енергију, телефон, грејање, итд.) Банке издају такозване токене-специјалне уређаје који користе и генеришу једнократне лозинке за кориснике који желе, поред редовних уплата на рачуне за комуналне услуге, да пренесу новац из девизног на денарски рачун и обрнуто, или друге трансакције које захтевају виши ниво заштите и безбедности. Међутим, остаје општи утисак да је потребна агресивнија маркетиншка кампања како би се подигао ниво свести потрошача о предностима које нуди електронско (интернет) банкарство, као и подизање квалитета услуга и смањење цена од стране банака које имплементирају систем Е-банкарства.

*Igor Kambovski, Ph.D., Associate Professor*
*Faculty of Law , University "Goce Delčev" in Štip*

## SECURE STORAGE AND SECURE DATA AND INFORMATION TRANSFER AT ELECTRONIC COMMERCE AND ELECTRONIC (INTERNET) BANKING

### *Summary*

*Securing transaction and providing secure storage and transmission of information at electronic commerce and electronic banking is a very complex and expensive process. They are based on the establishment of a protected system and a protocol that will be able to identify possible fraud and analyze the risk and loss that can occur. The protection system demands installation of a predefined security mechanism such as access controll, user authentication, encryption of information and establishing of security protocol. Each system which is collecting and storing data and information belongs to the group of threatened system and needs protection. Generally, each person, object or event, which can potentially leads to security breach, can be considered as threat. Such threat may be accidental (unwanted file deletion) or intentionall (malicious modification of sensitive data or hardware*

*system). However, those threats must be identified and prevented, and if they have already succeeded, an appropriatte procedure should be taken for the disposal and minimization of damages.*

***Key words:*** *protection, information, e-commerce, e-banking.*

## Литература

Камбовски, И., *Електронска трговина и електронски уговор*, (докторска дисертација), Правни факултет „Јустинијан Први“, УКИМ, Скопје, 2009.
Новаковић, Ј., *Електронско пословање*, Београд, 2005.

https://www.experian.com/assets/decision-analytics/reports/global-fraud-report-2018.pdf
https://financialregnews.com/banking-industry-suffered-2-2-billion-fraud-losses-2016/
https://www.idanalytics.com/solutions-services/fraud-risk-management/synthetic-identity-fraud/