

Факултет инжењерских наука Универзитета у Крагујевцу

Владимир Гулан

**Електронски системи плаћања и њихова
заштита**

Мастер рад

Крагујевац, 2014.

Факултет инжењерских наука Универзитета у Крагујевцу



Назив студијског програма: Машинско инжењерство

Ниво студија: Мастер академске студије

Модул: Инжењерски менаџмент

Предмет: Инжењерска економија

Број индекса: 617/2013

Владимир Гулан

ЕЛЕКТРОНСКИ СИСТЕМИ ПЛАЋАЊА И ЊИХОВА ЗАШТИТА

Мастер рад

Комисија за преглед и одбрану:

1. Др Рајко Чукић – ментор
2. _____
3. _____

Датум одбране: _____

Оцена: _____

У овом мастер раду студент треба да укаже на значај електронских система плаћања, да све начине детаљно обради, али и да посвети пажњу заштити електронских система. С обзиром на чињеницу да свет карактерише све већа глобализација и све бржи начин живота потребно је да се са научног аспекта обради тема како електронских система плаћања, тако и њихове заштите. Користећи домаћу и страну литературу студент треба да дође до закључка на који начин се системи електронског плаћања могу унапредити, и које су тренутно његове слабе тачке. Задатак кандидата је да на што систематичнији начин обради ову тему и да на крају да свој суд о изложеном.

Препоручена литература:

1. Вуксановић Е., *Електронски системи плаћања*, Универзитет у Крагујевцу, Економски факултет, 2009.
2. Вуксановић Е., *Механизми и инструменти плаћања у условима електронског преноса средстава*, SAM Konsalting, Београд, 1994.
3. Тан М., *E – payment, The Digital Exchange*, Rigde Books, 2006.

Крагујевац, 2014.

Ментор:

Име, презиме и звање ментора

Др Рајко Чукић, доцент

Резиме: Развој рачунара и телекомуникација створио је услове за глобализацију пословања, односно допринео је потпуној интеграцији локалног тржишта у национално, а преко њега и у интернационално тржиште. Главни циљ је постао да се без обзира на географске дистанце што брже и ефикасније повежу учесници у пословању, пре свега кроз поспешивање токова информација коришћењем електронске технологије. Наведени циљ се постиже управо коришћењем електронских система плаћања. Онда када учесници у платном промету више не морају да воде рачуна о томе у којој држави се налазе они, или њихови партнери, то олакшава повезивање с једне, и закључивање и извршавање тако закључених послова са друге стране.

Кључне речи: *електронско, плаћање, интернет, системи заштите*

Abstract: The development of computers and telecommunications has created the conditions for the globalization of business, that contributed to the full integration of local markets into national and, through him, and in the international market. The main goal is to become, regardless of geographic distance as quickly and efficiently connect participants in operations, primarily through the facilitation of information flows using electronic technology. Then when participants in the payment system does not have to care about what country are they, or their partners, to facilitate connecting with one hand, and the conclusion and execution of such transactions concluded on the other side.

Key words: *e – banking, electronics payment, protection systems*

САДРЖАЈ

УВОД.....	2
1. ОПШТИ АСПЕКТИ СИСТЕМА ПЛАЋАЊА	3
1.1. Основни елементи	3
2. ЕЛЕКТРОНСКИ СИСТЕМИ ПЛАЋАЊА.....	4
2.1. Инструменти и канали иницирања у циклусу е – плаћања	5
3. ТЕХНОЛОГИЈА Е – ПЛАЋАЊА	7
3.1. Електронске (платне) картице	7
3.2. Даљинско банкарство	9
3.3. Банкомати	11
3.4. ПОС терминали	12
3.5. Телефонско банкарство	14
3.6. РС банкарство.....	15
3.7. СМС банкарство	18
3.8. Интернет банкарство	19
3.9. Мобилно банкарство	21
4. СОФТВЕРСКА РЕШЕЊА ЗА Е – БАНКАРСТВО.....	24
5. УПРАВЉАЊЕ РИЗИЦИМА У ЕЛЕКТРОНСКОМ БАНКАРСТВУ.....	26
6. ПРОБЛЕМИ СИГУРНОСТИ И МЕРЕ ЗАШТИТЕ	41
7. ЕЛЕКТРОНСКО БАНКАРСТВО У СРБИЈИ	49
ЗАКЉУЧАК	58
ЛИТЕРАТУРА.....	60

УВОД

Развој рачунара и телекомуникација створио је услове за глобализацију пословања, односно допринео је потпуној интеграцији локалног тржишта у национално, а преко њега и у интернационално тржиште. Главни циљ је постао да се без обзира на географске дистанце што брже и ефикасније повежу учесници у пословању, пре свега кроз поспешивање токова информација коришћењем електронске технологије.

Појаву електронског пословања (енг. Electronic business или е – business) различити извори везују за различите временске периоде: неки сматрају да се електронско пословање појавило 70-тих година 20. века, док су други мишљења да оно има много дужу историју. У тражењу одговора на ово питање би можда ипак било најбоље кренути од саме дефиниције електронског пословања. Електронско пословање представља размену стандардизованих електронских порука у обављању разних послова у компанијама, банкама, управи, активностима грађана и у свим другим пословним трансакцијама. Електронско пословање подразумева обављање пословних процеса уз примену информационе и (теле)комуникационе технологије, које се збирно означавају као електронске технологије.

Чињеница да је први електронски трансфер новца извршен уз помоћ телеграфа давне 1860. године (Western Union) у први мах даје за право онима који заступају становиште много дуже историје електронског пословања. Међутим, савремено поимање електронског пословања подразумева примену не само комуникационих већ и информационих технологија, односно коришћење дигиталних уместо аналогних (телеграф) технологија, што за право даје онима који историју електронског пословања свode на претходних 40-ак година.

Оно што ни једног тренутка није спорно јесте чињеница да је електронско пословање убрзан развој доживело у последњих 15-ак година, пре свега захваљујући појави интернета.

1. ОПШТИ АСПЕКТИ СИСТЕМА ПЛАЋАЊА

Платни систем представља централни део инфраструктуре финансијског сектора у тржишној економији. Као такав има посебан значај за вођење монетарне политике и обезбеђивање финансијске стабилности. Посредством опште глобализације значај платног промета се увећава, а посебно имајући у виду све већу вредност финансијских трансакција.

Према дефиницији, плаћање је размена монетарне вредности за пријем добара или услуга. Са развојем облика новца мењају се и механизми плаћања и сама технологија обављања робне размене. Концепт новца као мере вредности постаје све више апстрактан током његовог историјског развоја. Са појавом интернета долази до стварања новог канала за инструкције плаћања са карактеристикама „е“.

1.1. Основни елементи

За реализовање циклуса плаћања могуће је издвојити следеће елементе:

1. Средства иницирања
2. Средства преноса и размене инструкција плаћања
3. Обрачун и извршавање плаћања и пренос власничких права између субјеката

Основни задатак у сектору **иницирања** је избор инструмената помоћу којег ће се трансакција извршити. Појам **инструмената** плаћања обухвата сва средства на којима се налази монетарна вредност препознатљива у трансакцијама плаћања. Ти инструменти данас егзистирају у различитим формама. У папирним системима плаћања то су готов новац и папирни инструменти за безготовинска плаћања, док се у беспапирним појављују и разне варијанте платних картица и електронске инструкције које се могу давати кроз различите канале.¹

¹ Вуксановић Е., *Електронски системи плаћања*, Универзитет у Крагујевцу, Економски факултет, 2009. стр. 37.

Као и у свим трансакцијама и овде постоје ризици, а све ризике можемо поделити на **кредитне и ликвидне**. **Ликвидни ризици** односе се на временски елемент и дефинишу се вероватноћом да новац неће бити на располагању примаоцу у очекиваном тренутку. **Кредитни ризик** се појављује као ризик губитка потраживања од других учесника у трансакцији и за разлику од ликвидног они увек значе губитак јер се ради о ризику да партнер неће извршити своју обавезу у пуној вредности, било у тренутку рока доспећа или касније.

2. ЕЛЕКТРОНСКИ СИСТЕМИ ПЛАЋАЊА

Трансакција е – плаћање би могла бити дефинисана као трансакција у којој се монетарна вредност преноси електронски између два ентитета, као компензација или накнада за пријем робе или услуга. Под бесплапирним инструментима подразумевају се електронске платне картице, жиро инструменти и такозвани виртуални новац.

Према подручјима примене трансакције е – плаћања могу се груписати у три сегмента:

1. Е – плаћања малих вредности
2. Е – плаћања предузећа
3. Е – плаћања велике вредности

Трансакције плаћања малих вредности обухватају три врсте трансакција: купац предузећу (C2B), предузеће купцу (B2C), и између индивидуалних учесника (P2P). Трансакције типа C2B су најубичајенија форма плаћања било да се ради о плаћању купљених роба или услуга, или пореза држави од стране индивидуалних пореских обвезника. Трансакције типа B2C обухватају исплату надница и плата послодаваца запосленима. У овој категорији трансакција најпопуларнија су плаћања државе појединцима (дистрибуирање пензија електронским средствима). И на крају, плаћање између појединаца најчешће произилази из online аукција или трансфера средстава између самих појединаца.

Корпоративна е – плаћања су трансакције плаћања за робе и услуге између пословних ентитета. Врсте корпоративних плаћања су следеће: плаћања предузећа предузећу (B2B),

предузећа банкама или банке предузећима као и плаћања на релацији предузеће држава (B2G). У новије време долази до пораста електронског плаћања између државних агенција (G2G).²

Трансакције плаћања велике вредности дефинишу се као плаћања између банака или банака и централне банке.

Према неким истраживањима процене су да ће сектор пословања са становништвом бити сектор са највећом заступљеношћу трансакција е – плаћања. С обзиром да је просечна вредност трансакције плаћање становништва знатно нижа у односу на трансакције које обаљају корпорације занимљива је чињеница да се ове две вредности постепено изједначавају. Према подацима из 2003. године од укупних трансакција е – плаћања 85% се односи на сектор становништва³.

Трансакције е – плаћања малих вредности реализују се у сектору становништва и у вези са тим постоје различити ставови у погледу утврђивања граничне тачке раздвајања поменутих категорија. Међу ауторима је присутан висок степен сагласности о потреби издвајања посебне категорије трансакције веома малих плаћања познате као микроплаћања, а односе се на трансакције испод 10 долара.

2.1. Инструменти и канали иницирања у циклусу е – плаћања

Циклусе е – плаћања обухвата одређени број етапа и активности. Све етапе се могу класификовати у три основне фазе:

1. **Иницирање**
2. **Процесинг**
3. **Потврђивање**

У првој фази циклуса плаћања врши се **иницирање** трансакције плаћања и односи се на трансмисију којом плаћац (потрошач или предузеће) даје инструкцију посреднику, обично

² Вуксановић Е., *навед. дело, стр. 40.*

³ Tan M., *E – payment, The Digital Exchange, Rigde Books, 2006. стр. 5.*

Електронски системи плаћања и њихова заштита

банци да изврши плаћање. Ова фаза углавном почиње активностима као што су давање инструкција односно налога за иницирање плаћања од стране ентитета који плаћа и прихватање датих инструкција за реализацију плаћања од стране посредника. Кључну улогу у овој фази има активност аутентификације учесника и ауторизације трансакције плаћања.

Друга фаза циклуса плаћања је **процесинг примљене инструкције** за реализацију трансакције плаћања. Ова фаза укључује валидацију и аутентификацију платиоца пре давања одобрења за задуживање рачуна платиоца и инструкција за клиринг и салдирање рачуна.

Финална фаза циклуса плаћања је **обавештавање о реализацији трансакција** плаћања и односи се на конкретан обавештавање корисника о пријему средстава.

3. ТЕХНОЛОГИЈА Е – ПЛАЋАЊА

Главне промене које су остварене у електронском пословању су обављање рутинских трансакција, као и увођење електронског трансфера новца, односно електронског плаћања. Коришћење Интернета као комуникационог канала у области плаћања условило је појаву интернет плаћања и одговарајућих инструмената којима се ова плаћања обављају.

3.1. Електронске (платне) картице

Почетком осамдесетих година прошлога века картице су постале уобичајено средство плаћања роба и услуга и достигле су размере масовне примене. У банкама и организацијама које су се бавиле картичним пословањем, за потребе картичног пословања, развијена је технолошка и рачунарска инфраструктура која је опслуживала овако масовно средство плаћања. Банкомати су функционисали на бази картица, а уводиле су их само поједине банке са циљем да смање трошкове шалтерског пословања, да ставе на располагање корисницима могућност да 24 часа дневно могу да подижу новац и да помоћу њих продуже време одлежавања новца на рачунима корисника. У оптицају се налазио велики број различитих картица. Свака банка је издавала или покушавала да издаје своју картицу, али се неколико светски познатих система издвојило и почело нагло да се шири и намеће као стандард. То је створило потребу за дефинисањем светског стандарда, како би се омогућило да се картице једне банке користе на банкоматима других банака. У том периоду појавио се Интернет.

У почетку, сама размена података преко Интернета била је довољна за академску мрежу и није било потребе да се било шта плаћа. Ширењем Интернета и масовним коришћењем његових могућности јавила се потреба да се извесне услуге плаћају путем Интернета. У том тренутку дошло је до спајања две различите технологије које су се допуњавале, а то су Интернет и платне картице. Интернет је пружио корисницима обиље могућности за пословање, а картица је својом технологијом омогућила да се то пословање финансијски затвори и изврши плаћање. Електронска технологија омогућила је употребу електронских

картица које се користе као инструмент безготовинског плаћања. Као издаваоци ових картица појављују се банке, где једну врсту картице може издавати више банака и у ту сврху формирају удружења (на пример DinaCard, Visa, MasterCard), небанкарске организације (Diners Club, American Express) и велике компаније, при чему издате картице важе само у интерним мрежама (најчешће је случај да трговац изда своју картицу, на пример M&S Card, Wall Maer Card, Пика картица, C-market). Електронске картице као инструменте плаћања можемо поделити према:

- 1. Технологији која је примењена: картице са магнетном траком и интелигентне картице (smart cards) са силицијумским микропроцесорским чипом,**
- 2. Према времену плаћања и анонимности трансакција: дебитне картице, кредитне картице и картице са унапред уплаћеним износима новца,**
- 3. Локацији примене: националне (важе у земљи где су издате) и интернационалне (важе равноправно, како у земљи тако и у иностранству),**
- 4. Кориснику картице: основну, додатну, пословну, и сл. ⁴**

У условима електронског банкарства ове картице омогућавају безготовински платни промет у реалном времену, путем дебитних картица и кредитирање власника картице, путем кредитне картице. Процес плаћања кредитном или дебитном картицом углавном захтева четири стране у свакој трансакцији:

- 1. Власника картице,**
- 2. Трговца који продаје производ или услугу,**
- 3. Компанију која врши обраду плаћања кредитном или дебитном картицом (тзв. процесора) и**
- 4. Емитента кредитне или дебитне картице.**

У извесним случајевима компанија која врши обраду плаћања кредитном или дебитном картицом и емитент кредитне или дебитне картице могу бити исти. Платне картице представљају замену (много комфорнију) за готовински новац, које уз обезбеђивање предуслова од стране пословних банака, и придржавања прописаних услова коришћења

⁴ Вуксановић Е., *Механизми и инструменти плаћања у условима електронског преноса средстава*, SAM Konsalting, Београд, 1994. стр. 95.

картица од стране клијента, могу и представљају изузетно сигурно средство свакодневног располагања средствима на пословним рачунима банака.

У домицилним условима пословања, картице су по укидању чекова као инструмента кредитирања (што никада чек и није смео да буде), доживеле прави процват у употреби. Данас, у нашим пословним банкама могу се добити све врсте савремених пословних картица (од Дине, Висе, Мастеркард-а до Динерс-а) које могу бити електронске (само уз магнетну траку), classic (ембосиране), до најсавременијих које се базирају на чип технологији. Банке у својим пословним буџетима улажу значајна финансијска средства у развој картичарства с обзиром на вишеструке предности, не само за њихове кориснике него и за банкарске установе.

Платне картице све више добијају на значају као метод обрачуна за плаћања на мало при куповини одређених производа или услуга. Највеће компаније које послују са кредитним или дебитним картицама организовале су засебне електронске клириншке и обрачунске системе. MasterCard и Visa имају своје сопствене мреже које се користе за верификацију трансакција широм света. Електронски терминали на месту продаје, ЕФТ/ПОС терминали, омогућавају да се подаци са картице провере за мање од 15 секунди у оквиру мреже која повезује продавце широм света са центром за обраду кредитних или дебитних картица и емитентом картица.

3.2. Даљинско банкарство

Технологије мењају начин комуникације међу људима, али и комуникацију између правних субјеката и њихових клијената. Донедавно је једини начин комуникације и пословања с банком била лична посета банци и разговор са службеником преко шалтера, ако не рачунамо извештаје који су долазили путем поште (поштом се нису могле обављати трансакције). Данас се канали које банке користе у комуникацији с клијентима више не могу побројати на прсте једне руке.

Историјски гледано прво су се појавили АТМ (Automated Teller Machine) уређаји, које чешће називамо банкоматима. Они су омогућили клијентима долазак до готовине у свако доба дана и ноћи. Напреднији АТМ уређаји могу и примати депозите. Мање-више упоредо

са АТМ уређајима су се појавили и ПОС терминали који су омогућили клијентима вршење електронског (безготовинског) плаћања на месту куповине. Базирајући се на својевремено најраширенијој комуникационој мрежи, мрежи фиксне телефоније, настало је Телефонско (кућно) банкарство које је од банака захтевало успостављање call центара и осмишљавање сигурносних мера како би се и клијенти и банка заштитили од злонамерника који би се лажно представљали. У ту сврху су се користиле ТАН картице у комбинацији с ПИН-ом, а касније и токени, уређаји који су генерисали једнократне лозинке које су гарантовале да се с друге стране жице налази управо онај клијент по чијем се рачуну обављају трансакције. Телефонско банкарство је омогућавало обављање трансакција и преглед стања на рачуну од било куда где постоји телефон, али телефон као такав није омогућавао једноставно и лако обављање трансакција (како због ограничене функционалности телефонске тастатуре тако и због потребе за комуникацијом са службеником с друге стране жице). Природан наставак те услуге је било слање извештаја факсом. РС банкарство је настало као одговор на изазове које је у себи носила чињеница да све већи број клијената располаже сопственим рачунаром (што су омогућили РС рачунари својим много приступачнијим ценама у односу на претходне генерације рачунара). РС банкарство је омогућило клијентима (правним и физичким лицима) да своје рачунаре повежу (преко класичних телефонских линија) са сервером банке и да на исти преносе своје (унапред) припремљене налоге и са њега преузимају податке који се тичу финансијских трансакција на њиховим рачунима. При томе је битно напоменути да је услугу РС банкарства корисник могао користити само на оном рачунару на којем је инсталисао одговарајући софтвер. Појава интернета је створила претпоставке за отклањање ове баријере, те је на таласу велике популарности веб сервиса глобалне рачунарске мреже настало интернет (веб) банкарство.

Интернет банкарство је кориснику први пут под прсте дало потпуну контролу над његовим рачунима. Трансакције које корисник обавља, односно задаје налоге банци, путем веб бровсера обављају се тренутно пред очима корисника. Али комуникација банака с корисником овде не стаје. Услуге банака се шире, како унутар интернет банкарства, тако и осмишљавањем нових канала комуникације према корисницима. СМС банкарство један је од тих канала који се базира на СМС сервису мреже мобилне телефоније. Мобилно банкарство је настало повезивањем мреже мобилне телефоније и интернет мреже. Овај облик електронског банкарства омогућује клијентима да са мобилних уређаја који су

мање-више стално уз њих користећи сервис интернета приступају својим рачунима. Као својеврстан резиме наведимо да се у електронском банкарству могу користити следеће дистрибутивне мреже и канали којима се остварују информациони и пословни контакти са банком.

- 1. АТМ системи (банкомати),**
- 2. ПОС системи,**
- 3. Телефонско банкарство,**
- 4. РС банкарство,**
- 5. СМС банкарство,**
- 6. Интернет банкарство,**
- 7. Мобилно банкарство,**
- 8. Видео банкарство.**

3.3. Банкомати

Први корак ка електронском банкарству је резултат развоја информационе мреже која је омогућила електронизацију шалтерског пословања путем банкомата, односно самоуслужних шалтера АТМ и ПОС терминала, с циљем повећања квалитета услуга банака и оријентације према клијентима.

АТМ (Automated Teller Machine) представља најраспрострањенију форму ЕФТ технологије. АТМ су машине које су дислоциране и повезане у банкарску мрежу. Погодност за клијенте је приступ рачуну 24 часа, брза услуга, без чекања у реду испред шалтера и све шира лепеза услуга која се нуди. Са друге стране, увођење АТМ за банке значи вишеструко смањење трошкова процесирања трансакција, смањење редова и гужва у банкама. Исто тако доводи и до рационализације броја запослених у пословима са становништвом и могућност остваривања додатних прихода од накнада за пружање услуга корисницима картица других банака. Поред већ традиционалне услуге подизања готовине, банкомати омогућују и упит у стање рачуна, полагање депозита, трансфер средстава са рачуна на рачун у оквиру банке, плаћање разних рачуна, куповину препаид бонова, и сл.



Слика бр. 1. Банкомат

У почетку пословања путем АТМ-а, поседовање мреже банкомата било је питање престижа међу банкама, па су се банке напросто утркивале у разгранавану сопствених мрежа банкомата. Касније су банке увиделе несврсисходност самосталног развоја мрежа банкомата, па су отпочели процеси њихове интеграције, при чему се две или више банака споразумевају о међусобном коришћењу својих мрежа банкомата. Банкомати су првобитно радили у offline режиму, шаљући податке о трансакцијама групно у одређеним временским интервалима, док данас већина банкомата ради у online режиму, односно трансакције се извршавају у реалном времену.

3.4. ПОС терминали

EFTPOS/POS систем (Electronic Fund Transfer on Point of Sale / Point of Service) је систем за електронски трансфер новца на месту продаје производа или услуга, који се остварује повезивањем малопродајног места са мрежом и базама података банака. Овај систем омогућава директан пренос средстава са рачуна купца на рачун продавца. EFTPOS терминали омогућавају да се подаци са картице провере за мање од 15 секунди у оквиру мреже која повезује трговце широм света са центром за обраду платних картица и емитентом картица.

Електронски системи плаћања и њихова заштита

Процес плаћања платном картицом на ПОС-у можемо упрошћено описати на следећи начин:

1. **Продавац израчунава вредност** купљеног производа или услуге и тражи од купца да плати,
2. **Купац даје платну картицу** продавцу,
3. **Продавац провлачи платну картицу** кроз ПОС терминал. Вредност продатог производа или услуге продавац уноси ручно или преузима из регистар касе,
4. **Продавац преноси податке о платној картици и вредности купљене робе или услуге својој пословној банци или ауторизационом центру, са захтевом за ауторизацијом.** Уколико се захтев преноси пословној банци трговца, она накнадно захтева ауторизацију од банке емитента картице,
5. Уколико власник картице има довољно средстава на свом рачуну или му је одобрена кредитна линија, банка **емитент картице или ауторизациони центар ауторизују трансакцију,**
6. **Банка емитент картице резервише средства на рачуну власника картице у износу вредности купљеног производа или услуге.** Рачун корисника картице се још увек не задужује. Банка емитент картице обавештава пословну банку трговца о прихватању (или одбијању) трансакције,
7. Након обрађене трансакције, **пословна банка трговца или ауторизациони центар шаље шифру одобрења (или одбијања) ПОС терминалу продавцу.** Сваки ПОС терминал има свој јединствени идентификациони број, тако да је институција која врши обраду трансакција у могућности да проследи податке управо том терминалу,
8. **Продавац штампа рачун (слип)** и захтева од купца да га потпише и на тај начин обавезује купца да надокнади назначени износ банци емитену платне картице,
9. На крају радног дана, **продавац упоређује ауторизације које су меморисане у ПОС терминалу са потписаним рачунима.** На основу тих података, банка која је емитовала платну картицу одобрава пословној банци продавца износ конкретног рачуна. Продавац је у обавези да плати дисконтну провизију од укупног износа продаје (у проценту који је договорио са емитентом картице).

Током задње деценије прошлог века, број ПОС-ова је значајно порастао. То значи да данас

већина продајних места прихватају платне картице којима се могу обављати плаћања. Плаћање путем ПОС-а је корисна алтернатива, како за купце, тако и за продавце (наравно не треба заборавити и корист за банке издаваоце платних картица). Продавци не морају да се брину да ли клијент има средства на рачуну, с обзиром да је провера online, док купац не мора да пише чек и безбедније је да не носи новац са собом.

3.5. Телефонско банкарство

Телефонско банкарство представља директно коришћење банкарских услуга од куће, пошто омогућава непосредан трансфер средстава, информација и налога путем телефонске мреже. Заснива се на тзв. позивним центрима, односно на системима којима се приступа преко одређених шифри откуцаних преко тастатуре. Може да се користи за проверу стања и трансакција на рачунима, отплате зајмова, плаћања унутар банке, слање стања рачуна на корисников факс, наручивање чекова, плаћање рачуна у земљи (телефонских рачуна, рачуна за струју, и сл.) и трансфера новца. За ову врсту услуга, ради идентификације, поред шифре може да се користи и токен.

Као карактеристични појавни облици телефонског банкарства у данашњим условима могу се навести:

1. **Говорни аутомати и**
2. **Call центри са оператерима.**

Коришћењем услуга **говорног аутомата** могуће је у сваком тренутку добити информацију о стању на рачуну. Једини услов за коришћење ове услуге је да се позив оствари са телефона који има могућност тонског бирања. Након позива телефонског броја говорног аутомата аутомат тражи да се унесе идентификациони број (ПИД), коришћењем тастатуре телефона. По уносу овог броја говорни аутомат даје инструкције у погледу даљих корака. Уколико су правилно унети подаци, аутомат ће одмах прочитати тренутно стање на унетом рачуну, а потом ће понудити и остале услуге:

1. **Слање обавештења о стању на рачуну на е-маил** дефинисан приликом попуњавања приступнице или
2. **Слање стања на рачуну на задати факс.**

У случају call центара са оператерима (банке ову врсту услуге најчешће наводе као Call центар сервис) комуникација преко телефона се, уместо са аутоматом, обавља са живим људима. У понуди Call центар сервиса најчешће се налазе следеће услуге:

Информативне услуге:

1. Стање и промене на рачунима
2. Информације о нереализованим чековима
3. Информације о позајмици
4. Информације о кредитима
5. Информације у вези трансакција са платним картицама, као и расположивим средствима за коришћење картице,
6. Информације о курсевима валута.

Финансијске трансакције:

1. Пренос средстава између динарских рачуна у банци
2. Пренос средстава између девизних рачуна у банци без конверзије валута
3. Куповина и продаја ефективе/девиза
4. Електронско плаћање предефинисаних налога
5. Плаћање рате кредита
6. Плаћање задужења по кредитној картици
7. Блокада картица у случају да је изгубљена или украдена.

3.6. РС банкарство

Online банкарство се спроводи путем интернета и представља комбинацију карактеристика програма за личне финансије и електронског плаћања рачуна. РС банкарство омогућава обављање банкарских трансакција директном везом клијента и банке уз помоћ специјализованог софтвера. Софтвер се инсталира на клијентов рачунар, тако да омогућује електронско повезивање корисника са рачунаром банке. На тај начин

клијент може да обавља трансакције (једино са датог рачунара).⁵ Сви подаци о извршеним налозима се налазе на персоналном рачунару на коме је инсталиран софтвер. За функционисање РС банкарства користи се директна online комуникациона веза између персоналног рачунара и рачунарског центра банке уз коришћење модема. РС банкарство је већу примену нашло код правних лица него код физичких лица.

Софтвер за online банкарство старије генерације захтевао је висок ниво познавања рачунара и искуство корисника. Садашњи програми који се користе за обављање online банкарских трансакција постали су лакши за употребу због тога што се имплементирају у стандардни Windows графички кориснички интерфејс, који пружа корисницима добро познате команде и функције. Највећи напредак да се олакша употреба истог постигнут је захваљујући томе што су на тржиште ушле фирме као што су Intuit и Microsoft, које имају више искуства од великих банака у писању софтвера за клијенте.

Произвођачи софтвера преузели су на себе улогу премошћавања јаза између банака и клијената и омогућили су и мањим банкама да понуде производе online банкарства путем софтверских решења (на пример, Halcom – ово решење за РС банкарство за правна лица). То је довело до извесног степена уопштавања online банкарства, тако да оно више не представља производ којим би нека банка могла да се диференцира од друге. За обављање банкарских трансакција у online РС банкарству:

- 1. Потребан је специјализован софтвер који се купује,**
- 2. Овај софтвер се инсталише на рачунар клијента,**
- 3. Потребно је време за овладавање програмом,**
- 4. Клијент може обављати трансакције само са свог рачунара,**
- 5. Трансакције се могу евидентирати у offline и online режиму**
- 6. Пренос/пријем података ка банци захтева он лине везу и**
- 7. Клијентови подаци о обављеним трансакцијама остају на његовом хард диску, а по преносу и на банчином серверу.**

Online РС банкарство има и одређене недостатке. Корисник електронске банке је ограничен да обавља трансакције само са оног рачунара на којем је инсталисан софтвер.

⁵ www.poslovnimagazin.biz/magazin/srbija прегледано: јун, 2014.

Поред тога, промена банке захтева и нови софтвер и поновни унос података, као и потребно време за обуку за рад. Online PC банкарство омогућава клијенту да припрема налоге у offline режиму, односно да припрема и чува налоге који ће тек касније бити реализовани. Трансакције могу да се обављају непрестано, а извршење трансакција у интерном платном промету је тренутно (између правних лица која су депоненти банке). Могуће је вршити пренос између својих рачуна, плаћање рачуна, вршити преглед стања на својим рачунима, и сл. Путем PC банкарства клијенти могу да добијају изводе и извештаје о променама на рачуну, по динамици која им одговара. Клијенти имају могућност и да врше издавање налога са валутирањем унапред. Поред тога, могу се дефинисати привилегије по појединцу-кориснику, на пример, може се омогућити увид у стање само одређених рачуна, плаћање само до одређеног износа, преглед промета без могућности плаћања, и сл. Сви подаци су тајни и доступни су само ономе коме су намењени.

Већина банака у домицилном окружењу користи е-банкинг решења словеначке софтверске куће Halcom. Једна од првих банака из домицилног окружења, која је омогућила овај вид електронског банкарства јесте некадашња Новосадска (сада Ерсте) банка. Под називом Новоклик је понуђено софтверско решење из домена PC банкарства намењено правним лицима, клијентима банке. Да би клијент користио решење PC банкарства потребно је да инсталира софтвер на свој персонални рачунар. Поред тога потребно је да корисник поседује читач смарт картице и смарт картицу (на коме се налази дигитални сертификат). Читач смарт картице прикључен је на персонални рачунар. За улаз у програм потребно је ставити смарт картицу у читач и уписати лозинку.

Активирањем дигиталног сертификата са смарт картице остварује се конекција између корисника и банке. Уколико клијент изгуби картицу и ако је налазач покуша употребити, картица се сама уништи након три покушаја уписа погрешне лозинке.

3.7. СМС банкарство

Уважавајући убрзани темпо живота, банке се опредељују да задовоље потребу својих клијената да било када и било где, брзо и дискретно добију корисне и тачне информације о стањима њихових рачуна. Да би клијент банке адекватно могао да управља својим средствима, потребна је тачна и поуздана информација о стању његовог рачуна у банци.

Традиционални модел прибављања овакве информације подразумева одлазак до шалтера банке или звање одговарајуће експозитуре, што изискује знатан утрошак времена и новца. Решење за превазилажење просторног и временског ограничења нашло се при употреби мобилног телефона и СМС-а. Уколико корисник жели да податке о свом рачуну добија путем кратких порука, неопходно је да у организационој јединици банке која пружа такву могућност попуни посебну приступницу у којој даје податке о рачуну и број мобилног телефона са кога ће постављати упите. За коришћење ове услуге потребан је рачун отворен код банке и било који тип мобилног телефона. После ауторизације и одобравања приступнице, клијент банке аутоматски добија поздравну поруку на свој мобилни телефон, која га обавештава да је постао активни корисник ове услуге.

Активирана услуга омогућава клијенту, у сваком моменту:

1. **Проверу стања на рачуну, на захтев, дневно или по промени** (где се дефинишу параметри прилива на рачун при којем се добија адекватна СМС порука, подаци о стању чекова, последња промена/транзакција, и сл.),
2. **Обављање платне трансакције**, при чему се могу вршити плаћања само на унапред наведене рачуне,
3. **Увид у важећу курсну листу** и сл.

Можемо дати упрошћени пример корићења СМС банке од стране корисника. Примера ради, клијент банке може да врши упит у стање свог рачуна. Потребно је да корисник са свог мобилног телефона пошаље поруку, на број сервисног центра банке, која ће садржавати шифру за проверу стања рачуна. Тражене податке о стању рачуна корисник добија у облику поруке на свој мобилни телефон. Порука стиже у врло кратком року, који варира у зависности од степена оптерећености мобилне мреже, али који је ретко када дужи

од једне минуте. Систем сигурности је заснован на повезаности трансакционог рачуна и броја мобилног телефона (неке банке користе и ПИН), као и унапред дефинисаним и похрањеним бројевима рачуна у корист којих се може извршити плаћање.⁶

За разлику од РС банкарства у СМС банкарству је доминантно учешће корисника физичких лица (преко 95%). Већу заступљеност СМС банкарства код грађана можемо објаснити следећим разлозима: први разлог је што у апсолутним бројевима гледано има много више потенцијалних корисника физичких лица, у односу на правна лица. Други разлог је што велика предузећа која користе online банкарство или Интернет банкарство имају online увид у стање и промене свог рачуна, па им услуге овог вида електронског банкарства нису толико неопходне. У прилог томе говори и чињеница да су корисници СМС банке правна лица углавном мања предузећа која не користе друге видове електронског банкарства, а имају потребу да, по потреби, провере стање свог рачуна или прате приливе и/или одливе са свог рачуна.

3.8. Интернет банкарство

Интернет банкарство представља прибављање банкарских информација и реализацију банкарских трансакција преко Интернета. Интернет банкарство је засновано на коришћењу World Wide Web, где се кориснику омогућује директан приступ путем веб браузера. Напредак у производима online банкарства, промене у конкурентској структури и растућа популарност Интернета су створили окружење у коме Интернет банкарство постаје производ за масовну потрошњу.

Обављање Интернет банкарства и поред сличности са РС банкарством претпоставља одређене разлике. Код Интернет банкарства приступ рачуну омогућен је путем бровсера (претраживача), што елиминише потребу за специјалним софтвером. Интернет банкарство омогућује приступ електронској банци са било ког рачунара у свету, који је на неки начин прикључен за Интернет. Подаци о обављеним трансакцијама нису ускладиштени на хард

⁶ Станкић Р., *Електронско пословање*, Економски факултет Београд, 2007. стр. 179.

диску, па је и сигурност већа, а банка одржава заштиту система. Трансакције се обављају online.

У самом почетку појављивања банака на Интернету, банке су се представљале само информативно, и то постојећим или потенцијалним клијентима. Таква једносмерна комуникација имала је углавном рекламни карактер. Касније, банке почињу са двосмерном комуникацијом са клијентима, и то путем е-маил-а или интерактивним приступом неком сервису. Овакав вид комуникације, поред маркетиншког аспекта омогућује и располагање додатним информацијама од стране клијената. Након тога, банке су се определиле за обављање банкарских трансакција на Интернету, и то представља највиши ниво комуникације банке са својим клијентима.

Веб банкарство има многобројне предности и ефекте у односу на досадашњи класичан пословни однос банка-клијент. Предности новог начина пословања путем веб банке су:

1. **Могућност обављања послова са било које локације** у земљи или свету,
2. **Није потребан специјалан софтвер** и подаци нису ускладиштени на клијентовом хард диску, што даје већу сигурност при обављању трансакција,
3. **Јефтинији начин обављања послова са банком** - уштеда у новцу јер је услуга обављена путем веб банке јефтинија него услуга реализована класичним методама (на шалтеру банке),
4. **Нема радног времена**, односно могућност обављања послова од стране клијената са банком је 24 часа дневно,
5. **Ажурност обавештавања о променама на рачуну**,
6. **Једноставност прикључивања на веб банку**,
7. **Лакоћа употребе**.

Ширењем примене Интернета и појавом виртуелних банака јавио се притисак на класичне банке да промене свој приступ клијентима и пословању, јер су почеле да губе клијенте, послове и профит, док су са друге стране виртуелне банке доживеле успех. Опстанак класичних банака је почео да зависи од њихове спремности да део пословања пренесу на интернет.

Платни системи и трансакциони механизми данас напросто не могу да заобиђу Интернет, који полако прожима све људске активности. Интернет је учинио да кућно банкарство буде једноставније за примену и јефтиније, будући да су улагања у опрему минимална ако је корисник већ прикључен на Интернет. То све наговештава да ће већу перспективу имати код домаћинстава. Са друге стране, трошкови по трансакцији су најнижи ако банка као канал за пружање услуга користи Интернет. Све форме виртуелног банкарства зависе од подршке call центра. Ова подршка је од изузетне важности и код Интернет банкарства. При коришћењу Интернет банкарства, клијенти имају доста питања, а посебно око њима непознатих процедура. Банке које пружају услуге Интернет банкарства би требале да омогуће да клијенти слање е-маил порука call центру, са веб сајта банке. Још напреднијим решењем се сматра успостављање chat room – а, где клијенти могу обављати конверзацију са банкарским службеницима.

Као и у случају РС банкарства већина домицилних банака користи Halcom – ово софтверско решење за обављање ове врсте послова.

Сам приступ клијентима је омогућен на више начина, путем корисничког имена и лозинке или путем смарт картице. Сматра се да је приступ путем смарт картице неупоредиво сигурнији али мање преносив јер је приступ овим услугама могућ само са рачунара који имају читач картице.

3.9. Мобилно банкарство

Мобилно банкарство омогућава трансакције путем преносних рачунара (лаптоп), дигиталних личних организатора (ПДА) и мобилних телефона, који су опремљени специјалним софтвером за мобилни приступ Интернету, па се могу користити за обављање свих врста услуга и трансакција.

Мобилна плаћања путем мобилних телефона (Mobile payments / М - payments) спадају у групу плаћања на мало. Мобилни телефони могу бити уређаји којима се обавља плаћање у садејству са другим уређајима (на пример, као што је случај код плаћања мобилним

Електронски системи плаћања и њихова заштита

телефоном на ПОС терминалима) или се плаћање може обавити само употребом мобилног телефона.

Учесници у мобилним плаћањима су мобилни оператери, банке и друге финансијске институције, трговци и потрошачи. Број људи који користе мобилни телефон за обављање плаћања се брзо повећава. Са развојем услуга мобилне телефоније и њиховим ценовним појефтињењем овај медиј намењен превасходно за комуникацију почиње да поприма улоге медија за трансакције и комуникацију не само са финансијским институцијама, већ и са малопродајним објектима.

У почетку су се мобилна плаћања обављала размењивањем СМС порука између клијената и банке. Развојем war стандарда који је омогућио приступ Интернету са мобилног телефона било је могуће користити све предности online банкарства. То значи да је клијентима банке омогућено да уз помоћ мобилног телефона, а путем Интернета приступе свом рачуну у банци. Конекција са банком се остварује путем мобилног телефона који у себи има уграђен war уређај. Да би могла да се користи war услуга било које банке, корисник мора да има war прилагођени уређај (мобилни телефон). При свему томе корисник једино плаћа утрошене импулсе оператору мобилне телефоније. Индикатор развоја и значаја мобилних плаћања у будућности је перманентан раст броја корисника м-банкарства.

Табела бр. 1. Број активних корисника мобилног банкарства у милионима

Регион	2010.	2011.
Северна Америка	19,0	29,8
Западна Европа	25,6	36,1

Подаци из табеле 1. указују да је за само годину дана број активних корисника мобилног банкарства у развијеним земљама порастао за око 50%. Данас је близу 10% власника мобилних уређаја у овим земљама уједно и корисник мобилног банкарства (у Европи у овом погледу предњачи Француска).

Фактори који утичу на динамичан развој мобилног пословања су:

1. Релативно мала улагања,
2. Једноставност уређаја и лакоћа употребе,
3. Већи комфор у коришћењу.

Фактори који утичу на успоравање динамичног развоја су:

1. Несигурност потрошача да шаљу податке преко мобилне мреже,
2. Непостојање јединствених стандарда у овој области и сл.

Коришћење мобилног банкарства је једноставан процес. Након обављене регистрације корисник добија СМС потврду регистрације, ПИН код и упутство за коришћење. Поступак је још сигурнији је корисник сваку трансакцију ауторизује својим личним кодом. Путем мобилног телефона, корисник се конектује на интернет и улази у апликацију а у оквиру апликације он бира жељену услугу.

4. СОФТВЕРСКА РЕШЕЊА ЗА Е – БАНКАРСТВО

Када је реч о развоју софтверских решења већ је у последњој деценији прошлог века била приметна тенденција компанија, па тако и банака, да све више имплементирају готова решења наменски развијена од стране софтверских кућа. До тада доминантан самосталан развој се у условима растуће тражње за новим софтверским решењима показао као недовољно ефикасан како у погледу брзине тако и у погледу трошкова развоја. Произвођачи софтвера су све више преузимали на себе улогу премошћавања јаза између информатичких развојних капацитета банака и потреба клијената.⁷

Третирање софтвера као робе широке потрошње и његово вишеструко продавање различитим банкама довело је до смањења његове продајне цене, што је омогућило да и мање банке много брже понуде производе електронског банкарства него што би то учиниле у случају потпуно самосталног развоја ових решења. С друге стране, преузимање решења развијених од стране софтверских кућа довело је до извесног степена уопштавања електронског банкарства, тако да решења из овог домена више не представљају елементе по којима би нека банка могла значајно да се диференцира од друге.

То је случај и код домицилних банака које претежно користе е-банкинг решења словеначке софтверске куће Halcom d.d. из Љубљане, која је уједно и регионални лидер у овој области. Банке могу бирати између куповине и инсталације софтверског решења на локацији банке (тзв. Inhouse решење) или аутсорсинга (енгл. Outsourcing) софтверског решења. Outsourcing је широк појам који у начелу значи поверавање пројекта, пословног процеса или неких послова на извршење outsourcing партнеру које се одвија изван компаније и не захтева ангажовање ресурса унутар компаније. У outsourcing варијанти банка и фирма испоручилац (е-банкинг) услуга потписују споразум којим се дефинишу услови под којима ће екстерна фирма пружати одређене услуге банци као свом клијенту. У конкретном случају то значи да ће outsourcing фирма на својој локацији инсталирати и одржавати софтверска решења електронског банкарства која ће бити доступна како радницима тако и клијентима банке на исти начин као да је софтвер инсталисан на локацији банке.

⁷ http://www.ef.uns.ac.rs/Download/informacioni_sistemi_u_finansijama_bankarstvu_i_osiguranju/2012-12-12%20-%20Skripta%203%20-%20e-Banking.pdf прегледано: јун, 2014.

Nalcom је 2002. године основао предузеће са седиштем у Београду које представља outsourcing центар за електронско банкарство и многе домицилне банке користе услуге исте. Ово значи да клијенти банке приликом коришћења својих клијентских е-банкинг решења заправо приступају серверима који се налазе у outsourcing центру.⁸

Поред Nalcom – а регионалним лидерима у области софтверских решења електронског банкарства сматрају се још и хрватске компаније Абит и Логос. Абитова решења Интернет (+СМС) и мобилног банкарства су изведена као Јава веб апликације, а нашла су примену на тржиштима Хрватске и БИХ. Попут АБИТ-а и ЛОГОС је предузеће специјализовано за развој, интеграцију и имплементацију решења намењених финансијском сектору. Једна је од водећих компанија у регији на подручју решења за call/контакт центре, аутентификацију, дигитални потпис темељен на PKI/smartcard технологији и мобилно банкарство. ЈiМВа је Логосово решење за мобилно банкарство које омогућује брз и сигуран приступ финансијским информацијама и услугама с мобилних телефона с подршком за Јава технологију. Захваљујући популарности и широкој примени Јава технологије, Логосова м-банкинг апликација ради на већини доступних мобилних уређаја и подржава различите мобилне мреже. Апликација додељује кориснику токен за аутентификацију чиме се елиминише потреба за додатним уређајем и интеракцијом корисника. Сигурност, укључујући периоде надоградње, је базирана на HTTPS енкрипцији.

⁸ www.bankerinter.net прегледано: јун 2014.

5. УПРАВЉАЊЕ РИЗИЦИМА У ЕЛЕКТРОНСКОМ БАНКАРСТВУ

Развој услуга електронског банкарства и електронске трговине (укључујући и електронски новац) могу да пруже значајне могућности за банке. Примера ради, то су ширење тржишта за депозитне и кредитне послове, могућност понуде нових производа и услуга, побољшање конкурентске позиције, смањење трошкова банке, и сл. Међутим, примена информационе технологије у банкарству доноси, са једне стране, снажан пораст организационих и економских потенцијала, а са друге стране, отвара простор за појаву нових облика ризика. Значи, брзи развој потенцијала е-банкинга носи и ризике и користи. Због тога се адекватно обезбеђење сигурности, појављује као посебан критичан фактор у функционисању електронског банкарства. Суштина проблема безбедности савремених система електронског банкарства своди се на ризике нарушавања безбедности података и идентитета субјеката, при чему се релативни однос значаја поменутих елемената мења са технолошким развојем.⁹

Остваривање потребног нивоа безбедности захтева мултидисциплинарни приступ, односно пружање подршке системима заштите од ризика, како техничко-технолошким средствима, тако и одговарајућим организационим мерама, као и адекватном законодавном регулативом. У складу са оваквом потребом дошло је до формирања посебне Групе за електронско банкарство при Базелском комитету који се бави глобалним надзором над банкама. Банке се током пружања услуга електронског банкарства и употребе електронског новца суочавају са одређеним сетом специфичних ризика, који су разматрани у документима Базелског комитета за банкарску супервизију, а то су:

1. **Оперативни ризик,**
2. **Репутациони ризик,**
3. **Правни ризик,**
4. **Ризик интернационалног пословања,**
5. **Остали ризици.**

⁹ Марић С., Новаковић И., *Електронско пословање*, Кварк Краљево, 2006. стр. 205.

Са развојем технологије информационих система, долази до битних промена у суштинским карактеристикама самих ризика, са једне стране, и развоју механизма и система заштите од губитака које они производе, са друге стране. Постоје различите класификације ризика који су иманентни е-банкарству, а брзина промена у техничко-технолошкој основи отвара простор за нове систематизације и проширења. Једна од корисних класификација може бити подела (према узроцима настанка) на објективне и субјективне ризике. Објективни ризици би били они који настају као последица природе и карактеристика самих информационих система, а субјективни ризици би били они који настају намерним понашањем појединаца или групе.

Оперативни ризик настаје из потенцијалног губитка услед недостатака у систему поузданости и интегритета. Разматрање сигурности је од највеће важности, услед могућности интерних и екстерних напада на банку, односно њених система и производа. Оперативни ризик може настати и услед злоупотребе од стране клијената или неадекватног дизајнираног или имплементираног електронског банкарства или система електронског новца. Сходно изнетом, могући су следећи облици оперативног ризика: ризици сигурности (поузданости и интегритета система), ризици дизајнирања, имплементације и одржавања система, ризици злоупотребе производа или услуга од стране клијената.

Ризици сигурности се појављују у вези са контролом информација помоћу којих банка комуницира са окружењем, трансфера електронског новца, као и спречавања проневере, односно фалсификата. Контрола приступа систему банке постаје све комплекснија с обзиром на проширење рачунарских система, географске дисперзираности приступних тачака систему и употребе различитих комуникационих путева, укључујући и јавну мрежу као што је Интернет. Неауторизовани приступ систему банке од стране хакера може проузроковати злоупотребу поверљивих информација о клијентима, као и директне трошкове банке. Такође у одсуству адекватне контроле, неовлашћено лице може приступити систему и убацити вирус у њега. Није занемарљива и могућа злоупотреба од стране запослених, чија превентива изискује успостављање система адекватне контроле. Постоји и ризик фалсификовања електронског новца, чија превентива захтева одређене видове техничке заштите.

Пример могућег ризика сигурности јесте неауторизовани приступ систему. То значи да поверљиве информације могу бити пресретане од стране неауторизованих лица, на пример, од стране хакера који улазе у интерне системе. Могуће је убацивање вируса у банкарски систем, што доводи до оштећења или уништења банкарског система или података. Потенцијални ефекат на банку је губитак и крађа података. Поред тога, онемогућава се функционисање банкарског информационог система или бар једног дела. Јављају се и трошкови за отклањање проблема. Поред тога, може се створити потенцијална несигурност у банкарски систем и негативна реклама. Банке могу да примене одређене мере за управљање ризиком. Могуће је применити сигурносне комуникативне мере, као што су, лозинке, технологија шифровања и ауторизација корисника. Потребно је вршити тестирање на „рањивост“ система, као и стално проверавање система на вирусе. Треба поменути и могући ризик по систем који се спроводи од стране запослених, односно преваре запослених. Могућа је злоупотреба података како би искористили средства са рачуна банке или прикупили одређене информације из система.

Репутациони ризик је ризик негативног јавног мњења, који резултира значајном губитку средстава или одливу клијената из банке. Његов негативан ефекат на имиџ банке, може да буде трајан. Може настати и као последица предузимања акција које имају за последицу губитак јавног поверења у способност банке да обавља своје пословање. Значајно нарушавање имиџа банке може настати и услед лоших комуникационих мрежа, при чему клијенти нису у стању да сазнају информације о стању на својим рачунима, и сл. Репутациони ризик може настати ако производи или услуге које банка пружа не задовољавају очекивања својих клијената, што доводи до негативне јавне реакције, или ако је банка изложена малверзацији и обмани од екстерне стране, која ће се одразити кроз несигурност клијената ка банкарском сектору. Одржавање репутационог ризика је битно не само због одржавања доброг имиџа поједине банке већ и целокупног банкарског сектора, јер ако би била нанета штета одређеној банци у делу електронског пословања, тиме би била пољуљана сигурност и у друге банке, односно у целокупан систем. Пример репутационог ризика је нарушавање безбедности система. Улазак хакера у интерни систем, или убацивање вируса у банкарски систем може изазвати значајне проблеме у функционисању система или у очувању интегритета података. То може довести до тога да клијенти престану да користе услуге банке, односно утиче на одлив клијената из банке.

Могућа мера је тестирање система и примена сигурносних мера, као и проверавање система на вирусе. Пример репутационог ризика за банке свакако би могао бити и спречавање настанка одређеног догађаја. Ако се банка може похвалити да у претходном временском периоду од неколико година није имала неовлашћених улазака у оперативни - електронски систем банке, да гарантује тајност података које електронски обрађује, свакако за ову банку можемо рећи да је минимизирала репутациони ризик. Насупрот томе, ако је банка позната по „честим“ неауторизованим уласцима у оперативни систем и ако се на овај начин може десити да дође до злоупотребе добијених информација свакако да ова банка може у будућности очекивати проблеме са клијентима управо услед настанка репутационог ризика. Да би банка могла да се заштити од репутационог ризика, потребно је да пружа услуге електронског банкарства доследно и константно, а све у складу са високим очекивањима клијената. Банка мора да има могућност да пружа услуге електронског банкарства свим корисницима, тако да је потребно да одржава доступност система у свим околностима. Битно је да се успоставе механизми за ванредне ситуације да би се минимизирао репутациони ризик који може произићи из неочекиваних догађаја, укључујући интерне и екстерне продоре у систем који могу утицати на пружање услуга електронског банкарства. Банке би, у циљу испуњења очекивања клијената, требале да ефикасно планирају капацитете, пословни континуитет и поступање у случају непредвиђених околности. То значи да би требале да израде одговарајуће планове за ванредне ситуације, укључујући комуникацијску стратегију, која би обезбедила континуитет пословања, као и контролу репутационог ризика. Планови за ванредне ситуације би омогућили опоравак система и услуга електронског банкарства при различитим сценаријима. Анализа сценарија би требала да обухвати разматрање вероватноће настанка ризика и његовог утицаја на банку. Поред тога, банке би требале да утврде механизме за утврђивање настале ванредне ситуације чим се она појави, уз јасно дефинисање противмере која треба да буду спроведена да би се минимизирао ефекат насталог догађаја. Такође је неопходно да службе за подршку клијентима редовно прате и преиспитују притужбе клијената, јер се на овај начин могу добити значајне информације о нефункционалности система и будућим пољима које је потребно успешније сервисирати, како би оперативност и ефикасност система била на вишем нивоу.

Правни ризик настаје услед нарушавања или неусаглашености са законима, правилима, регулативама или прописане праксе или у случају када законска права и обавезе учесника у трансакцијама нису правно регулисана. Посебно мора бити регулисано спречавање прања новца, јер савремена могућност пословања у великој мери може бити веома атрактивна за такав вид злоупотребе. То доводи до закључка да банке које примењују електронско банкарство и пословање са електронским новцем, морају посебну пажњу посветити идентификацији, односно аутентификацији клијента, као и заштити приватности (као метод аутентификације банке могу да користе дигиталне сертификате). Један од правних ризика је и прање новца. Електронска банка може бити злоупотребљена од стране клијената и за криминалне радње, односно прања новца. Могуће су правне санкције за банке, односно казне за непридржавање закона. Неопходно је да банка развије механизме за идентификацију клијената, као и процедуре које ће омогућити да се уочи и извести о сумњивим трансакцијама. Поред тога, потребно је развити планове за случај да се догоде непредвиђене ситуације и да се врши константна обука запослених.

Један од ризика је и заштита приватности клијената. Уколико би банка објавила информације о финансијским трансакцијама клијента без његове претходне сагласности, могла би бити тужена за нарушавање приватности, као и да сноси трошкове тужбе. У том случају, банка може да се суочи са правним санкцијама. Потребно је да банка преиспита процедуре заштите приватности и да врши периодично преиспитивање истих, као и да обучава запослене за примену усвојених процедура. Заштита клијената, као и прописи и закони који се односе на приватност клијената се разликује од земље до земље. Ипак, банке имају одговорност да осигурају својим клијентима одређен ниво сигурности, што се тиче објављивања информација, заштите података о њима, као када би клијенти обављали послове преко традиционалних банкарских канала дистрибуције производа и услуга. За банке је кључна одговорност очување поверљивости информација о клијентима. Злоупотреба или неауторизовано објављивање поверљивих података о клијентима може да изложи банку правном и репутационом ризику. Да би банке обезбедиле поверљивост информација о клијентима, потребно је да установе политике и стандарде које се односе на приватност клијената, а које би требале да буду усклађене са свим прописима и законима о приватности који се примењују у земљама у којима банка пружа производе и услуге

електронског банкарства. Поред тога, подаци о клијентима се не би смели користити, осим у посебно допуштене сврхе и ако су клијенти ауторизовали њихово коришћење.

У неким земљама, закони и прописи не обавезују банке да траже од клијената допуштење за коришћење података о њима у интерне сврхе. Међутим, они могу обавезивати банке да клијентима пруже могућност одбијања давања допуштења банци да дели такве информације с трећом страном или с повезаним друштвом. У другим земљама, клијенти могу имати право да спрече банке да се користе њиховим подацима било у интерне било у екстерне сврхе. Да би банке минимизирале правни ризик, повезаним са пословима електронског банкарства који се обављају у земљи и иностранству, потребно је да осигурају пружање адекватних информација на својим веб страницама. На тај начин би се клијентима омогућило да провере идентитет и регулаторни статус банке пре него што се упусте у трансакције електронског банкарства. Примера ради, информације које се могу ставити на веб сајт могу бити име банке и локација седишта, као и локалне филијале, начин на који клијент може контактирати са банком по питању рекламација, сумње на злоупотребу рачуна и сл., начин на који се клијенти могу жалити органу које се бави заштитом потрошача, и др.

У домицилним условима, значајном смањењу правног ризика допринела је и Народна банка Србије низом мера и одлука којим су уредиле пословање банака у овој сфери. Бројни су примери заштите потрошача путем обелодањивања основних информација о банци (на пример, на свим дописима тј. меморандумима пословних банака обавезно је да се наведу подаци који се односе на назив банке, матични број, седиште, број рачуна, али и подаци који се односе на последњи познат износ тј. висину капитала банке). Затим, НБС инсистира и на увођењу новог одељења у пословање банака - одељења Compliance.

Електронско банкарство и активности електронског новца су базирани на технологији која не познаје географске баријере. Таква тржишна експанзија може да се шири преко националних граница, али се са тим повећава и ризик пословања. Ризици, карактеристични за домицилно банкарство су такође релевантни и за интернационално банкарство, с тим што ови ризици могу бити још наглашенији. Примера ради, у пословању путем Интернет банкарства могући су карактеристични правни захтеви (заштита потрошача, законски пропис о спречавању прања новца, и сл.), чије непримењивање може

да изложи банку правним ризицима. У интернационалном пословању повећан је и кредитни ризик услед отежане оцене кредитне способности тражиоца кредита. Банке које се одлуче да пружају услуге клијентима на разним националним тржиштима требало би да упознају разне националне правне захтеве, као и да разумеју националне разлике у очекивању и познавању производа и услуга од стране клијената. Са друге стране, неопходно је да банка процени ризик земље и развије планове непредвиђених обавеза који ће предвидети активности у случају економских или политичких проблема на националном тржишту. Под економским проблемима се подразумевају промене привредних кретања, привредног развоја, услова пословања у одређеној земљи и њена спољна ликвидност, док се под политичким проблемима подразумева промена у саставу владе или владине политике, политички немири или ратови. Наравно да се наведене економске и политичке промене сматрају проблемима уколико иду на штету пословању банке. **Ризик трансфера** расте са прихватањем иностраних процесора и других иностраних учесника у електронском пословању. Страни процесори или други учесници у електронском пословању са банком могу бити у немогућности да испуне своје обавезе због социјалних, економских или политичких разлога. Постоје и потенцијални трошкови решавања проблема купаца. Поред тога, банка може да се суочи са тужбом корисника услуга. Мере које банка може применити у управљању ризиком јесте да изврши процену ризика земље.¹⁰

Остале банкарске ризике укључује и **кредитни ризик, ризик ликвидности, каматни ризик и тржишни ризик**, који могу настати из електронског банкарства и пословања са електронским новцем.

Кредитни ризик је ризик који се односи на корисника кредита да неће испунити своју обавезу у пуној вредности или у предвиђено време. Банке имају могућност да електронским путем приме захтеве за кредит и да га одобре, што захтева адекватне процедуре за утврђивање кредитне способности клијената, јер се у противном повећава ризик за банку. Као што је наведено, пример кредитног ризика је и неспособност плаћања обавеза дужника који је кредит добио путем Интернета. Банка може одобрити кредит клијентима ван свог тржишта, при чему се може десити да јој подаци нису познати или су

¹⁰ Вуксановић Е., навед. дело, стр. 118.

скупи да би их прикупила. Потенцијални ефекат за банку је да мора изврши резервисања за лоше пласмане. Банка може да спроведе одређене мере за управљање ризиком. Примера ради, да обезбеди да је процена кредитне способности клијената који су на овај начин затражили кредит, иста као и код „традиционалних” тражилаца кредита и да изврши ревизију процедура одобравања кредита.

Могући ризик за банку је и неспособност плаћања обавеза издаваоца електронског новца. Издавалац електронског новца може постати несолвентан и неликвидан, док банка „држи” електронски новац у свом поседу. Ефекат тога је да ће банка можда морати да користи сопствена средства како би ослободила електронски новац који се налази код њених клијената.

Могуће мере за управљање ризиком јесте ревизија свих издавалаца електронског новца и мониторинг, односно надгледање финансијске снаге издавалаца електронског новца. Кредитни ризик представља основни ризик у пословању банке са клијентима, који настаје када дужници банке нису у могућности да сервисирају своје обавезе према банци, односно да врате кредит (или друге видове пласмана) са припадајућом каматом (и/или накнадом) о року њиховог доспећа. Као резултат тога јавља се губитак у билансу успеха банке. Банка може да управља са кредитним ризиком на следеће начине:

1. **Применом лимита** (однос ризичне и укупне активе, однос готовине и краткорочних хартија од вредности према укупној активи, однос капитала и резерви банке),
2. **Ригорозном селекцијом кредитних захтева,**
3. **Диверзификацијом пласмана кредитне активе** (на већи број корисника кредита са мањим обимом одобрених кредитних износа),
4. **Инструментима обезбеђења** (цедирано потраживање, ломбардна залога, хипотекарна залога, положени депозит за измирење главнице кредита и камата, положен будући девизни прилив и сл.).

Ризик ликвидности је ризик који настаје у случају да банка није у могућности да извршава доспеле обавезе које настају током електронског банкарства. Ризик ликвидности је ризик могућности настанка негативних ефеката на финансијски резултат и капитал

банке услед неспособности банке да испуњава своје доспеле обавезе. Банка својом имовином и обавезама управља на начин који јој омогућава да у сваком тренутку испуни своје доспеле обавезе (ликвидност) и да трајно испуњава све своје обавезе (солвентност). У циљу ефикасног управљања ризиком ликвидности, банка усваја и спроводи политику управљања ликвидношћу, која обухвата планирање прилива и одлива новчаних средстава, праћење ликвидности и доношење одговарајућих мера за спречавање или отклањање узрока неликвидности. Неликвидност издаваоца електронског новца може да изненадно повећа тражњу за повлачењем електронског новца из оптицаја. Банка може претрпети губитке тражећи алтернативне изворе финансирања. Уколико се у јавности наслути проблем ликвидности, биће још више присутније повлачење депозита из банке или повлачење електронског новца. Неиспуњавање ових обавеза (у смислу поврата депозита) може довести и до озбиљних репутационих проблема. Мере које банка може спроводити су да инвестира средства у ликвидну активу и да развије мониторинг коришћења средстава. Пример ризика ликвидности у електронском банкарству је пример ризика секундарног значаја, наиме ризик ликвидности је више класичан банкарски ризик и настаје у тренуцима када банка није у могућности да испуњава своје дневне обавезе услед повећаног повлачења депозита њених клијената или услед великог одлива средстава. Исто овакво дејство ризик ликвидности може да произведе и код пословних банака које су се оријентисале на електронско пословање (у домицилним условима још увек немамо овакву институцију и морамо напоменути да су све банке, банке класичног – универзалног типа које су више или мање развиле електронске канале комуникације са клијентима). Наиме, услед одређених информација које се могу појавити на тржишту (поготово у развијеним земљама где је приступ информацијама лакши и бржи), услед лоших пословних потеза управе банке или лошег, односно погрешног инвестирања финансијских средстава, у јавности може да се створи утисак да банка не послује адекватно, да ће у будућности претрпети губитке и др. Све ово може да доведе, уколико управа и менаџмент банке не одговори адекватно, до одлива депозита и физичких и правних лица и нарушавања ликвидности банке. У оваквим ситуацијама банка мора да има план односно одговор како би се са једне стране смањиле и минимизирале последице настанка штетног догађаја, а са друге стране банка мора да задуживањем на финансијском тржишту преброди проблем ликвидности који је настао као последица повлачења средстава клијената.

Каматни ризик се односи на смањење каматних стопа до степена када негативна кретања каматних стопа смањује вредност имовине у зависности од неиспуњених обавеза. Неочекиване и непожељне измене у каматним стопама могу умањити вредност активе издаваоца електронског новца у односу на стање издатог електронског новца. Неочекивано опадање вредности активе може довести до ситуације да банка не испуњава законске захтеве. Може настати и проблем ликвидности. Каматни ризик се састоји од ризика промене каматних стопа на пласмане и обавезе банке, наравно уколико су ове промене неповољне за банку. На пример, клијенти увек имају захтеве према пословним банкама да се пласман средстава банке врши уз што ниже каматне стопе, с обзиром на тржишну утакмицу између пословних банака. Ризик каматне стопе може да настане у случајевима када банке одобре одређене пласмане по фиксним каматним стопама на дуже временеске периоде, који нису пропраћени адекватном структуром извора средстава банке. Ово значи да је банка пласирала средства по одређеној каматној стопи на дуже рокове него што има обезбеђене депозите. У случају одређених поремећаја на тржишту, извори средстава могу да поскупе, што би довело до ситуације да банке имају одређене губитке на пласманима - кредитима који су одобравани на дуже рокове и под условима који су тренутно неодрживи на тржишту. Овде се увек поставља питање који је начин одбране банака од појаве каматног ризика. Први случај би био да банке имају рочну усклађеност биланса, затим да банке имају валутну усклађеност биланса. Уколико пак ово није случај, постоје алтернативни али мање популарни начини одбране од каматног ризика. Један од њих свакако јесте ревизија каматних стопа у унапред утврђеним временским интервалима, како на пласмане банке, тако и на депозите банака (уговарање промене, а не фиксне каматне стопе). Други модел, који је све присутнији и на домаћем тржишту код банака које су приватизоване од стране пословних банака из иностранства, јесте да се одобравање кредита врши уз променљиву каматну стопу (ЕУРИБОР) и фиксну маргину. На овај начин, повлачењем средстава из иностранства уз исте услове ЕУРИБОР и маргина банке смањују могућност настанка каматног ризика. У домицилним условима, једини ризик који се у овим случајевима може појавити јесте ризик државе - односно промене обавезне резерве на задуживања у иностранству, чиме се и цена коштања повучених средстава значајно мења.

Тржишни ризик који може настати услед промене у ценама на тржишту, укључивши и промене девизног курса, којег свакако карактеришу осцилације, тако да су банке које обављају плаћања у форми електронског новца у страниј валути изложене ризику. Може се јавити увећање ризика девизног курса насталог због прихватања страних валута као начина плаћања. Измене у девизном курсу могу да доведу до губитака у пословању банке, и коначно до смањења прихода. Пример за овај случај ризика односи се на прихватање одређених ризика у пословању са нестабилним валутама. Случај који можемо навести из домаће пословне праксе односио би се на инвестирање банке у нпр. државне записе који имају одређену фиксну стопу приноса изражену у динарима. С обзиром на нестабилност домаће валуте (и тренутни низак курс евра), поставља се питање, шта уколико банке инвестирају одређену количину средстава у динарске записе државе и после одређеног временског периода (6 месеци до годину дана) дође до поремећаја на тржишту девиза и померања курса евра. Ово може довести до тога да пословна банка не заради ништа на оваквом виду пословања, без обзира на релативно високу номиналну каматну стопу, већ чак и да претрпи одређене губитке услед осцилација курса динара. Такође, можемо да наведено и „другу страну медаље“ која се односи на чињеницу да је у току 2006. године, курс евра значајније, чак за 10% опао. То је довело до чињенице да су банке као и друга правна и физичка лица која су уложила своју активу у динарске пласмане (обвезнице, штедњу...), оствариле не само адекватну зараду по питању камата на приносе, већ су и износи који су враћени по истеку периода на име главнице вредели у еврима више него што је то било на дан улагања.

Процену ризика потребно је организовати као перманентан процес, који се одвија у три фазе. У првој фази потребно је да банка идентификује, а по могућности и квантификује ризике. Идентификација ризика је кључна полазна претпоставка у проценама ризика, с обзиром на то да су најопаснији ризици они којих банке нису свесне, јер могу да доведу до великих и непланираних трошкова. Идентификација ризика могућа је на неколико начина, а најчешћи методи односе се на емпијска искуства досадашњег пословања банака, као и на размену искустава између самих пословних банака. Уколико није могуће квантификовати ризик, потребно је утврдити како потенцијални ризик настаје и какве су могућности да се ови ризици ограниче. Поред тога, битно је и то да се утврди учесталост, односно фреквенција појаве ризика. У другој фази одређује се могућност банке у погледу

нивоа толеранције ризика, базираној на оцени губитка који ће банка моћи да поднесе. Кључно за све банке јесте да, када постану свесне ризика с којим послују, начина његовог испољавања и фреквентности појаве, утврде процену испољавања одређеног ризика. Ова процена је изузетно битна с обзиром на то да на основу процењене вредности - односно губитка услед испољавања одређеног ризика, банка треба да дефинише превентивне и корективне мере. Приоритет свакако треба да буде дефинисање превентивних мера и елиминисање свих прелиминарних фактора који могу да доведу до настајања одређеног ризика. С тим у вези банке би требало да за сваки од утврђених ризика дефинишу који су то индикатори, односно показатељи чије би појављивање могло да укаже на настанак одређене негативне појаве, тј. ризика и да на основу тих индикатора дефинишу листу акција за отклањање истих. Корективни фактори имају само дејство на ублажавање последица насталих дејством одређеног ризика односно негативног случаја у пословању банке. У трећој фази оцењује се да ли се изложеност ризику креће у оквиру подношљивих лимита. Трећа фаза је фаза у којој би требало да се дефинише надгледање ризика уколико се он и деси. Ово се посебно односи на примену корективних мера којима би ризик, односно његов утицај треба да се минимизира.

Квалитативно управљање ризицима се углавном користи за ризике који се не могу квантификовати. Ова метода управљања ризиком се заснива на искуственим оценама банкарских експерата. У савременом банкарству тенденција је да се, када је год то могуће, користе квантитативне методе управљања ризицима. Код квантитативног сагледавања банкарских ризика, основни приступ се састоји у сагледавању просечног износа губитака, као и стопе дисперзије губитака. Прорачунавање ризика се може вршити по типовима активе, линијама банкарских производа и нивоа индивидуалних клијената. Постоје и мишљења да је најефективнији приступ у управљању ризицима онај који укључује мешавину квантитативног и квалитативног приступа, односно који би ускладио математичко моделирање са тржишним искуством. Уколико банка не би добро управљала ризицима, постоји опасност од несолвентности. Из тог разлога је тежиште управљања ризицима пренето на повезивање висине ризика са адекватним нивоом капитала, укључујући и резерве, као извора за њихово покривање. Очекивани губици се покривају из оперативних резерви за покриће губитака, док капитал банке служи као извор за покриће само неочекиваних губитака.

Након што се процене ризици и одреде нивои њихове толеранције, на менаџменту банке је да почне са управљањем ризицима и њиховој контроли. Управљање ризиком укључује активности: имплементацију сигурносних механизма и мера, координацију интерне комуникације, вредновање и побољшање производа и услуга, имплементацију мера за контролу ризика који се односе на спољне даваоце услуга и планирање непредвидивих околности.

Сигурносни механизми и мере које се примењују при управљању и контроли ризика, подразумевају комбинацију система заштитних мера, апликација и интерне контроле, који се користи да се осигура интегритет, аутентичност и поузданост података, оперативних процеса (обрада) и извештаја. Заштита је базирана на развоју и имплементацији адекватних сигурносних механизма и мера за интерне процесе. Поред тога, развијају се и имплементирају механизми и мере за комуникацију између банке и екстерних система, све у циљу смањења ризика од екстерних и интерних напада на систем електронског банкарства и електронског новца.

Сигурносне мере су комбинација хардверских и софтверских алата. Као сигурносне мере користи се: **шифровање података, дигитални сертификат, инсталација заштитних зидова, антивирусна контрола, коришћење ПИН-а**, и сл. Шифровањем података се решава проблем тајности преноса података путем рачунарских комуникационих мрежа. Шифровање је процес трансформације информација у шифроване садржаје које разуме прималац информација. Процес шифрирања укључује шифровање података, где пошиљалац поруке врши шифрирање са кључевима за шифровање и дешифровање података, где прималац поруке врши дешифровање са кључевима за дешифровање. Дигитални сертификат представља електронску потврду којом се потврђује веза између података за верификацију електронског потписа и идентитета корисника. Дигитални сертификат издају сертификациона тела. Заштитни зидови представљају комбинацију хардвера и софтвера и ограничавају екстерни приступ интерном систему прикљученом на отворену мрежу, као што је Интернет. Поруке које долазе из екстерног окружења преко заштитног зида нису апсолутно заштићене од вирусно заражених програма који доспевају преко Интернета. У ту сврху се користе антивирусни програми. Антивирусна контрола се користи са циљем да се предупреди упад и наношење

штете од стране рачунарских вируса, који представљају написане програме који узрокују штетно дејство код корисника рачунара, као што је присуство разним порукама, а затим и брисање датотека и дискова. Рачунарски вируси се обично преносе Интернет порукама, путем дискета и ЦД-а. ПИН се користи у циљу превенције од неауторизованог приступа подацима банке.

Путем њих се осигурава интегритет, аутентичност и поузданост података, оперативних процеса и извештаја. Употребом наведених сигурносних мера се врши додељивање и контрола ауторизације корисника система и апликација електронског банкарства. Они обезбеђују чување података из система, односно обезбеђују заштиту и контролу приступа. На тај начин се спречава неауторизовани приступ кључним системима електронског банкарства, базама података и апликацијама. Наведене мере служе и за минимизирање екстерних претњи за системе електронског банкарства. Наведене сигурносне мере штите од неауторизованог приступа екстерних страна као што су посетиоци, спољни сарадници или техничка лица. То значи да је потребно примењивати поступке преиспитивања сигурности за запослене, кориснике услуга, као и пружаоце екстерних услуга.

За менаџмент је од основног значаја да успостави комуникацију са запосленима у банци који су задужени за функционисање електронског банкарства (координацију интерне комуникације). Такође, неопходна је комуникација менаџмента са ИТ сектором у погледу функционисања дизајнираног система и информисања о евентуалним слабостима, са предлогом мера за њихово отклањање. За имплементацију и функционисање електронског банкарства потребан је висок ниво едукације запослених и корисника услуга банке, што за резултат има директно смањење оперативног и репутационог ризика.

Оперативни и репутациони ризик се може смањити и вредновањем производа и услуга банке пре него што се понуде на тржишту. Ово укључује: тестирање валидности опреме у складу са жељеним резултатима, израда пилот програма и прототип пројеката нових апликација и њихово тестирање, као и тестирање дизајнираног система електронског банкарства. Након извршеног тестирања и анализе резултата, врше се евентуалне корекције дизајнираног система у циљу побољшања.

Да би осигурале несметано функционисање електронског банкарства, банке ангажују спољне даваоце (информационих) услуга. То у условима електронског банкарства означава ангажовање спољних испоручиоца сигурносних пакета, односно, провајдера. Технологија електронског банкарства захтева планирање непредвидивих околости које могу довести до ризика у функционисању, било да су настали у интерним процесима или екстерним (од стране даваоца услуга). Ово планирање треба да обухвати: могућност обнове података, организовање back up система (резервни систем), подршку сервисима према корисницима услуга. Технологија електронског банкарства ослања се на екстерне ентитете, као што су: испоручиоци харвера, софтвера, телекомуникационе компаније и Интернет провајдере. Неопходно је да и они имају организоване back up – ове система.

6. ПРОБЛЕМИ СИГУРНОСТИ И МЕРЕ ЗАШТИТЕ

У конкретним пројектима обезбеђења адекватног нивоа сигурности битна су два момента:

1. **Процена конкретног ризика и**
2. **Проналажење конкретне трошковно-ефикасне солуције.**

Природа поруке која се преноси треба да оправда трошкове који ће бити начињени за њено обезбеђење. У условима електронског преноса, сигурност система односи се на сигурност преноса и сигурност пријема, аналогно сигурности електронске размене података уопште. Основни захтев преноса у овом контексту је обезбеђење расположивости и поузданости мреже. Емитент иницијатор мора бити овлашћен и не би требало да буде у могућности да демантује (порекне) слање поруке, порука мора стићи на праву адресу без модификације, а прималац порука не би имао право и могућност да демантује извршен пријем. Конкретни ризици ове врсте који могу настати су:

1. **Губитак услуге коришћења мреже;**
2. **Модификација садржаја, порекла и дестинације поруке (услед грешке, преваре и сл.);**
3. **Губитак поруке, одрицање (демантовање) поруке од иницијатора или примаоца;**
4. **Недозвољено обелодањивање њеног садржаја,**
5. **Илегалне употребе рачунарских система или мреже за пренос.**

У циљу елиминисања ових ризика развијају се посебне функције сигурности: расположивост мреже – подразумева обезбеђење доступности мреже за коришћење одређеном ентитету, интегритет поруке – подразумева спречавање мењања или уништења поруке недозвољеним руковањем, непорецивост – мера дизајнирања заштите од накнадног демантовања од стране ентитета који су укључени у комуникацију учешћем у делимичној или целокупној комуникацији, поверљивост података – спречавање могућности да подаци буду доступни и на располагању неовлашћеним појединцима, ентитетима или процесима, потврда – мера обезбеђења од накнадне злоупотребе пренете поруке кроз потврђивање валидности преноса, стационирања и порекла, контрола приступа – ограничавање права

или могућности субјекта да недозвољено комуницира са другим субјектима, или употребљавају функције и услуге у систему или мрежи.

Програм сигурности може бити постављен на различитим техничким решењима, мора да буде спроведен на свим поднивоима који представљају област повредивости:

- 1. Ниво терминала,**
- 2. Ниво рачунара и комуникационих веза и**
- 3. Ниво обезбеђења функционалности целокупног система.**

Проблем обезбеђења сигурности терминала и идентификације клијента своди се на уклањање две врсте ризика:

- 1. Ризика од злоупотребе трећих лица и**
- 2. Ризика злоупотребе од самог клијената/корисника услуге.**

У првом случају ради се о проблему спречавања недозвољеног уласка трећих лица у систем, а у другом о спречавању злоупотребе самих средстава улаза клијената. Проблеми идентификације клијената који имају дозвољен приступ и његово коришћење за одређене, дозвољене намене повећава се са порастом броја и врсте терминала, а конкретна решења доста зависе од природе веза са рачунарским центром.

Идентификација појединачних учесника, корисника одређених система је посебно значајна због тога што су појединци као индивидуални корисници електронских система плаћања веома бројни, мада су износи њихових плаћања релативно мали. У складу са тим, средство улаза које они користе треба да буде, погодно за ношење и употребу, да поседује висок степен заштите од злоупотребе и релативно јефтино. Пракса је показала да ће такву функцију моћи да обављају већ поменуте трансакцијске финансијске картице. У овом домену проблеми настају због могућности коришћења туђих изгубљених, или украдених картица.

Сложеност спречавања злоупотреба ове врсте показује искуство САД које спадају у највеће кориснике електронских картица у свету. Контрола приступа на терминалима обезбеђује се увођењем лозинке, електронских сигнала (симбола) и биометријским средствима. Кључно средство које је коришћено за заштиту у овом домену је увођење тзв.

ПИН-а који се уграђује на магнетну траку или чип, а састоји се од неколико дигиталних знакова или алгоритама. Проблеми су се у пракси јављали у случајевима када су трећа лица откривањем ПИН-а туђих украдених или изгубљених картица успевала да уђу у систем. Сама могућност овакве злоупотребе у великој мери је зависила од самог техничког решења писања и коришћења ПИН-а.

За посебно осетљиве трансакције или за велике новчане трансфере примењује се додатни систем заштите – ТАН. ТАН представља низ случајних бројева које генерише банка и даје их кориснику картице. Корисник када жели да обави трансфер новца или плаћање попуњава број картице, затим уноси ПИН и на крају уноси ТАН. ТАН је број за једнократну употребу, за само једну трансакцију и не може се више користити.

Алтернативе за ПИН познате су као биометријске методе, због тога што се заснивају на мерењу и верификовању јединствених физичких карактеристика појединаца. До сада је познато пет метода биометријске идентификације: верификација потписа, геометрија шаке, поређење отисака прста и длана, мерење отисака слуха и снимање очне зенице, а појављује се и идеја о шестом - узорак крви. Идентификација лица које користи картицу врши се веома једноставно. Приликом издавања картице, потребне биометријске информације се меморишу у систем и са њима се врши поређење одређених биометријских карактеристика лица које користи картицу. Практични проблеми за њихову примену настају због тога, што је за идентификацију корисника потребан велики обим података, тако да њихова употреба претпоставља коришћење картице са чипом и комплексност уређаја за читање. Поред тога, из разних разлога (нпр. болести) код биометријских карактеристика може доћи до промена. По својој природи, а у зависности од биометријске методе, бројни неуспели покушаји идентификација могу довести до незадовољства корисника. Највећи проблем је што су биометријски подаци неизоставно јавни и што могу бити употребљени иако стварни власник није физички присутан. Једном када је биометријски запис направљен у дигиталном облику може бити копиран и коришћен врло лако за обману. Једном компромитована биометрија не може се изменити. Ово је мањи проблем код затворених мрежа или појединачних система, али за удаљену идентификацију преко Интернета постаје озбиљан проблем. Индустрија која се бави биометријским методама препоручује стандардан сет принципа за очување приватности.

То је редовно шифровање биометријских података пре било каквог слања и строга контрола дистрибуције података.

Када се ради о проблему елиминисања ризика од неадекватног коришћења финансијских трансакцијских картица од стране самог власника, онда се поставља питање уклапања њихових техничких карактеристика са банкарским принципима пословања. Како оне у основи представљају само технику, њихова имплементација може да се усклађује са различитим конкретним финансијским аранжманима које банка изграђује са својим клијентима (коришћење средстава са одређених рачуна, кредитне линије до одређеног износа и сл.). Конкретну солуцију, банка би требало да бира у складу са проценом бонитета сваког појединачног клијента и одмеравања властите политике сигурности.

Слабијим клијентима могло би се вршити максимирање износа по појединачној употреби преко механизма дозвољеног оптерећења финансијске трансакционе карте. Клијентима просечног бонитета могао би се одредити максимални број коришћења (или износа) преко којих клијент више не би могао да користи картицу, док би клијентима изузетног бонитета могао бити дозвољен аутоматизам у коришћењу без икаквих посебних ограничења.

Проблем функционисања рачунарског система као целине односи се на неопходност, да систем као целина перманентно и исправно функционише у техничком смислу. Овај проблем добија посебно на значају, због тога што се тешкоће у раду једног центра преносе на рад осталих делова система и могу изазвати блокаду целокупног система. У пракси су познати проблеми изазвани овим разлозима. Електронски банкарски систем у САД-у је 2003. године претрпео велики ударац ове врсте, у трајању од неколико часова, када се појавио вирус који се ширио великом брзином са рачунара на рачунар, услед чега је дошло до прекида у неколико глобалних информационих мрежа. Хиљаде мејлова је сатима каснило, а услуге на мрежама АТМ-ова неколико водећих банака САД-а и Канаде биле су угрожене. У конкретном случају, систем је враћен у функционисање у току истог дана, озбиљним напорима банака.

Ниво заштите података код размене електронских порука изузетно је значајан елемент на основу којег се корисници опредељују за или против примене е-трансакција. То је посебно карактеристично у случајевима када губитак, измена, неовлашћени увид или неке друге

претње електронским документима могу да изазову значајне правне и финансијске последице по учеснику у онлине трансакцији. Наиме, у е-пословању и размени електронских докумената учествују бројни партнери и сви морају да имају одговарајући ниво заштите. Под заштитом података подразумева се намера да подаци остану познати само пошиљаоцу и примаоцу, и тако да једино они могу да их користе. Могућност увида трећих лица може да доведе до злоупотребе одређених података, а то може да изазове негативне последице по учеснике у размени. Подаци могу да се поделе на следеће четири групе: јавни подаци – подаци у које сви могу да имају увид; ауторизовани подаци – подаци у које сви имају увид, али су од неауторизованог коришћења заштићени ауторским правом; поверљиви подаци – подаци који су тајни (чији садржај не сме да буде читљив неовлашћеним лицима).

За заштиту поверљивих и тајних података користе се многе методе и технике. Ако се подаци шаљу неким средством комуникације, примењују се технике које су развијене у **криптологији**. Када се подаци чувају или примају на одређеном месту, обезбеђују се применом техника персоналне идентификације. За заштиту информационих система од негативних утицаја са Интернета обично се користи гранични сервер, антивирусни софтвери и сл.

Постоји много разлога због којих се тешко могу проценити стварне димензије сајбер – криминала, а бројне случајеве компаније и не пријављују зато што страхују од губитка поверења потенцијалних корисника и потрошача. Али, и у случајевима када је криминална радња пријављена властима, често се тешко може проценити ниво губитка. Мотиви свих сајбер – криминалних радњи нису везани за новац – неки напади су срачунати само на то да униште или онеспособе веб страну. Губици у таквим случајевима не чине само средства која су потребна за обнављање своје веб стране већ и губитак репутације и имица сајта, као и прихода који би се остварио у периоду док сајт није радио.

Може се закључити да је **сајбер – криминал** усмерен на е-трговинске сајтове у порасту, да је реч о штети која се тешко може тачно проценити и да се очекује њен даљи раст. С обзиром на ниво губитка компанија насталих због сајбер – криминалних радњи, развој и примена добро осмишљене политике заштите постаје приоритетан задатак и потреба. Смањивање ризика у електронском пословању комплексан је поступак, који обухвата нове

технологије, организационе политике и процедуре, нове законе и индустријске стандарде на основу којих ће се дати овлашћења надлежним органима да гоне и кажњавају починиоце сајбер – криминалних радњи. Међутим, потпуна сигурност не постоји. Сваки сигурносни систем може да буде „проваљен“, уколико се у остварење такве намере уложи довољна средства. Али, трајна сигурност у информатићкој ери није ни потребна. Подаци обично имају вредност у одређеном временском периоду, тако да се према потреби заштите један дан, или месец, или годину. Ниво сигурности повезан је са сагледавањем два односа:

1. **Однос нивоа сигурности и лакоће употребе сајта** је дивергентан. Бројне мере сигурности које се додају е-трговинском сајту чине да сајт постаје спорији и тежи за коришћење. Тако превелика сигурност може да нашкоди профитабилности, док недовољан ниво сигурности, с друге стране, може власника да избаци из посла;
2. Такође, постоји дивергентан однос између **настојања појединаца да обезбеде своју сигурност и сакрију свој идентитет и потребе да се обезбеди одговарајући ниво јавне сигурности**, коју могу да угрозе криминалци и терористи.

Да би се разумели различити системи заштите на појединим нивоима заштите, неопходно је да се знају најчешћи облици претњи и нарушавања сигурности у електронском пословању. То су: злонамерни код – ову групу штетних утицаја чине вируси, црви, „тројански коњи“ и „бад аплетс“ који су претња интегритету система и његовој континуираној оперативности. Њихово деловање, донекле различито, углавном се испољава у промени начина рада система, или промени докумената креираних у оквиру система. Вируси су рачунарски програми који имају способност да се умножавају, да праве сопствену копију и да се шире на друге фајлове. Највећу категорију (75-80%) чине макровируси, који нападају само апликације за које су креирани на пример, затим вируси који најчешће нападају извршне и скрипт вируси, написани у скрипт програмским језицима. Осим што се шире из фајла у фајл, црви су дизајнирани тако да се шире са рачунара на рачунар.

Хакер се дефинише као појединац који жели да оствари неовлашћени приступ рачунарском систему. Некада се задовољавају тиме што продру у фајлове е-трговинског сајта, али има случајева када им је намера везана за тзв. сајбервандализам, што

подразумева прекидање, промену или уништавање сајта. У оквиру хакерске заједнице, крекерима се називају хакери који предузимају криминалне активности. Током времена, активности хакера се мењају и шире, па се, осим на упад у систем, оријентишу и на крађу информација и робе, као и на уништавање система.

Злоупотреба кредитних картица/крађа је најчешћа појава и један од главних разлога због којег више потрошача не учествује у електронској трговини. Најчешћи случај је изгубљена или украдена картица коју користи неко други, као и крађа бројева кредитних картица ради даље злоупотребе и лажног представљања идентитета власника картице. У електронској трговини највећа претња купцима је да ће продавачев сервер изгубити податке о кредитним картицама који су на њему депоновани, или ће дозволити да се користе у криминалне сврхе. Осим тога, е-трговински сајтови су одличан извор персоналних података купаца (име, адреса, број телефона), који могу да се злоупотребе.

Хакери некад покушавају да прикрију свој прави идентитет, или се лажно представљају на основу лажне (туђе) е-маил адресе. Ово може да значи и преусмеравање веб линка на адресу другачију од намеравања, при чему се лажна адреса приказује као да је права (лажни сајт је идентичан правом). На тај начин хакери могу да преузимају поруџбине и краду посао правом сајту. Уколико им је намера да нанесу штету, могу да измене оригиналну поруџбину и затим да је пошаљу на први сајт, а резултат је незадовољан купац, који добија оно што није поручио, тако да се обично не враћа наведеном сајту. На тај начин, осим интегритета, нарушава се и принцип аутентичности, јер отежава утврђивање идентитета праве личности која шаље поруку.

Хакери некад оптерете веб сајт некорисним порукама (саобраћајем) да би оптеретили мрежу, што често изазива затварање мреже и наноси штету репутацији сајта и односима са потрошачима.

„Њушкање“ је тип програма за прислушкивање који прате информације које се крећу по мрежи и омогућавају хакерима да украду поверљиве информације са било које локације на мрежи, укључујући е-маил поруке, фајлове компаније и поверљиве извештаје. „Њушкање“ је у ствари, претња да ће поверљиве информације бити јавно презентоване.

Иако је највећа претња од спољних напада, постоји и значајна опасност да запослени, изнутра, неовлашћено користе податке и информације које су им доступне.

Најосетљивије тачке на којима треба поставити заштитне механизме, са технолошког гледишта, јесу следећи нивои заштите:

- 1. Заштита на нивоу телекомуникационе мреже,**
- 2. Заштита на апликативном нивоу и**
- 3. Заштита на нивоу поруке.**

7. ЕЛЕКТРОНСКО БАНКАРСТВО У СРБИЈИ

Када се оцењује стање е-банкарства у Србији, значајно је упоређивање са ситуацијом у овој области са развијеним земљама, са једне стране и са стањем у другим областима у земљи, са друге стране. У економски развијеним земљама проценат учешћа е-банкарства у платном промету је веома висок (нпр. у Француској 70 и 80%), док је у Србији знатно нижи, посебно када су у питању физичка лица, али са тенденцијом убрзаног развоја. Да би Србија достигла економски развијене земље, неопходно је да се у електронски систем пословања укључи што већи број фирми, све државне институције, трговине и грађани. У односу на друге сегменте у земљи, е-банкарство је релативно добро развијено и што је још значајније, показује тенденцију даљег интензивног развоја. Некада је Србија била у великом заостатку за оваквим начином пословања, али данас то више није тако. У „поплави“ банака, данас у Србији, квалитет е-банкинга који нека банка пружа, је један од фактора који одлучује којој ће се банци клијент приклонити.

Сматра се да су корени релативно добре основе за развој е-банкарства постављени у ранијој технолошкој и организационој инфраструктури Завода за обрачун и плаћања (ЗОП-а), као и у стеченим навикама коришћења неких сервиса ЗОП-а за пословне банке и предузећа. Интегрисани систем банака наспрам НБС и самих корисника, тренутно функционише путем неколико веза са централном банком. Основна веза се односи на платни промет (све банке су повезане у реалном времену, тј. имају могућност да у сваком моменту процесирају захтеве за извршавање платног налога). Друга битна веза се односи на платни промет у ширем смислу, односно пренос новца и хартија од вредности у купопродајним трансакцијама преко Централног регистра.

Значајније унапређење постојећих и увођење нових финансијских сервиса у е-банкарство Србије, везано је за промене у макроекономском амбијенту које су се одиграле у претходним годинама. Усвајање новог Закона о платном промету 1. јануара 2003. године, једним делом имало је за циљ замену постојећег монополског система плаћања тржишним системом, а другим делом стварање институционалних услова за развој електронског банкарства. Његов утицај на развој е-банкарства произилази, како из директних ефеката на сам систем плаћања, тако и из стварања предуслова за радикалну трансформацију модела

пословања банака и њихових клијената. Главни проблем је што постојећа информациона – комуникациона инфраструктура није на задовољавајућем нивоу. Циљ је да се оствари међусобна електронска повезаност свих учесника у електронским трансакцијама и да банке прошире асортиман услуга које нуде електронским путем. Преласком платног промета у пословне банке и гашењем ЗОП-а у јануару 2003. године, створени су сви услови да домаће банке понуде нешто ново нашем тржишту. То су биле безготовинске трансакције (вирманска плаћања) путем Интернета. У то време на територији Србије су постојале само три компаније које су обезбеђивале софтвер за е-банкинг и уједно представљале сертификациона тела. Ни данас их нема много више – тек шест регистрованих у земљи. Крајем 2003. године, пошто је сервисирао правни сектор, банке у Србији су биле спремне за још један велики скок – е-банкинг за физичка лица. Четири године касније, банке промовишу да је проценат укупног платног промета електронским путем чак 65%.

Трансформацијом платног система и преласком платног промета у банке отворена је нова област пословања банака – рад са клијентима електронским путем, који се популарно назива е-банкинг. Банкарство је постало лидер у области електронског пословања у Србији. Развој електронског банкарства неопходан је услов за опстанак банака на финансијском тржишту. Све већи број грађана плаћа рачуне и проверава девизни курс путем Интернета, или мобилног телефона. Овакав начин пословања брзо су прихватиле готово све банке, а неке постижу и да чак 50% укупног броја налога долази до банке електронским путем. По обиму пословања у овој области не заостајемо за земљама у региону. Према неким оценама, нисмо далеко од Румуна, Македонаца и Бугара, а за разлику од Хрвата и Словенаца, код нас је брже обављен прелазак платног промета из ЗОП-а у банке. Веома је важно образовање што већег броја грађана да користе рачунар и да се упознају са ИТ технологијама.

Електронско пословање и његова аутоматизација присутна у нашим банкама је на веома напредним технолошким основама. Домаћа софтверска решења су често ефикаснија, интегрисанија и савременија него инострана. Проблем представља уклапање у европске стандарде и прописе који се разликују од наших, али на том приближавању банкарски свакодневно раде. Домаће софтверске компаније брзо и успешно имплементирају сва

решења из области банкарске технологије. Са увођењем нових регулационих тела, институција и критеријума, Србија се постепено интегрише у савремене светске токове пословања. У електронском банкарству, Србија не заостаје за земљама у региону, али у оквиру других облика електронског пословања, е-трговине, или Б2Б пословања, још је на почетку.

Банке су се успешно укључиле у нове системе међубанкарских обрачуна по светским принципима: РТГС за приоритетна плаћања и плаћања великих вредности и нето систем за мала плаћања. Организовале су преузимање жиро рачуна предузећа и обављање послова платног промета, пружајући виши ниво и квалитет услуга, уз афирмацију концепта „у сусрет клијенту“. Постојеће основне информационе системе сада надограђују са новим слојем апликација за подршку електронском пословању са привредом и становништвом. Тренутна ИТ инфраструктура није неразвијена. Већина банака „засипа“ своје тренутне и потенцијалне кориснике рекламама у којима су баш они лидери на пољу е-банкарства, при чему свака потенцира своје најбоље решење за е-банкарство. Тенденције иду ка томе да у будућности сви субјекти буду електронски повезани, да банке проширују асортиман услуга које пружају електронским путем уз оптималну динамику промена. Општа конкуренција подстиче појединачне банке у настојању да понуде што више погодности за своје клијенте.

Веома је изражена подршка владиних програма у области платних картица (картичарство). Влада има директан интерес да пружа ову подршку, због тога што свака оваква трансакција представља легалан ток готовине који са собом носи фискални рачун и наплату пореза. Асортиман понуде е-банкарства се драстично шири у кратком временском периоду. Банке својим клијентима омогућавају: увид у стање рачуна, преглед промета, преглед извода промена на рачуну, пријем и слање личних порука, плаћање обавеза платним налозима са текућим датумима и датумима унапред. Појављују се могућности коришћења услуга платног промета путем банкомата, платних картица, ПОС терминала банака, Call Центра и мобилних телефона (СМС).

Суштина нуђења сервиса е-банкарства (посебно када су у питању грађани) јесте да се њима обезбеди доступност преко целог дана, без посете банци и ограничења радног времена. Велике фирме су у већем броју корисници услуга е-банкарства, што је добрим

делом резултат стечених искустава коришћењем „удаљеног улаза“ преко терминала из својих пословних просторија кад су радиле преко ЗОП-а. За мале фирме е-банкарство постаје све атрактивније, јер баш зато што су мале оне могу низ послова да обављају не напуштајући своје радне просторије, а имају непрекидно увид у стање свог рачуна.

Банке ће у наредном периоду улагати много више у промоцију електронског банкарства у раду са становништвом. Наши грађани су већ прихватили системе електронског плаћања јер штеди време, доступан је 24 часа са било ког места или уређаја, а становништво радо прихвата све што олакшава свакодневни живот. Грађане је ипак потребно образовати у примени електронског банкарства, што ће допринети популарности е-банкинга, а уз снижавање тарифе електронских трансакција у односу на шалтерске трансакције учиниће се да он постане преовлађујући начин плаћања грађана. Треба да тежимо да будемо лидери у овој области и да се поредимо са савременим светом, јер је ту простор за напредовање огроман.

Иако су многи људи у Србији и даље изузетно скептични када је у питању сигурност при коришћењу електронског банкарства, за шест година, колико се овај систем користи у нашој земљи, није забележен ни један случај преваре. Неопходно је, ипак, образовати кориснике, напомињу банкарски, како се не би десило да лако упадну у хакерске замке којих ће у будућности неминовно бити. Паралелно са експанзијом употребе електронске банке „развила“ се и могућност превара у овом домену пословања. Банке у Србији су са одређеним кашњењем стартовале са понудом ове врсте сервиса, али су то искористиле као предност и поучене искуством банака са Запада, увеле прилично сигурне системе заштите за сервисе електронске банке. У Србији су тренутно у примени методе корисничке аутентификације и трансакционе ауторизације при коришћењу електронске банке, којима је у старту спречена могућност преваре.

Најраспрострањенија и скоро стопостотна заштита је ССЛ протокол, који обезбеђује шифрован пренос података, како корисника тако и сервера. И поред тога број људи у Србији који користе предности електронског банкарства, попут детаљног увида у сопствени банковни рачун и могућност плаћања рачуна преко Интернета, још увек је мали. Експанзија плаћања путем електронског банкарства тек се очекује. Прихватањем праксе е-

пословања, Србија мора да искористи нове економске могућности које се отварају са циљем да:

- 1. Промовише привредни раст и социјални развој,**
- 2. Унапреди пословну ефикасност и продуктивност,**
- 3. Смањи трошкове пословања,**
- 4. Омогући домаћим компанијама лакшу реинтеграцију у европско и светско тржиште.**

Применом е-банкинга у различитим секторима националне привреде повећава се повезаност и међузависност рачунарских мрежа приватних и јавних организација укључених у домаће и међународне економске активности. На овај начин, национална привреда се креће из фазе интерактивног деловања аутономних субјеката ка фази интегрисаног система за управљање информационим токовима у привреди, што јој даје карактеристике е-економије, или друштва заснованог на информацијама (информационог друштва). У савременој ери глобалног развоја светске привреде и друштва, е-пословање постаје покретач светског привредног пораста. Изостанак примене е-пословања води ограничавању развоја националне привреде.

Почетком јануара 2003. године реализован је један од највећих системских пројеката у Србији. Платни промет је из Завода за обрачун и плаћања пренет у пословне банке. Нови систем платног промета у целини испуњава свих десет основних принципа пословања, које је установила Банка за међународна поравнања (БИС). Електронски платни промет у Србији се обавља разменом електронских порука кроз информационе системе учесника у трансакцији плаћања. Електронска порука је информација, која је електронски генерисана, проверена, послата, примљена и сачувана електронски. Електронски пренос новчаних средстава између учесника у платном промету, сматра се електронском платном трансакцијом. Електронски налог за плаћање мора да садржи елементе утврђене одлуком којом се уређују облик, садржина и начин коришћења јединствених инструмената платног промета, као и елементе за проверу аутентичности и тачности тих налога и аутентичности њихових подносилаца.

Електронски системи плаћања и њихова заштита

У електронском платном промету између Народне банке Србије и банака које учествују у међубанкарском обрачуну, НБС обезбеђује електронску размену података и њихову заштиту. Народна банка Србије, услуге електронског платног промета врши преко информатичке инфраструктуре за обављање платног промета Републике Србије. Електронска платна трансакција сматра се окончаном кад крајњи субјект прими електронску поруку. Електронска порука се сматра примљеном када пошиљалац прими потврду о њеном пријему. Валидна електронска порука је свака електронска порука прописаног формата, која је оверена електронским потписом и примљена, за коју се утврди да садржи податке који нису мењани од тренутка слања те поруке – ако је њен пошиљалац регистровани учесник у електронском платном промету, односно овлашћено лице тог учесника. Учесник у електронском платном промету, обавезе преузима на основу валидне електронске поруке, односно на основу њене измене или опозива.

Домаћи платни промет обухвата:

1. **Међубанкарски платни промет** – који се обавља између учесника у РТГС и клиринг систему НБС и
2. **Интерни платни промет** – који се обавља између клијената који имају отворене рачуне код исте банке.

Обрачун у реалном времену по бруто принципу (РТГС) обавља Народна банка Србије – за учеснике у РТГС систему. Учесници у РТГС систему су:

1. **Народна банка Србије,**
2. **Банка која поседује дозволу за рад Народне банке Србије** и уписана је у судски регистар,
3. **Република Србија** (министарство надлежно за послове финансија, учествује преко консолидованог рачуна трезора који се води код Народне банке Србије),
4. **Централни регистар, депо и клиринг хартија од вредности,**
5. **Удружење банака Србије.**

РТГС систем (обрачун у реалном времену по бруто принципу) подразумева пријем и извршавање појединачних налога у најкраћем могућем времену од момента њиховог пријема и то до висине покрића на рачуну. У РТГС-у се могу извршавати сви налози за

плаћање, с тим што се обавезно извршавају налози за плаћање који гласе на износе веће од 200.000 динара („велика плаћања“), а што је утврђено оперативним правилима за РТГС и клиринг. Наведена плаћања реализују се у реалном времену, порукама SWIFT формата (клијент једне банке – клијенту друге банке) и (банка - банци). Реализацијом РТГА трансакције у реалном времену се мења стање на рачуну банке, односно другог учесника РТГС и клиринг система.

Под клирингом, односно нето обрачуном, подразумева се пријем појединачних налога за плаћање, или група налога за плаћање, уз које се доставља спецификација појединачних налога, ради обрачуна мултилатералних нето износа на обрачунским рачунима. Након тога, за сваког учесника у клирингу се утврђује нето позиција, чије се поравнање врши преко његовог жиро рачуна. Плаћања у клирингу („мала плаћања“) су налози чији је износ до 200.000 динара и „пакују“ се у поруке SWIFT формата. У једној поруци може бити до 100 налога за плаћање. Плаћања у клирингу извршавају се у процесу нето поравнања у три клириншка циклуса сваког радног дана (у 11.00, 13.30 и 16.15 часова). Учесници у РТГС и клиринг систему НБС повезани су у јединствену целину у којој се платне трансакције размењују порукама, заснованим на SWIFT стандарду, кроз приватну комуникациону мрежу НБС. НБС је оператор и власник РТГС и клиринг система, конфигурисаних као један систем, на једној платформи. Систем је флексибилан у смислу постојања могућности раздвајања РТГС-а и клиринга на одвојене системе, на две платформе. НБС је од јануара 2005. године учесницима понудила нови сервис – извршавање „малих, клириншких плаћања“ у РТГС систему, по Тарифи за клириншка плаћања. То је омогућило банкама са бољом ликвидносном позицијом да извршавају плаћања путем РТГС система, не чекајући клириншки циклус, а по нижој Тарифи. Сервис је доживео успех и широко је прихваћен од стране учесника у систему. Илустративан је податак да је током првог месеца удео наведених плаћања у укупним плаћањима износио 7%, да би га временом све већи број банака почео користити, тако да је 2008. године учешће ових плаћања у укупном броју трансакција износило 56,82%. То је, наравно, утицало и на учешће клириншких плаћања у укупном броју плаћања које је са 51,92%, колико је износило у 2007. години, пало на 43,18% у 2008. години.

Електронски системи плаћања и њихова заштита

Мрежа НБС покрива територију Републике Србије. Као преносни путеви се користе ресурси домаћег телекомуникационог провајдера. На територији Републике Србије се налазе четири мрежна чвора која нуде различите технологије приступа. Пословне банке се укључују у мрежу НБС посредством најближег мрежног чворишта. У мрежи се користи комуникациони протокол. Подаци у платном промету се шифрују, а затим транспортују кроз мрежу. Поруке којима се извршавају плаћања у РТГС систему су SWIFT поруке. Одмах после извршења трансакције, систем упућује пошиљаоцу одговарајућу поруку о извршеном обрачуну, након чега се трансакција сматра коначном. Учесници електронског платног промета дужни су да електронску поруку чувају најмање 5 година после истека године у којој је извршена електронска платна трансакција, као и податке и средства за верификацију аутентичности те поруке.

За проверу аутентичности електронских порука и исправности преноса тих порука кроз мрежу НБС, користи се технологија јавних кључева. НБС врши сертификацију јавних кључева и учесници своје јавне и тајне кључеве генеришу софтвером који им обезбеђује НБС. Банке и њихови клијенти уговором уређују начин и услове међусобне размене електронских порука. НБС је донела Одлуку о електронском начину обављања платног промета, а донет је и Закон о електронском потпису и Закон о електронском документу.

Архитектуру информационог система платног система НБС чине:

1. **Централни рачунар**
2. **Рачунар за развој**
3. **Рачунар за подршку**, чије је коришћење предвиђено за ванредне ситуације (елементарне непогоде и сл.).

Платни систем, са становишта логичке и функционалне организације, чине четири целине:

1. **Продукциони сајт**
2. **Hot backup Site**
3. **Remote backup Site**
4. **Test Site**

На оваквој функционалној архиктетури НБС заснива Business Continuity план платног система, у којем су дефинисане процедуре које, заједно са имплементираним технологијама, обезбеђују да критични радни процеси остану расположиви, или да се веома брзо врате у функцију, у случајевима поремећаја који узрокују нерасположивост дела информационе инфраструктуре или целог рачунског центра (ванредне околности, као што су природне катастрофе и сл.).

ЗАКЉУЧАК

Развој е-банкарства везан је за све ширу примену рачунарске и телекомуникационе технологије у процесу обраде и преноса података и информација. Ове технологије доводе до крупних промена у функционисању банака. Покренути процеси доводе до увођења нових поступака и технологија, које собом носе нове изазове и могућности. Техничко - финансијске иновације, са своје стране, воде интензивирању конкуренције у свим сегментима. Долази, не само до реинжењеринга пословних процеса у банкама, већ и до реинжењеринга у пословним процесима и односима између самих банака, банака и њихових клијената и између клијената и трећих лица међусобно. Класично банкарско пословање и лични сусрет са клијентима све се више замењују аутоматизованом производњом и испоруком услуга. Трошкови великих трансакција се смањују, а банкарске и финансијске услуге деперсонализују.

Услед убрзаног ширења електронских банкарских система долази до великих преокрета у суштини самог е-банкарства, које све више постаје синоним модерног банкарства. Данас банкарско пословање у потпуности почива на техничко - технолошким ресурсима, а информационо комуникационе технологије постају водич за стратегију и реинжењеринг. Тренд модерног банкарства је аутоматизација свих функција (финансијских операција) применом рачунарских технологија. Примарни циљ увођења система електронских плаћања је решавање проблема система плаћања заснованих на папиру, коришћењем потенцијалних предности примене информационе технологије. Појава електронског новца наметнула је потпуно нову филозофију у банкарству која се заснива на електронској размени података и средстава, која је појмовно одређена као електронско банкарство.

Главни циљ е-банкарства је да се без обзира на географску удаљеност што брже и ефикасније повежу клијенти и токови информација. Тајна успешног савременог информационог система је флексибилна инфраструктура базирана на персоналним рачунарима, модерним рачунским мрежама и Интернету пре свега. Развој информационе и телекомуникационе технологије створио је услове за глобализацију пословања банака тј. до увођења нових канала дистрибуције банкарских услуга, односно електронског

банкарства. Примена електронског банкарства на националном, регионалном и на глобалном нивоу, промовише се у неопходан процес експанзије банкарског система.

У овом раду су обрађени електронски системи плаћања са свим својим предностима и манама и дат је посебан осврт на Србију. Након оваквог разматрања општи закључак је да Србија у погледу технолошких средстава који се користе не заостаје много, али да и даље треба доста радити на едукацији становништва како би приступили оваквом начину пословања.

ЛИТЕРАТУРА

1. Вуксановић Е., *Електронски системи плаћања*, Универзитет у Крагујевцу, Економски факултет, 2009.
2. Вуксановић Е., *Механизми и инструменти плаћања у условима електронског преноса средстава*, SAM Konsalting, Београд, 1994.
3. Марић С., Новаковић И., *Електронско пословање*, Кварк Краљево, 2006.
4. Станкић Р., *Електронско пословање*, Економски факултет Београд, 2007.
5. Tan M., *E – payment, The Digital Exchange, Rigde Books*, 2006.
6. www.poslovnimagazin.biz/magazin/srbija прегледано: јун, 2014.
7. http://www.ef.uns.ac.rs/Download/informacioni_sistemi_u_finansijama_bankarstvu_i_osi_guranju/2012-12-12%20-%20Skripta%203%20-%20e-Banking.pdf прегледано: јун, 2014.
8. www.bankerinter.net прегледано: јун 2014.