



336.7:004.738.5]:005(470)
336.7:004.738.5]:005(497.7)

M.Gogova Samonikov, E. Veselinova

Goce Delcev University, Faculty of Economics, Krste Misirkov St., 10-A, Republic of
Macedonia, e-mail: marija.gogova@ugd.edu.mk

Goce Delcev University, Faculty of Economics, Krste Misirkov St., 10-A, Republic of
Macedonia, e-mail: elena.veselinova@ugd.edu.mk

МЕНАЦИРАЊЕТО СО Е-ФИНАНСИИТЕ КАКО ПРЕДИЗВИК ПРЕД МАКЕДОНСКАТА И РУСКАТА ЕКОНОМИЈА

Апстракт: Финансискиот систем постои како посебен дел составен од институции и инструменти чиешто функционирање се одвива на финансиските пазар. Тековно постојат и светски процеси кои се надвор од финансискиот систем, ама се условени или влијаат на него. Токму тие процеси влијаат на финансискиот систем. Финансиското опкружување влијае на конкурентската способност на финансиските институции, предизвикува создавање или развивање на современи пристапи. Овие современи пристапи на финансиските институции предизвикуваат одредена еволуција во функционирањето на финансискиот пазар.

Посебно развојот на информатичката технологија предизвикува сè поголемо учество на електронското тргување од една страна, а од друга страна предизвикува и постоење на нови методи во работењето на финансиските институции. Со овие современи методи институцијата цели кон: приближување кон потрошувачот, прв (побрз) пристап до потрошувачот и лидерство на пазарот.

Горенаведеното е предизвик пред која било економија и овој труд дава одговор до каде се и како треба да се развиваат руската и македонската економија во однос на електронското работење во финансискиот сектор. За таа цел се користени методи на анализа, синтеза, обработка на податоци кои квантитавно се поткрепени.

Клучни зборови: *е-финансии, финансиски пазари, финансиски иновации, менаџирање на е-финансии, македонска и руска економија.*

MANAGING E-FINANCE AS A CHALLENGE TO THE MACEDONIAN AND RUSSIAN ECONOMY

Abstract: The financial system exists as a separate part made up of institutions and instruments whose operation is taking place in the financial market. Currently there are mundane processes that are beyond the financial system, but are conditioned or sustain it. It is that these processes affect the financial system. Financial environment influences the competitiveness of financial institutions, causing the creation or development of modern approaches. These modern approaches to financial institutions caused a certain evolution in the functioning of financial markets.

Especially the development of information technology is a growing share of electronic commerce on the one hand and on the other hand causes the existence of new methods of operations of financial institutions. These modern methods institution aims to: approaching of first (faster) access to consumer and market leadership.

Above stated challenges for any economy, this paper provides an answer to where and how to develop the Russian and Macedonian economy in terms of e-banking in the financial sector. For this purpose were used methods of analysis, synthesis, processing quantitative data etc.

Key words: *e-finance, financial markets, financial innovation, management of e-finance, Macedonian and Russian economy.*

1. Предуслови за употреба на електронски трансакции

Русија е шесторангирана земја со 102,258,256 корисници на Интернет, тоа е 71.3% од вкупното население, што ја позиционира на ранг од 67. место. Република Македонија е 113. рангирана земја по број на жители кои користат Интернет. 1,277,349 македонски жители имаат



пристап до Интернет. 61.20% е податок кој оваа земја ја рангира како 68-ма во однос на процентот на лица кои користат Интернет од вкупниот број на жители.

Овие податоци укажуваат дека Република Македонија и Русија се една зад друга во рангирањето на земјите според процентот на население кое користи Интернет во споредба со вкупниот број на жители. Тој процент е 61.20 и 71.3 (соодветно), односно просек од 66.25% што не е воопшто за занемарување. Ова значи дека во овие земји има услов за развивање на електронско тргување, посебно ако компарираме со податоците кои се прикажани во табелите 1 и 2, подолу во текстот. Во светски рамки до 2014 година 40 проценти од жителите го употребуваат Интернетот. Ова покажува дека и Република Македонија и Русија се над просекот. И по региони состојбата е слична. Просекот за Азија изнесува 32%, а за Европа е 75%. Ова укажува дека Република Македонија е нешто под просекот на европските земји во нивната употреба на Интернет. Сепак за да се земе предвид релевантноста која се наоѓа во фактот за различната големина на овие две земји по број на жители и површина е прикажана на слика 3, која ја укажува пенетрацијата на интернет пристапот во светски рамки.

**Табела бр. 1 Светска
употреба на интернет**

	2005	2010	2014
Светска популација	6.5 милијарди	6.9 милијарди	7.2 милијарди
Некорисници на Интернет	84%	70%	60%
Корисници на Интернет	16%	30%	40%
Корисници во земји во развој	8%	21%	32%
Корисници во развиени земји	51%	67%	78%

Извор: International Telecommunications Union

Овие податоци укажуваат на фактот дека овие земји имаат релативно добри услови за користење на електронско работење, кое се однесува на електронска трговија, електронско банкарство, електронски маркетинг и слично. Овие земји имаат добар предуслов за користење на електронските финансии.

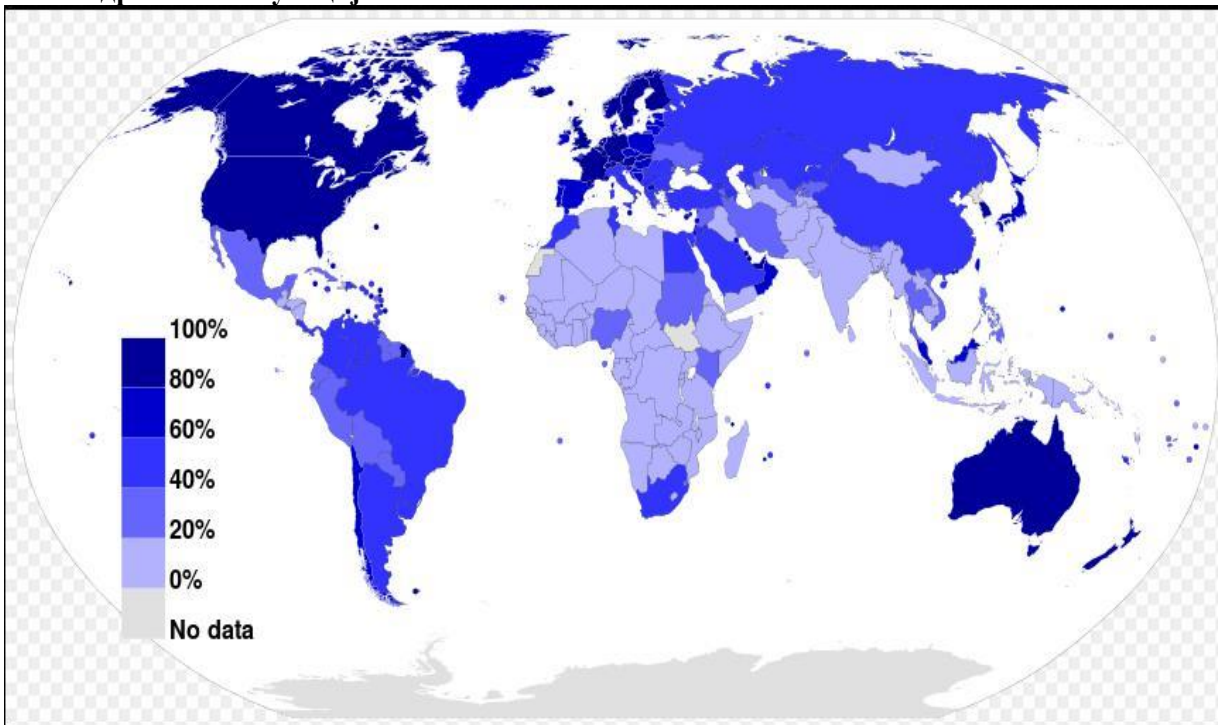
**Табела бр 2 Корисници на
Интернет по региони**

	2005	2010	2014
Африка	2%	10%	19%
Америка	36%	49%	65%
Арапски држави	8%	26%	41%
Азија и Пацифик	9%	23%	32%
Заедницата на независни држави	10%	34%	56%
Европа	46%	67%	75%

Извор: International Telecommunications Union



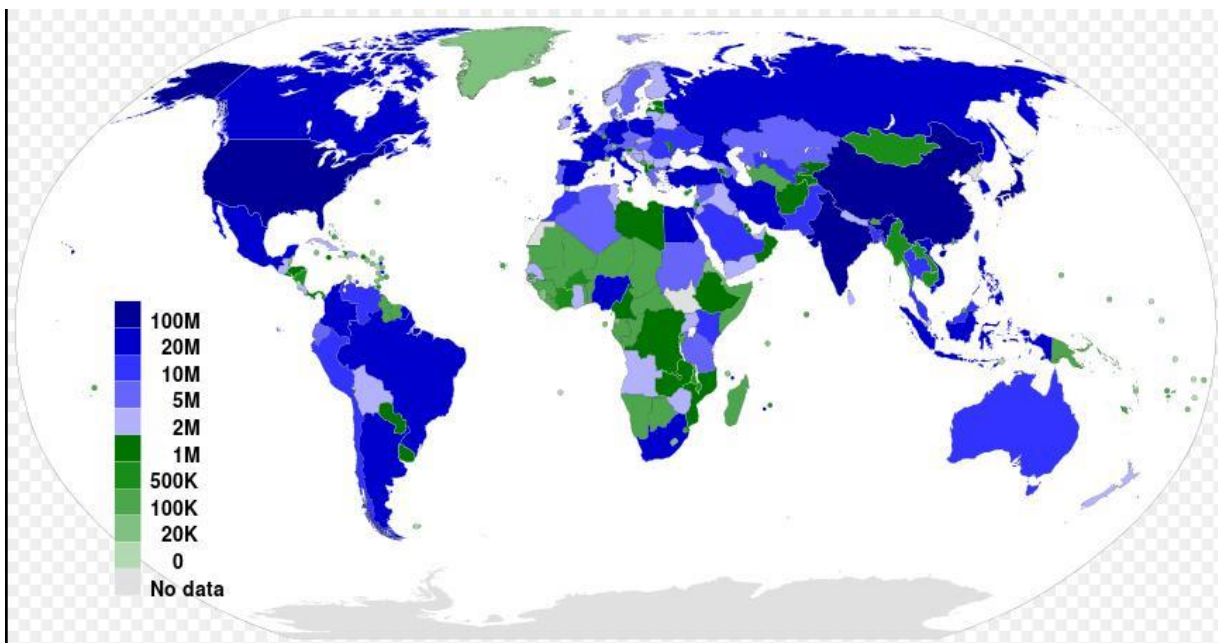
Слика бр. 1 Интернет корисници во 2012 година како процент од државна популација



Извор: International Telecommunications Union

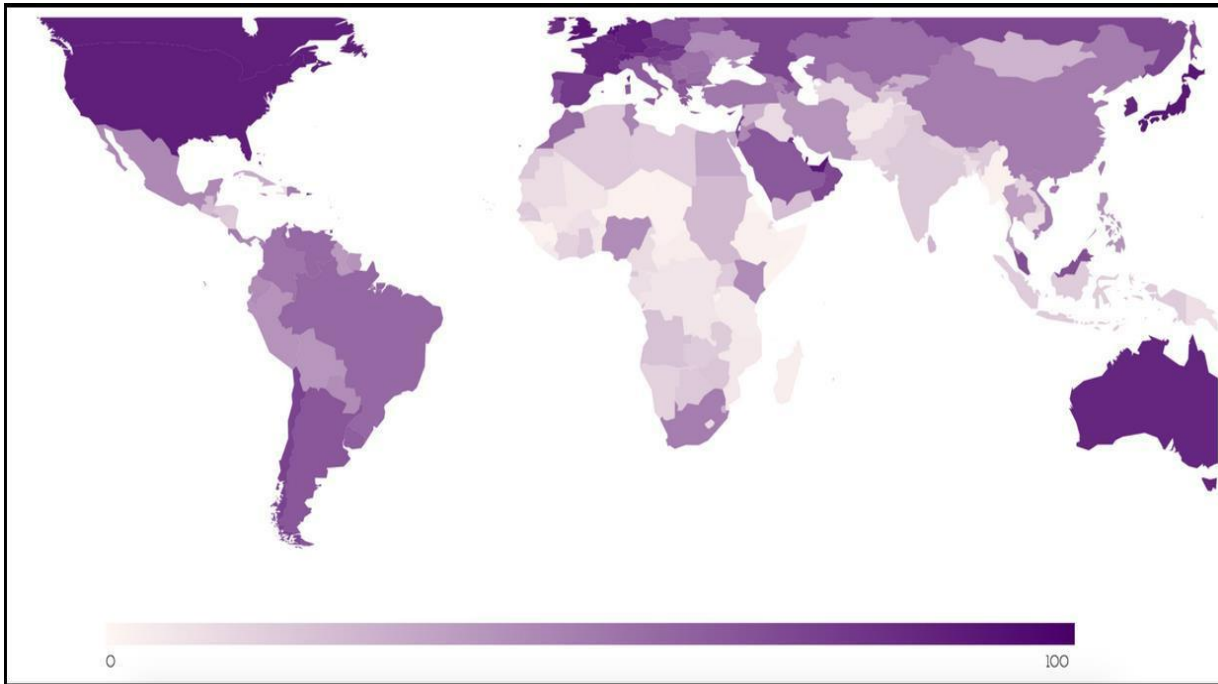
Сепак, постојат низа предизвици на кои треба да се одговори кога станува збор примената на електронските финансии. Посебно станува збор за нивно менаџирање затоа што тие веќе имаат примена, но прашањето за нивно одржување и развој значајно може да влијае на унапредувањето на економските текови.

Слика бр. 2 Број на интернет корисници во 2012 година





**Слика бр. 3 Интернет пенетрација низ светот во
2014 година**



Извор: World Bank

2. Предици за менаџирање на електронските финансии

Бизнисите континуирано ги прошируваат своите услуги базирани на Интернет и електронско тргување со цел да се намалат севкупните трошоци, а да се зголемуваат приходите. За ефективно и ефикасно остварување на овој процес потребна е контролирана инфраструктура која ќе нуди безбедност со која ќе се гарантира сигурност во ваквите системи, а со тоа и опстанок на оваа база на долг рок.

Крајните корисници треба да бидат сигурни во своите добавувачи и нивната способност да спроведат онлајн бизнис. А процесот треба да е гарантиран и во обратна насока. Без таква доверба, ниту бизнис секторот, ниту потрошувачите ќе спроведуваат трансакции или чувствителни комуникации низ овој медиум. Безбедноста на е-трансакциите најмногу е гарантирана низ банкарските институции, т.е. низ е-банкарство од причина што ова се најзастапените финансиски институции. Сепак, потребно е пошироко дефинирање на терминот е-трансакции.

Во текот на последните години, организациите не се комплетно превентирани од разочарувања поврзани со продавачите. Акцентот на електронската безбедност не губи во значење. Земјите дури создаваа критични стратегии за безбедност за водење бизнис преку интернет со отстранување на слабостите поврзани со корисникот како: идентификации и лозинки за пристап. Целта секогаш е едноставна и е: да го споделите со компаниите и поединците водењето бизнис преку Интернет со исто ниво на доверба колку што има во светот на хартијата. За какви било електронски трансакции треба да се воспостави доверба меѓу двете страни кои се вклучени.

Со ветувања за зголемување на приходите и оперативна ефикасност многу организации се сопнуваат на слепо во скапа опрема, а подоцна се разочаруваат заради реализацијата. Како резултат на тоа, продавачите често ја наметнуваат значајноста на вредноста на нивните вложувања како гаранција за квалитет и безбедност на процесот. Но, често се случува и наместо да се фокусираат на технологијата, продавачите да се фокусираат на градење на апликации со кои ќе привлечат клиенти. Сепак, токму ваквата селекција знае да е погрешна во целиот систем. Суштински недостаток од почеток е дизајнирањето на системи за да обезбедат пристап до бази на податоци за електронска трговија, мислејќи дека безбедносната архитектура може да се изгради независно од системот на архитектура. Премногу акцент беше ставен на технологијата, а не доволно за: леснотијата на распоредување и политиката на развој на бизнис постапки кои го опкружуваат тој процес. Решенијата



беа технички комплицирано изведени. Поради ова, потрошувачите и понатаму се загрижени во користење на интернетот за безбедна размена на пораки и електронски трансакции.

Можеби двофакторската автентичност е клуч за зголемување на довербата во електронскиот систем на тргување. Тоа подразбира се поголема застапеност и на дигиталниот потпис како клуч за реализација на трансакција. Но, од друга страна, овој процес треба да се внимава да се одржува во рамки на едноставност. Исто така, законодавноста и покриеноста на овие процеси во рамки на легислативата е многу значаен фактор кој допринесува за безбедност кај потрошувачот од една страна, но и понудувачот од друга.

Многу од дигиталните потписи, кои се често распоредени не се соодветно заштитени и затоа се изложени на ризик на измамнички активности. Соодветно складирање и оптимална заштита на дигиталниот потпис на корисникот и лозинката за да се правилно идентификува трансакцијата ќе биде од голема важност за идниот развој на електронската трговија. Постои алтернатива, која може да се постигне ова ниво на безбедноста се перципира како да не е голем пресврт. Со следниве правила на двофакторска проверка - нешто што знаете вие и - нешто имаат организациите, може да се спроведе недвосмислено безбедно решение и да се обезбеди клиенти со доверба и уверување да ги бараат овие услуги. Пример за стандардна двофакторска проверка на автентичност е статична лозинка - нештото што го знаете вие - заедно со динамична еднократна лозинка, која се испраќа или преку СМС порака на вашиот мобилен телефон, печатени на картичка или генерирани од еден знак – тоа е нештото што го имаат организациите. Финансиски институции кои го користат овој метод се штедилниците преку Центарот за податоци (SDC) во Данска. SDC ја заснова својата безбедност за мобилни дигитални потписи за домашните банкарски клиенти со реномиран успех. Копчето за потпис и проверка на корисникот се чува во рамките на модулот на хардвер за безбедност во централен сервер, наместо на хард дискот на корисникот. Невозможно е да се украде клуч од овој заштитен сервер, дури и за администраторот на системот. За да пристапите до копчето, корисникот треба да докаже дека ја знаат лозинката и се сопственици на телефонот / картичка / токен. Откако се користи, лозинка се бриши, што ја прави неважечка за идните трансакции. Ова е идеално за корисници кои немаат пристап до читач на смарт картичка, а исто така нуди мобилност без да се загрози безбедноста.

Насоката на апликациите, денес, а и во иднина е кон задоволување на сите потрошувачки потреби. Едни од најважните потрошувачки потреби во електронското тргување е и безбедносниот праг. Од тие причини технологиите се развиваат и во насока на подобрување на преференците, јазиците, методите за заштитите на приватноста и сопственоста при електронските тргувања. Најнов модел на кој се работи е „mind reader security check“ безбедносен читач кој работи на проверка на мозокот. Се работи за програма со која предвид ќе се земаат не само физичките и електронските сигнали и карактери, туку ќе се анализираат и нервни вибрации, кои се појавуваат како реакција на некое однесување. Пример, време до одговарање, време за одговарање, начин на пишување, начин на изговарање и слично.

Во светот на електронското тргување безбедносните системи постојат поради тоа што се среќаваат повеќе форми на сајбер закани. Од сите нив посебен акцент е ставен на заканата позната како „phishing“. Станува збор за лажно претставување како некоја легитимна институција која ги користи личните податоци подоцна за сопствени потреби. За валидноста на институцијата која ги бара податоците, корисникот не знае, а ги внесува сите потребни информации поради тоа што смета дека е приклучен на легитимна и законски уредена организација. Проблемот за ваквата форма на хакерство е во тоа што никој од никого не краде податоци, туку тие се добиваат на „доброволна“ основа, поради тоа што корисникот е доведен во заблуда.

Начин на решавање на овој проблем се бара во повеќе насоки, но некои експерти се на мислење дека целокупното „плашење“ само ги одвраќа оние кои не работат со електронски начини на тргување воопшто и да не почнат. Мислењето се движи во насока дека сите треба да се свесни за постоење на опасност при користење со одреден начин на трансакција и дека треба внимателно да се следат известувањата и законските правила и принципи кои важат за електронското тргување. „Ако сте идентификувани каде било како некоја форма на институција со е-тргување значи дека има тек на пари преку таа институција, вие, независно кој сте, сте потенцијален таргет за така наречените phishers“ [10, стр.11-12]. Специфично е дека бројот на вакви измамници е голем, но и дека се откриваат исто така како што се и создаваат. Ова остава простор експертите да внимаваат за тоа стравот кој се создава да не е непотребен и да предизвикува непотребна одбивност кон електронското тргување. Посебно, ако се земе предвид дека веќе е факт дека банките и финансиските институции се



подложни на вакви напади од вакви лажни претставувачи поради тоа што банките и финансиските институции веќе предолго време се потпираат само на единечна факторска технологија – лична идентификација и лозинка со кои корисниците се најавуваат за да ги добијат онлајн финансиските услуги. Поради тоа и активно се работи на сите гореспоменати методи за заштита на потрошувачите и за заштита на финансиските институции.

Финансиските институции за да се заштитат од потенцијалните напади и користења на нивното име за малверзациски цели можат да применуваат повеќе претпазливи мерки [10, стр.11-12]:

да ги пријават најсличните домени на нивниот бренд за проверка дали и тие се регистрирани и валидни;

користење на лого за сопствените домени;

мониторинг (на сите регистрации на нови домени слични на нивниот);

објавување на јасна политика за сопствените имејл корисници, како и на барање лични податоци или користење линкови на клик;

создавање имејл со кој потрошувачите ќе можат да препознаат дека мејлот е легитимен;

мониторинг на означувањата;

подготовка на клиентите и комуникација со нив за можните напади од измамници и

сл.

Електронското тргување сè повеќе зазема сложени форми и конфигурации, неговата употреба застапена на финансиските пазари со тенденција да се надградува и проширува. Покрај електронското банкарство, воопшто економијата сè повеќе се користи со електронското тргување.

Современите трендови наметнаа потреба до доближување кон потрошувачите. Тоа доближување се врши на начини да се олесни набавката, употребата, користењето на производите. Покрај електронското комуницирање, светот на финансиите употреба и поинакви методи во работењето, услугите и маркетингот.

Користена литература

- Catherine S. Wier, Gary Douglas, Martin Carruthers, Mervyn Jack, “User perceptions of security, convenience and usability for ebanking authentication tokens”, Elsevier, UK, 2008
- Chi Shing Yiu, Kevin grant, David Edgar, “Factors affecting the adoption of Internet Banking in Hong Kong – implications for banking sector”, International Journal of Information Management, UK, 2007
- Fethi Calisir, Cigdem Altin Gumussoy, “Internet banking versus other banking channels: Young consumers’ view”, International Journal of Information Management, UK, 2008
<http://www.efinance.com.eg/about.htm>
<http://www.financialservicescompanies.net/>
- Jack Ribeiro, “Financial Services in 2010 - Hallmarks of Success”, Deloitte – Global Financial Services Industry, USA, 2005
- James S. Harrison, Mary Gotschall, “E – Finance Debut New Era”, Segal Saved, USA, 2003
- Marta Orviska, John Hudson, “Dividing or uniting Europe? Internet usage in the EU”, Elsevier, UK, 2009
- P. Robinson and A. Yautsiukhin, “Security and Trust in IT Business Outsourcing: a Manifesto”, Elsevier, UK, 2007
- Sally Robert, “Increased security needed to tackle phishing threat”, Business Insurance; 11/28/2005, Vol. 39 Issue 48
- Tommi Laukkanen, Suvi Sinkkonen, Pekka Laukkanen, “Communication strategies to overcome functional and psychological resistance to the Internet banking”, Elsevier, UK, 2009
- Yoris A. Au, Robert J. Kauffman, “The economics of mobile payments: Understanding stakeholder issues for an emerging financial technology application”, Science Direct, UK, 2007
- Михаил Петковски, „Финансиски пазари и институции – второ дополнето изменето издание“, Универзитет „Св. Кирил и Методиј“ Скопје, 2009
- Ристо Фотов и Марија Гогова Самоников, „Финансиски пазари и институции“, Универзитет „Гоце Делчев“, Штип, 2014

