Универзитет „Гоце Делчев“-Штип, Правен факултет
Штип, Република Македонија

ПЕТТА МЕЃУНАРОДНА НАУЧНА КОНФЕРЕНЦИЈА

ОПШТЕСТВЕНИТЕ ПРОМЕНИ ВО ГЛОБАЛНИОТ СВЕТ

ЗБОРНИК НА ТРУДОВИ

Штип, 2018

Fifth International Scientific Conference: SOCIAL CHANGES IN THE GLOBAL WORLD © 2018 Copyright Goce Delcev University in Shtip, Republic of Macedonia. Address: Goce Delcev University, Shtip, Faculty of Law, ul. Krste Misirkov bb, PO box 201, 2000, Shtip, R. Macedonia. www.ugd.edu.mk;

Печати / Print 2-ри Август-Штип / 2- ri Avgust- Shtip
Уредници: Марија Амповска, Кристина Мишева, Елена Максимова

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

316.42(100)(062)

INTERNATIONAL scientific conference Social change in the global world (5; 2018 ; Штип)
Општествените промени во глобалниот свет : зборник на трудови
/ Петта меѓународна научна конференција = Social change in the global world : proceedings /
Fifth international scientific conference = Социальные изменения в глобальном мире :
сборник материалов / Пятый международная научная конференция. -
Штип : Универзитет "Гоце Делчев"-Штип, Правен факултет ; Shtip :
Goce Delcev University, Faculty of law, 2018
Начин на пристап (URL): http://js.ugd.edu.mk/index.php/scgw. - Текст во PDF формат,
содржи 1047 стр. - Наслов преземен од екранот. - Опис на изворот на ден 29.08.2018. -
Трудови на повеќе јазици. - Фусноти кон текстот. - Библиографија кон трудовите

ISBN 978-608-244-548-9
а) Општествени промени - Свет - Собири COBISS.MK-ID 108125706

Организациски комитет / Organizational Committee/ Организационный комитет конференции

Kristina Misheva PhD, Faculty of Law, Goce Delcev University in Shtip, Macedonia, kristina.miseva@ugd.edu.mk
Marija Ampovska PhD, Faculty of Law, Goce Delcev University in Shtip, Macedonia, marija.radevska@ugd.edu.mk
Elena Maksimova, LL.M, Faculty of Law, Goce Delcev University in Shtip, Macedonia, elena.ivanova@ugd.edu.mk
Strasko Stojanovski, PhD, Faculty of Law, Goce Delcev University in Shtip, Macedonia, strasko.stojanovski@ugd.edu.mk

Програмски комитет / Program Committee / Программный комитет конференции

Agim Nuhiu PhD, Faculty of Law, State University of Tetovo, Macedonia, agim.nuhiu@unite.edu.mk
Alenka Verbole PhD, currently- OSCE Mission in Tirana, University of Ljubljana, Slovenia, alenka.verbole@osce.org
Ana Nikodinovska Krstevska PhD, Faculty of Law, Goce Delcev University in Shtip, Macedonia, ana.nikodinovska@ugd.edu.mk
Anastasia Bermúdez Torres PhD, Faculty of Law, Political Science and Criminology, University of Liege, Belgium, abermudez@ulg.ac.be
Andon Majhoshev PhD, Faculty of Law, Goce Delcev University in Shtip, Macedonia, andon.majhosev@ugd.edu.mk
Belul Beqaj PhD, University of Business and Technology, Department of Political Science, Prishtina, Kosovo, belul.beqaj@gmail.com
Borka Tushevska PhD, Faculty of Law, Goce Delcev University in Shtip, Macedonia, borka.tusevska@ugd.edu.mk
Elena Ivanovna Nosreva PhD, Faculty of Law, Voronezh State University, Russia, elena@nosyreva.vrn.ru
Gabriela Belova PhD, Faculty of Law, University “Neofit Rilski”, Blagoevgrad, Bulgaria, gbelova@hotmail.com
Gemma Andreone PhD, Institute for International Legal Studies of the Italian National Research Council (ISGI - CNR), Italy, gemma.andreone@gmail.com
Ice Ilijevski, PhD, Faculty of security – Skopje, University St. Kliment Ohridski – Bitola, iilijevski@fb.uklo.edu.mk
Igor Kambovski PhD, Faculty of Law, Goce Delchev University in Shtip, Macedonia, igor.kambovski@ugd.edu.mk
Ivana Bajakić PhD, Department of Economic Sciences, Faculty of Law, Zagreb, Croatia, ivana.bajakic@pravo.hr

Jadranka Denkova PhD, Faculty of Law, Goce Delcev University in Shtip, Macedonia, jadranka.denkova@ugd.edu.mk
James C. Helfrich PhD, Global Scholars, Liberty University, Colorado, USA, jchelfrich@aol.com
Jovan Ananiev PhD, Faculty of Law, University “Goce Delcev”- Shtip, Macedonia, jovan.ananiev@ugd.edu.mk
Jovan Zafiroski, PhD, Faculty of Law, St Cyril and Methodius University in Skopje, j.zafiroski@pf.ukim.edu.mk
Kristina Misheva PhD, Faculty of Law, Goce Delcev University in Shtip, Macedonia, kristina.miseva@ugd.edu.mk
Kristine Whitnable PhD, Faculty of Law, Goce Delcev University in Shtip, Macedonia, kristine.whitnable@ugd.edu.mk
Maciej Czerwinski PhD, Institute of Slavic Philology, Jagiellonian University, Krakow, Poland, maciej.czerwinski@uj.edu.pl
Marija Ignjatovic PhD, Faculty of Law, University of Nis, Serbia, marija@prafak.prafak.ni.ac.rs
Migena Leskoviku Prof. Dr, University of Tirana, Albania, migena.leskoviku@gmail.com
Naser Ademi PhD, Faculty of Law, State University of Tetovo, Macedonia, dr.naserademi@gmail.com
Natalia Vladimirovna Butusova PhD, Faculty of Law, Voronezh State University, Russia, butusova@law.vsu.ru
Nikolai Baranov PhD, Baltic state technical university Voenmeh, At. Petersburg State University, St. Petersburg, Russia, nicbar@mail.ru
Nives Mazur Kumrić PhD, Faculty of Law, Political Science and Criminology, University of Liège, Belgium, nives.mazurkumric@ulg.ac.be
Novak Krstić, PhD, Faculty of Law, University of Niš, novak@praf.ni.ac.rs
Olga Koshevaliska PhD, University “Goce Delcev”- Shtip, Faculty of Law, Macedonia, olga.kosevaliska@ugd.edu.mk
Ruzica Simic Banovic, PhD, Assistant Professor, Faculty of Law, University of Zagreb, Croatia, ruzica.simic@pravo.hr
Silviu G. Totelecan PhD, Cluj-Napoca Branch of Romanian Academy, Socio-Human Research Department of "G. Baritiu" History Institute, Romania, silviu.totelecan@g,ail.com
Slavejko Sasajkovski PhD, Institute for Sociological, Political and Legal Research, University “St. Cyril and Methodius”, Skopje, Macedonia, bilbilef@isppi.ukim.edu.mk
Strahinja Miljkovića PhD, Faculty of Law, Mitrovica, strahinja.miljkovic@pr.ac.rs
Strashko Stojanovski PhD, Faculty of Law, Goce Delcev University in Shtip, Macedonia, strasko.stojanovski@ugd.edu.mk
Suzana Dzamtoska Zdravkovska PhD, American University of Ras Al Khaimah, Ras Al Khaimah, UAE, suzana.zdravkovska@aurak.ac.ae
Tamara Perisin, MJur (Oxon) PhD, Department of European Public Law - Jean Monnet, University of Zagreb - Faculty of Law, Croatia, tamara.perisin@pravo.hr

Tunjica Petrašević PhD, Faculty of Law, University of Osijek, Croatia, tpetrase@pravos.hr
Wouter Van Dooren PhD, Public Administration and Management, University of Antwerp, Belgium, wouter.vandooren@uantwerpen.be
Yuriy Nikolaevich Starilov PhD, Faculty of Law, Voronezh State University, Russia, juristar@vmail.ru
Zeynep Ece Unsal, PhD, Istanbul Gelisim University, Faculty of Economics Administrative and Social Sciences - Department of Political Science and International Relations, zeunsal@gelisim.edu.tr

Содржина

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

СИГУРНОСНИ АСПЕКТИ НА ЕЛЕКТРОНСКАТА ТРГОВИЈА

Апстракт
Секоја компанија, честопати и индивидуи, здружени за исполнување одредени потреби или едноставно за забава, имаат свои внатрешни мрежи, како и истовремен пристап до глобалната компјутерска мрежа. Компјутерите, лаптопите и паметните мобилни телефони се достапни практично за сите социјални сегменти на општеството, со што се унапредуваат комуникациите и поврзувањето. Интернетот нуди многу начини да се едуцираат корисниците, но и да се препознаваат основни и напредни функции на компјутерите. Овој пристап е истовремено револуционерен, значаен од гледиште на развој на човечката цивилизација, од причина што, за прв пат во историјата, може "на едно место "да го најде целото знаење, искуство и достигнувања. Од друга страна, истиот е опасен бидејќи на интернет се кријат различни „замки“ за неискусните корисници, па дури и за оние кои знаат нешто за заштитата на својата приватност и финансии. Најмногу корисници на интернет имаат одредена цел за тоа - допишување со пријатели, изнаоѓање на разни информации, електронска трговија или електронско банкарство - можностите се многу различни и разновидни. Сепак, сите такви корисници имаат еден заеднички проблем, во исполнувањето на својата цел при користењето на интернетот - немаат доволно внимание, време или волја да се заштитат и запознаат со можните проблеми што можат да ги снајдат ако наивно или недоволно сериозно влегуваат во различни видови на трансакции или комуникации. Општо познат факт е дека е можно да се извршат многу класични кривични дела на интернет, како и да се приберат информации за корисниците со кои може да се подготви или да се овозможи извршување на речиси сите кривични дела против животот и физичкиот интегритет, имотот, авторските права, како и многу други. Покрај овие, постојат и кривични дела чија појава и развој се поврзани исклучиво за развојот на електронските комуникации и интернетот. Станува збор за широка палета на однесувања кои можат да бидат безопасни, но може да доведат и до сторување на најтешки кривични дела.

Faculty of Law, Goce Delcev University, Shtip, Republic of Macedonia

Клучни зборови: *интернет, криминал, е-трговија*

Igor Kambovski, Ph.D.
Associate Professor,
Faculty of Law, “Goce Delchev” University – Shtip,
Republic of Macedonia
igor.kambovski@ugd.edu.mk

SECURITY ASPECTS OF ELECTRONIC COMMERCE

Abstract

Every company, and often individuals, which are able to fulfill certain needs or simply just for fun, have their own internal networks as well as a simultaneous approach to the world wide web. Computers, laptops and smart mobile phones are available to all segments of society, which improves connectivity and communication. This is generally possible with the unstoppable spread of internet and unlimmited use of it`s capacities. The Internet itself offers many ways to educate users and to recognise basic and advanced computer functions. This approach is at the same time revolutionary, remarkable from the point of view of the development of human civilization that, for the first time in history, can "at one time" find all of its knowledge, experience and achievements. On the other hand, it is dangerous because there are different traps for inexperienced, and even for those who know something about protecting their privacy and finance. Most Internet users have a specific goal of doing it - correspondence with friends, finding different information, electronic commerce or electronic banking - тhe possibilities are very different and varied. Nevertheless, all those users have one thing in common, in fulfilling their goal of staying online - they do not have enough attention, time or even the will to properly protect themselves and get to know the possible troubles thay may encounter if they enter into different types of transactions or communications. It's a fact that many classic crimes can be committed on the Internet, as well as acquiring information on users can prepare or enable the execution of almost all criminal offenses against life and physical integrity, property, copyright, and many others. In addition to them, there are also criminal offenses whose development is exclusively related to the development of electronic communication and the Internet. There is a wide range of behaviors that can be harmless, but can lead to the most serious crimes.

Key words: *Internet, crime, E-Commerce*

1. Појавата на интернетот, новите предизвици и закани

Динамичноста на современото живеење и работење носи привилегии, предности, олеснувања, поедноставувања на секојдневните процеси, но крие и извесни опасности и закани, некогаш доволно очигледни за неукиот човек, а некогаш високо софистицирани и прикриени. Денес е тешко да се најде семејство без компјутер, човек без паметен телефон или компанија без сопствена мрежа на сервери и компјутери. Од почетокот на 21 век, интензивниот развој на комуникациите и напредните технологии овозможи експанзија на користењето на компјутерите и мобилните телефони, истите станаа достапни до секој човек и можностите за нивно користење, како за работа така и за едукација, забава или комуницирање, станаа неограничени. Интернетот се разви во невидени размери, што овозможи брзо, непречено и неограничено дистрибуирање на информациите[1]. Појавата и развојот на социјалните мрежи Facebook[2], Instagram, комуникациските канали Viber[3], Whatsapp, Messenger и други, значат револуција во поврзувањето на луѓето ширум планетата Земја, но зад себе кријат и можност за потенцијални измами, кражби на личните податоци и идентитети на невнимателните и неискусните корисници. Така, дојде до појава на еден нов вид криминал, кој се крие зад високотехнолошките достигнувања, а кој е глобално познат под името Сајбер криминал.

Не е тешко да се претпостави дека таквиот развој на настаните ќе предизвика интерес кај јавноста за покренување иницијатива за соодветна заштита од новонастанатата закана. Имено, се појавија поединци кои за себе препознаа лесен начин на незаконско и неосновано збогатување, преку упад во туѓи компјутерски мрежи и кражба на податоци. Интернетот покажа слабост-беше ранлив и овозможуваше неовластен пристап до приватни компјутери и мрежи, нешто што како најголем проблем се провлекува и постои и денес. Таквиот развој на настаните доведе до појава на глобален бран на кривични дела кои се во директна врска со компјутерските технологии и интернетот. Така, во

[1] Во јуни 2017 година, бројот на корисници на интернет во светски размери изнесувал 3 милијарди и 885 милиони, што претставува 51,7 % од вкупната светска популација. види: http://www.internetworldstats.com/stats.htm

[2] Во јуни 2017 година, бројот на корисници на Facebook во светски размери ја надминал бројката од 2 милијарди; види: https://techcrunch.com/2017/06/27/facebook-2-billion-users/, за да во мај 2018 година бројката на активни корисници изнесува 2 милијарди и 230 милиони-види: https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/

[3] Во јуни 2017 година, бројот на корисници на Viber во светски размери изнесувал 920 милиони, а во март 2018 година бројката на активни корисници надмина 1 милијарда; види: https://www.statista.com/statistics/316414/viber-messenger-registered-users/

1998 година се случи првиот масовен напад на интернет, при што во светската мрежа беше уфрлен таканаречен „црв“ или worm, во вид на самообновувачка програма која се шири низ мрежата, ги напаѓа индивидуалните компјутери и ги брише и уништува податоците. Овој напад резултираше со уништување на речиси една третина од интернет содржините во САД. Креаторот на „црвот“ Роберт Морис беше уапсен и осуден во САД на 400 часови доброволна работа и парична казна од 10.000 долари. Во летото 1994 година Владимир Левин од Санкт Петерсбург успеа неовластено и незаконито да префрли средства во износ од 10.7 милиони долари од системот на американската Ситибанк, но во 1995 година беше уапсен во Лондон, екстрадиран во САД и во август 1997 година е осуден на казна затвор во траење од 3 години и парична казна од 250.000 долари. Во 1995 година беше уапсен Кевин Митник, хакер од САД, заради кражба на податоци од повеќе од 20.000 кредитни картички. Денес, Митник е сопственик на угледна консултанска компанија во САД која пружа услуги во областа на безбедноста и сигурноста на информатичките системи и комуникации[4].

Во периодот меѓу 1995 и 2002 година речиси и да не постои поважна владина институција или агенција во САД, меѓународна корпорација или организација чија интернет страница не беше „хакирана“, односно пробиена нејзината заштита при што беа бришени, заменети или видоизменети содржините на тие страници[5]. Паралелно со овој, речиси безопасен „тренд“ на привлекување внимание или изразување протест поради одредени, најчесто политички причини, се појавија и првите финансиски измами на интернет, особено после појавата на електронското банкарство и започнувањето на користењето на платежните картички за трансакции на интернет. Ова се фундаментите на новиот, модерен вид криминал, таканаречен сајбер криминал. Веќе постоечките и познатите криминални групации веднаш се прилагодија на новото опкружување и создадоа плодно поле за ширење на нивните нелегални активности. Организираниот криминал, тероризмот, порнографските и педофилските мрежи и групи, трговијата со оружје, дрога, органи и луѓе започнаа да ја користат новата глобална платформа за организирање на своите активности. Се проценува дека штетата која била причинета во 2006 година, од страна на наведените криминални групации, преку сајбер криминалот, во глобални размери изнесувала околу 200 милијади евра[6]. Во февруари 2007

[4] види; http://www.nytimes.com/1995/02/16/us/a-most-wanted-cyberthief-is-caught-in-his-own-web.html?pagewanted=all; како и; https://en.wikipedia.org/wiki/Kevin_Mitnick

[5] во 2003 година преку интернетот бил дистрибуиран дотогаш најдеструктивниот црв, таканаречениот „Сафирен црв“ кој во неколку минути успеал за контаминира 90 проценти од активните компјутери во светот, кои биле без адекватна заштита. види: https://www.caida.org/publications/papers/2003/sapphire/sapphire.html

[6] Prlja D., Reljanović M., *Pravna* informatika, Beograd, 2009, стр.46

година беше извршен симултан напад, заради целосно онеспособување на шест од тринаесет таканаречени „root“ сервери на интернет. Доколку напаѓачите успееле во своите намери, интернетот би колабирал. Сепак, во нападот беа онеспособени само два сервери и складирањето и протокот на информации не претрпеле позначајни повреди.

Од погоре изнесеното, можат да се забележат извесни закономерности и правилности кои го дефинираат сајбер криминалот. Имено, користењето на компјутерите и интернетот се единствената точка на врзување меѓу сите наведени нелегални активности. Сепак, во последните години овој елемент е проширен, со појавата и развојот на „паметните“ мобилни телефони. Така, сајбер криминалот веќе не е исклучиво поврзан и зависен од компјутерите, туку е зајакнат со користењето на сите видови нови технологии и електронски комуникации. Бројот на кривични дела кои можат да бидат сторени преку новите технологии и комуникации се шири како по број така и по разновидност.

2. Е-трговијата и сигурноста на трансакциите

Од најраните зачетоци на трговијата, кога луѓето почнале да разменуваат стоки и услуги, постојат поединци кои својата креативност и интелигенција ја насочувале во погрешен правец, смислувајќи нечесни дејствија заради полесно остварување на лична материјална корист. Почнувајќи од штелувањето на вагите на пазарите, изработката на лажни пари, доведување во заблуда во поглед на предметот на продажбата, лажното претставување-ваквите обиди постојат од секогаш и траат до денес, но во услови на Е-опкружување, современите измамници се прилагодуваат на новонастанатите услови и го следат чекорот на технолошките промени, секогаш подготвени да "понудат" нова измама, нов начин на незаконско стекнување противправна имотна корист.

Е-трговијата и Е-бизнисот во целина, и покрај својата голема ефикасност, поради фактот што станува збор за вршење на деловните активности меѓу отсутни лица, многу инспиративно делува за различните видови нечесни дејствија и измами. Компјутеризацијата на сите сегменти на општественото живеење во голема мерка го зголемува ризикот од измами и други видови злоупотреби, од причина што компјутерите често претставуваат замена за луѓето (автоматизација на купувањето) и во услови на Е-трговија се појавуваат нови и непредвидливи недозволени активности кои не е можно да се реализираат во услови на традиционалната трговија. Поради тоа, мора да се посвети особено внимание на безбедносните аспекти на Е-трговијата.

Заштитата на трансакциите кај Е-трговијата е исклучително сложен и скап процес. Тој се базира на воспоставување заштитени системи кои ќе бидат способни да ги идентификуваат евентуалните закани и да ги анализираат можните ризици и загуби кои можат да настанат. Системот бара вградување

одредени заштитни механизми како што се контролата на пристап, кодирањето на информациите и воведување на сигурносни протоколи. Доколку дојде до злоупотреба на Интернет технологиите можат да настанат сериозни економски последици, како што се[7]:

-директни финансиски загуби, преку префрлање на определен паричен износ од една на друга сметка или преку бришење на чувствителни податоци од финансиска природа;

-губење на вредни и доверливи информации. Многу компании зачувуваат и испраќаат податоци од технолошка природа или лични податоци за своите клиенти, кои претставуваат доверливи податоци од голема важност за кмпанијата. Неовластениот пристап и користење на таквите податоци може да предизвика значителни финансиски и репутациски загуби за компанијата;

-губење деловни потфати и зделки заради недостапност на електронските услуги. Електронските сервиси можат да "паднат" и да станат недостапни во подолг временски период или во оној период кој е од значење за вршење на конкретната трансакција, поради напад врз системот од страна на злонамерници или поради случајни откажувања на системот. Ова може да предизвика катастрофални финансиски последици за компанијата.

-Неовластена употреба на ресурсите. Неовластеното лице (т.н. "хакер") кое може да пристапи кон одредени ресурси на системот, истите може да ги злоупотреби заради лични интереси и профит;

-Губење на деловниот углед и довербата кај клиентите. Компаниите можат да претрпат сериозни загуби заради лошото искуство на нивните клиенти или заради негативниот публицитет, како резултат на нападот на нивниот систем или заради лажното претставување на неовластеното лице како припадник или претставник на таа компанија;

-Трошоци генерирани како последица на неизвесните услови на тргување. Честите прекини на функционирањето на системот и услугите предизвикани од надворешни или внатрешни напади, грешки и слично, можат да го парализираат вршењето на деловните трансакции, и тоа на подолг временски период, што повторно води кон сериозни финансиски загуби.

Сите горенаведени последици можат да ги почувствуваат и потрошувачите, како директни корисници на таквите услуги на Е-трговијата.

Секој систем во кој се чуваат и процесираат податоци спаѓа во групата на загрозени системи и потребна му е заштита. Генерално, како закана за секој систем можат да се сметаат секое лице, објект или настан кои потенцијално можат да доведат до загрозување на безбедноста на податоците во системот. Таквите закани можат да бидат случајни (несакано бришење на некое досие или

[7] Novaković J., *Elektronsko poslovanje, drugo izmenjeno i dopunjeno izdanje,* Megatrend Univerzitet, Beograd, 2008, стр.215

фајл со податоци) или намерни (злонамерна модификација на чувствителните податоци или хардверот на системот). Токму затоа, овие закани треба да се идентификуваат и да се спречат, а доколку веќе настапиле треба да се спроведат постапки за нивно отстранување и минимизирање на штетите.

Основни цели на преземањето мерки за безбедност на системите кај трансакциите во рамки на Е-трговијата се[8]:

-доверливост-обезбедува недостапност на информациите на неовластени лица;

-интегритет-обезбедува конзистентност на податоците, спречува неовластено генерирање, промена или уништување на податоците, односно обезбедува потврда дека податоците останале непроменети;

-достапност-овластените корисници можат да ги користат услугите и базите на податоци во секое време;

-ексклузивна употреба на системот од страна на овластени корисници-ресурсите не можат да се користат од неовластени лица. Овде посебен акцент е ставен на превенцијата од лажно претставување со воспоставување на контролни механизми-идентификација на изворот и верификација на идентитетот на лицето.

Заштитата на системот, податоците и трансакциите најчесто се врши преку софистициран систем на механизми и процедури за заштита. Тука спаѓаат: идентификацијата и веродостојноста на Е-записот (автентикација), потврдувањето на веродостојноста на потпишаниот Е-запис во случај на спор, електронскиот запис и енкрипцијата, идентификација на потписникот и друго[9].

Автентикацијата е еден од начините за оневозможување на лажното претставување. Во услови на Е-трговија купувачот, продавачот, посредникот и институциите преку кои се врши плаќањето треба да се убедени во идентитетот на странката со која ја вршат трансакцијата. Идентитетот на корисникот се утврдува преку неколку параметри: шифра, лозинка/пасворд (нешто што само корисникот го знае); картичка (нешто што само корисникот го има); потпис, глас, папиларен отисок, снимка на окото, геометрија на дланка и други карактеристики (нешто што корисникот е) што се утврдуваат со биометриски контролни средства и инструменти. Ако за автентикација се користи само шифрата, како најнесигурен заштитен механизам кој може да биде откриен или пресретнат при трансферот низ системот, во тој случај безбедносниот систем може да биде компромитиран и тоа претставува сериозна закана за целиот систем. Затоа наведените безбедносни техники и механизми треба да се

[8] Novaković, *ibid*, стр.181

[9] Коевски Горан, *Електронското склучување на договорите,* Деловно право бр. 20, Здружение на правниците на РМ, Скопје, 2009, стр.245

користат во комбинација, со што ризикот од неовластен пристап и злоупотреба на податоците и трансакциите би бил сведен на рационален минимум[10].

Многу потрошувачи кои сакаат да купат одредена стока преку Интернет сакаат нивниот идентитет да биде безбеден и скриен. Тие не сакаат другите да знааат што купиле и преферираат да останат анонимни, како кога плаќаат со готови пари кај традиционалната трговија. Заради обезбедување на приватноста и тајноста на определени податоци се користи соодветна програма за нивна заштита, што се спроведува преку веќе споменатата енкрипција на податоците и нивно кодирање и декодирање, како при преносот, така и при архивирањето и чувањето на податоците. Со енкрипцијата податоците се преведуваат во облик кој е неразбирлив за оној кој не го познава или кој го нема клучот за нивно декодирање и повторно враќање во иницијалниот облик. Со тоа, конечно, се оневозможува пристап, користење на информациите и нивна злоупотреба од страна на неовластено лице[11]. Исто така, при постапката на трансфер на податоците и нивно кодирање и декодирање можно е да дојде до несакано изместување на редоследот на податоците и нивно изменување, со што тие ја губат почетната форма и содржина. Заради спречување на ваквите несакани појави и губење на податоците, потребно е да се обезбеди компјутерски софтвер-систем за интегритет на податоците кој ќе обезбеди заштита на информациите, серверите и другите компоненти на компјутерскиот систем и мрежа од неовластено модифицирање на информациите. Со овој систем за проверка можат да се откријат евентуални измени на редоследот на деловите на пораките и информациите, нивното бришење, додавање на информации и др. Со оваа програма не може во целост да се заштити системот од неовластена модификација, но може да се обезбеди детекција на таквите модификации, освен во случај кога информациите се трајно избришани и изгубени.

Комплексноста на Е-трговијата и компаниите кои се занимаваат со овој вид трговија, користењето на високи технологии и зголемената интерконективност меѓу субјектите на Е-трговијата создаваат сериозна основа за можни злоупотреби и незаконски дејствија од страна на злонамерни корисници. Со развојот на Е-трговијата, надворешните и внатрешните, во рамки на компаниите, измамници можат да ги користат традиционалните недостатоци во поглед на безбедноста, но можат и да посегнат по новите можности кои им се пружаат-нарушување на системите за безбедност преку упад и пореметување на софтверската и хардверската архитектура која најчесто претставува стожер на компаниите. Во услови на мрежно опкружување во рамки на Интернетот,

[10] Novaković, *ibid*, стр.182

[11] Drakulić M., *Osnovi kompjuterskog prava,* DOPIS, Beograd, 2003, стр.61

такви злоупотреби можат да се преземаат од било кое место и можат да предизвикаат штети на компании кои се оддалечени со илјадници километри. Затоа, во процесот на развој на бизнис стратегиите, секоја компанија мора да ги има предвид можните опасности кои се закануваат да ја загрозат доверливоста, интегритетот и достапноста на податоците со кои располага компанијата. Во тој контекст, компаниите треба да знаат како можат да бидат "нападнати" и какви се ризиците од т.н. сајбер криминал.

Современите компании и трговци кои се вклучени во Е-трговијата користат технологии во рамки на нивната инфраструктура без да претпостават дека истата таа технологија може да биде искористена и злоупотребена против нив, и тоа по цена на огромни загуби. Напаѓачите можат да ги пренасочат финансиските средства, да ги исклучат системите за комуницирање, да извршат грабеж на интелектуалната сопственост, да ја наламат репутацијата на трговецот, дури и да го уништат целокупниот процес на Е-трговија. Компјутерите можат да бидат средство за постигнување деловни успеси, но истовремено се и моќно оружје во рацете на криминалците.

Постои општо мислење дека злоупотребите и упадите на Интернет ги вршат тинејџери или фрустрирани асоцијални лица кои поминуваат премногу време пред компјутерот и кои се само желни за слава. Сепак, истражувањата укажуваат дека состојбите не се ни малку наивни и дека овие категории опфаќаат сосема мал процент од вкупната бројка извршители на Е-криминалот. Постои своевидна поделба на извршителите, и тоа според фактот дали истите делуваат од внатре, во рамки на компанијата, или нивниот упад е извршен однадвор. Така, надворешните криминалци работат сами или во рамки на добро организирани и технички опремени групи. Внатрешните напаѓачи најчесто работат сами и произлегуваат од редовите на незадоволните работници. Компаниите можат да претрпат сериозни напади и од лица кои се поранешни вработени во таа компанија и кои располагаат со доверливи информации кои можат да ги злоупотребат и да нанесат штета. Исто така, во оваа група потенцијални напаѓачи спаѓаат и добавувачите и деловните партнери кои имаат пристап кон чувствителните информации или техничката инфраструктура.

Напаѓачите ги избираат своите цели на ист начин како што тоа го прават и останатите криминалци. Тие прибираат јавно достапни информации за техничките слабости на мрежните системи и ги комбинираат со вербалните информации од лица кои имаат пристап кон доверливи и чувствителни инсајдерски информации, се со цел да се развие што е можно посигурен и подобар метод за напад. И надворешните и внатрешните напаѓачи бараат што е можно полесен и поедноставен начин да ги истражат слабостите и да извршат незаконски продор во мрежата на компанијата. Не секогаш нападите започнуваат во сајберпросторот. Напротив, физичката кондиција и безбедност на системите и објектите е од круцијално значење за соодветен безбеден сајбер

простор. На пример, нападот може да биде насочен кон објектите на компанијата, со цел да се предизвика пожар кој ќе иницира исклучување на напојувањето со електрична енергија и привремен пад на компјутерскиот систем, сосема доволен за упад во истиот и причинување штета. Исто така, напаѓачот може да провали во објектот на трговецот и да инсталира програма во компјутерот на трговецот преку која подоцна ќе може од надвор да ги контролира трансакциите. Од овие причини, компаниите и трговците истовремено мораат да се грижат за сигурноста на компјутерската инфраструктура, но и за сигурноста и безбедноста на објектите во кои се врши дејноста.

Постојат определени "алатки" со кои вообичаено се служат напаѓачите, и тоа: анонимни автоматски препраќачи на електронска пошта, Интернет филтери за пресретнување и контрола на мрежниот сообраќај, пробивачи на лозинки/пасворди, скенери за автоматско откривање на услугите и трансакциите, софтвер кој овозможува "маскирано" делување на напаѓачите во име на некој друг, методи за енкриптирање на податоци и нивно понатамошно препраќање во вид на графички или аудио записи, и тројанци-легитимни програми кои се изменети со вметнување на неавторизирани кодови со што програмот започнува да врши непознати и недозволени активности на штета на системот[12].

Во глобални рамки постои определен континуитет со тенденција на зголемување во поглед на обемот на компјутерскиот криминал при што како негови жртви се јавуваат милиони потрошувачи, но и трговци. Конкретно, во САД во периодот меѓу 2012 и 2016 година 13 милиони американци-корисници на кредитни картички биле жртви на компјутерскиот криминал, поточно на кражба на идентитетот[13]. Кражбата на идентитетот е сложен проблем кој е распространет секаде низ светот и постојат повеќе дефиниции за тоа кривично дело кое, всушност претставува прикриена измама преку споменатата кражба на идентитетот. Извршителите можат да дејствуваат и самостојно и изолирано, но во поголем број случаи станува збор за добро организирани мрежи кои дејствуваат на меѓународно ниво, со логистика во повеќе земји, со што бројот на нивните жртви секојдневно се зголемува. Крадците многу лесно доаѓаат до идентитетот на секој корисник на платежна картичка, на пример, со инсталирање камери над банкоматите, додека пак апаратите за копирање, дуплирање на кредитните картички многу лесно можат да се набават на Интернет. Интернетот нуди и броеви на кредитни картички, во неограничени количества, претходно украдени од хакери. Хакерските групи се добро

[12] Trifković S., *Senke interneta*, Novinski-izdavački centar "Vojska", Beograd, 2003, стр.52

[13] види: https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php

организирани, најчесто имаат свои бази во источна Европа и Азија, а нивниот интерес е насочен кон стекнување огромен профит преку украдени и "пробиени" кредитни картички[14]. Во август 2008 година американското ФБИ после пообемна истрага и следење подигна повеќе обвиненија против осомничени лица од САД, неколку земји во источна Европа и од Кина кои беа дел од најголемата и најсложената мрежа за кражба на идентитет која некогаш била откриена. Оваа криминална група изврши упади во безжичните мрежи на неколку американски синџири за малопродажба и ги украде броевите на преку 40 милиони дебитни и кредитни картички. Се претпоставува дека причинетата штета изнесувала неколку стотици милиони долари[15].

Република Македонија, во меѓународни рамки, до скоро важеше за ризично подрачје за тргување и плаќање со кредитни картички. Иако сите банки имаат инсталирано ПОС и АТМ терминали и имаат имплементирано современи и софистицирани системи на заштита, сепак, злоупотребите на кредитните картички бележат континуиран тренд на благ пораст во изминатите десетина години. Конкретно, во периодот јануари-јуни 2009 година 26 измамници, користејќи лажни кредитни картички, подигнале над 15 милиони денари од банкомати ширум државата, што е за пет пати повеќе од вкупните штети кои биле причинети од вакнвите нелегални активности во текот на 2008 година[16]. Обично криминалците биле фаќани на дело, но во наведениот период на територијата на Република Македонија оперирала и двочлена група која крадела броеви на сметки на германски државјани, ги вметнувала на бланко-кредитни картички во Бугарија и извршила нелегални трансакции на 286 банкомати во Македонија при што "заработила" над 3.180.000 денари. Нелегалните трансакции биле откриени откако германските државјани забележале одлив на средства од нивните сметки во Република Македонија, по што реагирала германската полиција и Интерпол. Сторителите биле бугарски државјани. За споредба, во текот на 2016 година се регистрирани 13 кривични дела на изработка и употреба на лажна платежна картичка каде што сторителите преку интернет на различни начини, преку употреба на соодветни технички уреди, прибавувале банкарски податоци од странски државјани. Потоа ги употребувале како вистински платежни картички и правеле нелегални трансакции.

Од статистиките и извештаите на Министерството за внатрешни работи на Република Македонија може да се констатира дека злоупотребите се прават на различни начини, а најчесто преку „скимер уреди“ кои крадците ги

[14] Petrović R. S., *Kompjuterski Kriminal,* Vojnoizdavački Zavod, Beograd, 2004, str.197
[15] види: http://www.micreditlawyer.com/7-of-the-largest-identity-theft-crimes/
[16]vidi:
http://www.novamakedonija.com.mk/NewsDetal.asp?vest=6994246546&id=12&prilog=0&setIzdanie=21707

поставуваат на банкоматите. Овие уреди се состојат од два дела, камера и читач на податоци од магнетната лента на самата картичка. Камерата ја поставуваат на различна страна, зависно од банкоматот, за да се сними ПИН-кодот. Вака украдените податоци се користат за вршење нелегални трансакции на интернет или се изработуваат фалсификувани платежни картички со кои нелегално се подигнува готовина од банкоматите. Друг начин на крадење податоци од платежни картички е при купување од интернет, односно доколку се прави трансакција преку лажна интернет-страница т.н. „fishing“ страница, која е идентична со оригиналната. Граѓаните не ја забележуваат разликата и ги внесуваат податоците, со што истите одат во рацете на криминалците.
„Скимер уредите“ ги има и во Македонија. во 2016 година е откриена криминална група од шест члена која во 13 наврати поставила вакви уреди на банкомати во Куманово, Битола, Охрид, Штип, Скопје, Прилеп и во Тетово. Тие успеале од 209 картички да извршат 201 нелегална трансакција и украле повеќе од милион денари[17].

Според последната публикација на Народната банка за платниот промет во 2016 година[18] (за жал, не е изготвена анализа за 2017 и 2018 година), македонските граѓани повеќе плаќаат со готовина отколку со картичка. Анализите за користењето на платежните картички покажуваат дека и покрај нивната зголемена употреба во последниот период, навиките на домашните потрошувачи отстапуваат од навиките на корисниците во ЕУ. Употребата на платежните картички во земјава сѐ уште првенствено се однесува на повлекување готовина од банкоматите, за разлика од европските земји каде што плаќањата во трговијата имаат високо учество. Бројот на трансакции со домашни платежни картички остварени во трговијата во Македонија во 2016 година изнесува 18 трансакции по глава на жител, што е пониско за два и пол пати во споредба со земјите од Централна, Источна и Југоисточна Европа (45 трансакции по глава на жител) и неколкукратно пониско во однос на старите земји членки на ЕУ (102 трансакции по глава на жител).

Заклучок

________Во функција на надминување на проблемите и заканите кои потекнуваат од Е-криминалот, компаниите мораат да остапат од старите навики и да развиваат стратегии за борба против новите облици на криминалитет.

[17] види: http://www.fakulteti.mk/news/17-07-18/zloupotreba_na_platezhna_kartichka_mozhe_da_vi_se_sluchi_i_koga_povlekuvate_pari_od_bankomat.aspx

[18] види: http://www.nbrm.mk/content/Platni%20sistemi/Godisna_info_platen_promet_2016.pdf

Поради тоа, тие мораат да создадат јасни и фокусирани политики за безбедност и сигурност на работењето, да ги обучуваат своите вработени за борба против новите закани и да ангажираат високо стручни и искусни експерти за одржување и заштита на компјутерските системи. Единствено така компаниите кои се вклучени во тековите на Е-трговијата ќе можат да се заштитат и себе и своите клиенти од неовластени упади, закани и можни штети кои со себе ги носи и ги предизвикува сајбер криминалот.

Користена литература:

Drakulić Mirjana., *Osnovi kompjuterskog prava,* DOPIS, Beograd, 2003

Коевски Горан, *Електронското склучување на договорите,* Деловно право бр. 20, Здружение на правниците на РМ, Скопје, 2009

Novaković Jasmina., *Elektronsko poslovanje, drugo izmenjeno i dopunjeno izdanje,* Megatrend Univerzitet, Beograd, 2008

Petrović R. Slobodan, Kompjuterski Kriminal, Vojnoizdavački Zavod, Beograd, 2004

Prlja Dragan, Reljanović Mario, *Pravna* informatika, Beograd, 2009

Trifković Slobodan, Senke interneta, Novinski-izdavački centar "Vojska", Beograd, 2003