УДК: 657:[343:004
Biblid 1451-3188, 17 (2018)
Год XVII, бр. 63, стр. 193–208
Изворни научни рад

ИЗАЗОВИ ФОРЕНЗИЧКОГ РАЧУНОВОДСТВА У САЈБЕР ОКРУЖЕЊУ

Жаклина СПАЛЕВИЋ
Косана ВИЋЕНТИЈЕВИЋ[1]

Abstract: Information technologies with the expansion of the global computer network (the Internet) have brought new forms of socially unacceptable behaviour, which should be sanctioned accordingly. The emergence of cybercrime has provoked the need for the engagement of specially trained specialists, for the suppression and prevention of such criminal actions. In this paper, we identify the state of cybercrime in the global environment, which is the biggest threat to the stability of business entities. We provide guidelines for future research in order to monitor investments in the security of information systems of businesses, in order to reduce the costs of cybercrime.

Key words: cyber-attacks, cyber security, forensic accounting, Cyber Law.

1) УВОД

Према схватању индијског професора *Subramaniana* преваре су погубни, пажљиво скривани, тајни, злонамерни и малигни, углавном инсајдерски, послови који се временом умножавају.[2] Обављање великог броја послова коришћењем информационих технологија ствара нове могућности за преварне радње. Сајбер криминал је омогућен или почињен злочин коришћењем дигиталних комуникационих уређаја и интернета.[3] Привредним субјектима могу помоћи стручњаци из области информационе безбедности тако што ће да

[1] Универзитет Сингидунум, Факултет за туристички и хотелијерски менаџмент, Београд; Универзитет Сингидунум, Факултет здравствених, правних и пословних наука, Ваљево, E-mail: zspalevic@singidnum.ac.rs

[2] Интернет: http://www.ignou.ac.in/ignou/aboutignou/icc/aciil/staff/detail/Prof_K_Subramanian-775; 12.3.2017.

[3] *Cybercrimes,* National Crime Prevention Council, United States of America, 2012, pp. 1.

осмисле и спроведу контра мере ради ублажавања безбедносних ризика током електронског пословања. Дигитална форензичка истрага у рачуноводству одвија се након што је дошло до инцидента и она у широком спектру помаже обраду кривичних предмета пред судом.[4] Најчешће се ради о индустријској шпијунажи, финансијским истрагама у вези са економским питањима (прање новца, преваре са кредитним картицама, преваре осигурања) и корпоративној политици (*e-mail* злоупотребе, недолично понашање и запошљавање). Промене у пословном окружењу које утичу на процес финансијског извештавања су: технолошки напредак, глобализација економије и пословања, промене на финансијским тржиштима и на тржишту капитала.[5] Ове промене активно прате и прилагођавају им се у свом пословању запослени у рачуноводственом сектору у привредним субјектима и запослени у ревизорским друштвима. Да би се одговорило на захтеве корисника финансијских и нефинансијских информација привредних субјеката, у време дигитализације спроведено је редизајнирање рачуноводства и ревизије. *Big data* обухвата не само класични свет рачуноводствених трансакција, већ укључује нови свет интеракција и запажања који носе широк спектар мултиструктуралних извора података који од рачуновођа и ревизора траже нове дигиталне приступе пословању. Већина врхунских дигиталних форензичких алата и техника настала је у задњих двадесет година. Преовладавање дигиталних медија и информација у скоро сваком аспекту деловања привредног субјекта, узрокује повећану потребу за дигиталним форензичким стручњацима. Дигитална форензика обухвата налажење, чување, идентификацију, извлачење, анализу, документацију и припрему случаја повезаног са дигиталним подацима и догађајима.[6]

2) УЛОГА ФОРЕНЗИЧКОГ РАЧУНОВОЂЕ У ПРЕВЕНЦИЈИ САЈБЕР НАПАДА

Информационе технологије и дигитално окружење утичу на преваре и сајбер криминал због: повећане употребе информационих технологија у пословању, повећане употребе података од стране ревизора финансијских извештаја, повећаног коришћења информационих технологија од стране починилаца превара и сајбер криминалаца[7]. Интерпол истиче да све више

[4] UK Legislation, Criminal Damage Act 1971. Интернет: http://www.legislation.gov.uk/ukpga/1971/48/contents, датум прегледа 25.03.2017.

[5] Zabihollah Rezaee, Richard Riley, *Prijevara u finansijskim izvještajima, sprečavanje i otkrivanje*, Zagreb, 2014, str. 287.

[6] Ibid., str. 301.

[7] *Education and Training in Fraud and Forensic Accounting: A Guide for Educational Institutions, Stakeholder Organizations, Faculty, and Students*, NIJ Special Report, West Virginia University – Forensic Science Initiative, 2012, p. 15.

криминалаца користи брзину, практичност и анонимност на интернету да изврше широк спектар криминалних активности које не познају границе, било физичке или виртуелне, изазивају велике штете и представљају реалне претње жртвама широм света.[8] По проценама фирме за безбедност – *McAfee Labs* (извештај из 2014. године) сајбер криминал кошта глобалну економију 445 милијарди долара годишње.[9] У глобалном привредном окружењу *on line* криминалне активности су се интензивирале од 2010. године. Према истраживању *Juniper Research* процењују се да ће до 2019. године трошкови сајбер криминала износити 2,1 трилиона америчких долара.[10] Због тога су у скоро свим земљама покренуте активности против сајбер криминала. Стручњаци у заједници технолошке сигурности процењују да губици због интернет криминала износе до 100 милијарди долара годишње, надмашујући вредност кријумчарења наркотика и опојних средстава на светском нивоу.[11] Напредак технолошких достигнућа повећава опасност за глобалну економију и сигурност. *Г*20 земље имају велике губитке од сајбер криминала. Четири највеће привреде (САД, Кина, Јапан и Немачка) имају губитак од 200 милијарди долара годишње. Земље са ниским дохотком имају мање губитке, али се и то мења јер ће те земље повећати употребу интернета, а сајбер криминалци користе мобилне платформе.[12] У корак са новим техникама напада највећи изазов безбедносних тимова данас је одбрана од тих претњи, истиче се у *Водичу за сајбер решења* сигурносне компаније *Palo Alto*, која помаже десетинама хиљада организација широм света да спрече сајбер нападе.[13] У САД постоји неколико форензичких сертификата које истражитељи морају имати да би могли да сведоче на суду. Један од сертификата је *Global Information Assurance Certification* (*GIAC*)[14]. Форензичар који поседује тај сертификат постаје сертификовани *GIAC* форензички аналитичар – *Certified Forensic Analyst* – GCFA. *Tom's IT Pro* компанија за 2017. годину фаворизује следећих пет сертификата из области дигиталне форензике: CCE: *Certified Computer Examiner*, EnCe: *EnCase*

[8] Интернет: https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime%20; 12.3.2017.

[9] McAfee, Inc., *Net Losses: Estimating the Global Cost of Cybercrime*, Santa Clara, USA, 2014, p. 3.

[10] *Cybercrime Will Cost Businesses Over $2 Trillion by 2019, Finds Juniper Research*, PR Newswire; Интернет: *www.prnewswire.com/news-releases/cybercrime-will-cost-businesses-over-2-trillion-by-2019-finds-juniper-research-503449791.html* ; датум прегледа:19.3.2017.

[11] Alison Diaz, *Meet A-Z: The Computer Hacker behind a Cybercrime Wave*, USA TODAY; Интернет: http://usatoday30.usatoday.com/tech/news/computersecurity/2008-08-04-hacker-cybercrime-zeus-identity-theft_N.htm, датум прегледа: 19.3.2017.

[12] *Net Losses: Estimating the Global Cost of Cybercrime*, Intel Security, USA, 2014, p. 5.

[13] *Buyers Guide: Cybersecurity – The definitive guide for evaluating cybersecurity solutions*, Palo Alto Networks, Santa Clara, California, USA, 2015, p. 1.

[14] Интернет: http://www.giac.org/

Certified Examiner, CFCE: *Certified Forensics Computer Examiner*, GCFA And GCFE Certification, CSFA: *CyberSecurity Forensics Analyst.*[15]

Прикупљање електронских информација је први корак током истраге дигиталних доказа. Успешна истрага дигиталне форензике захтева ангажовање стручњака који има техничке основе компјутерских технологија и који је упознат са релевантним правилима правног субјекта и истрагом. Већина алата за анализу *е-података* може вратити, исфилтрирати, извући, сортирати и анализирати податке из рачуноводствених база. Ови алати такође могу идентификовати празнине, дупликате, информације које недостају и статистичке аномалије.[16] Данас са развијеним софтверима и технолошким способностима за обраду велике количине података 100% популације у оквиру датотека може се анализирати и тестирати. Једна од предности ИТ алата у форензичком рачуноводству је да се подаци могу преузимати код клијента из главне књиге, могу се преузети и новчани токови, мрежни диск, корисничке датотеке, разне врсте веб евиденција, било где да се налазе електронски подаци. Према истраживању *AICPA Forensic and valuation Services* (*FVS*), спроведеног са *CPA* форензичарима 2011.[17] године, они на терену у 25% истрага користе *CAATS* алате, ИТ ревизорске вештине у 25% истрага, *Data Retrieval Methods* у 41% истрага и друге методе које користе су у 9% истрага.[18] Током 2014. године иста организација је објавила истраживање које показује да је *Cybersecurity* наредних две до пет година највећа претња информационој безбедности привредних субјеката – 40% свих претњи ће се односити на *Cybersecurity*.[19] Компјутери постају све савременији из дана у дан, тако да област дигиталне форензике мора да прати њихов развој. *InfoSec Institute* издваја и препоручује следеће форензичке алате који су адекватни за данашње компјутере: *SANS SIFT*, *ProDiscover Forensic*, *Volatility Framework*, *The Sleuth Kit* (+*Autopsy*), *CAINE*, *Xplico*, *X-Ways Forensics*.[20] У зависности од обима и предикције ангажовања, сваки седми форензичар у истражним техникама значајно се може ослањати на електронска складишта информација за ефикасно и ефективно анализирање и разматрање велике количине различитих

[15] Ed Tittel, Kim Lindros. est Digital Forensics Certification, Интернет: http://www.tomsitpro.com /articles/computer-forensics-certifications,2-650.html, 12.03.2017.

[16] Zabihollah Rezaee, Richard Riley: op. cit., str. 303.

[17] Интернет: http://www.aicpa.org/Pages/default.aspx; 19.3.2016.

[18] *AICPA Forensic and valuation Services: The 2011 Forensic and Valuation Services (FVS) Trend Survey*, AICPA, American Institute of CPAs, 2011, p. 19.

[19] *AICPA Forensic and valuation Services: The 2014 AICPA Survey on International Trends in Forensic and Valuation Services*, AICPA, American Institute of CPAs, 2014, p. 8.

[20] *7 Best Computer Forensics Tools,* Интернет: http://resources.infosecinstitute.com/7-best-computer-forensics-tools/#gref; 19.3.2016.

дигиталних података познатих као *electronically stored information* (*ESI*).[21]

Слика 1: Трихотомија сајбер криминала

Извор: Accountancy Europe[22]

Прилике за усклађивање технологија за анализу података за потребе откривања преваре и истраживања су одавно препознате. У студији коју су заједно издали Институт интерних ревизора (*The Institute of Internal Auditors – IIA*[23]), Амерички институт сертификованих јавних рачуновођа (*The American Institute of Certified Public Accountants – AICPA*) и Асоцијација сертификованих истражитеља превара (*Association of Certified Fraud Examiners – ACFE*[24]) „*Managing the Business Risk of Fraud: A Practical Guide*“,[25] аутори идентификују како анализа података, континуирана ревизија и мониторинг технике, као и други сродни алати и технологије, могу да се користе за откривање преварних активности.

[21] *Forensic Procedures and Specialists: Useful Tools and Techniques*, AICPA, American Institute of CPAs, 2006, pp. 3-6.

[22] *Present and future of cybersecurity,* Интернет: https://www.accountancyeurope.eu/wp-content/uploads/29.03.2017-Digital-Day_Lars-van-Mullighen.pdf, 19.3.2016

[23] Интернет: https://na.theiia.org/Pages/IIAHome.aspx; 19.3.2016.

[24] Интернет: http://www.acfe.com; 19.3.2016.

[25] Интернет: http://www.theiia.org/media/files/fraud-white-paper/fraud%20paper.pdf; 19.3.2016.

Студија описује анализу података, коришћење технологија у идентификовању аномалија, трендове и индикаторе ризика у разним трансакцијама, као и идентификовање односа међу људима у организацији и дешавања. Европол је уврстио у своје активности превенцију и сузбијање сајбер инцидената, јер криминалци брзо искоришћавају нове прилике и вешто се одупиру традиционалним мерама спровођења закона.[26] Европол представља трихотомију сајбер криминала на следећи начин. Дигитална форензичка истрага има за циљ да испита доказе како би се утврдило да ли је дошло до преваре, када се то и како десило, ко је био укључен и колико новца је изгубљено.[27] Методологија дигиталне форензичке ревизије објашњава: смернице да се пронађу трансакције које треба подвргнути тестирању, упућује на начине лоцирања скривених знакова преваре, идентификацију *црвених заставица* које доводе до незаконитих трансакција и наводи процедуре планирања ове ревизије.[28] Ако дође до прекида *ланца доказа*, суд такве доказе не прихвата. Одржавање *ланца дигиталних доказа* и метода заштите интегритета дигиталних доказа спроводе се у циљу одржања животног циклуса дигиталног доказа, да би био валидан пред судом или у извештају за менаџмент. Према Yeager-у термин *ланац очувања* или *ланац чувања*[29] односи се на потпуну ревизију и контролу оригиналног доказног материјала који би потенцијално могао бити употребљен у легалне сврхе. Допринос пружању комплексних рачуноводствених форензичких услуга дају национални и међународни закони и прописи о приватности. Такви прописи захтевају да форензички рачуновођа пажљиво процени потребу да се добију поверљиви лични подаци. Ако је потребно форензички рачуновођа ће можда морати да спроведе мере безбедности да ублажи ризик од повреде података и сакупи само податке који се могу сматрати релевантним за ангажовање. Ако добије поверљиве податке форензички рачуновођа мораће да спроведе одговарајуће стратегије за смањење опасности од неовлашћеног коришћења таквих информација.[30]

---

[26] Интернет: https://www.europol.europa.eu/, 19.3.2016.

[27] Tracy L. Coenen, *Expert Fraud Investigation: A Step-by-Step Guide*, John Wiley & Sons, Inc., Hoboken, New Jersey, 2009, p. 19.

[28] Leonard W. Vona: *Fraud Data Analytics Methodology: The Fraud Scenario Approach to Uncovering Fraud in Core Business Systems*, John Wiley & Sons, Inc., Hoboken, New Jersey, 2016, p. 10.

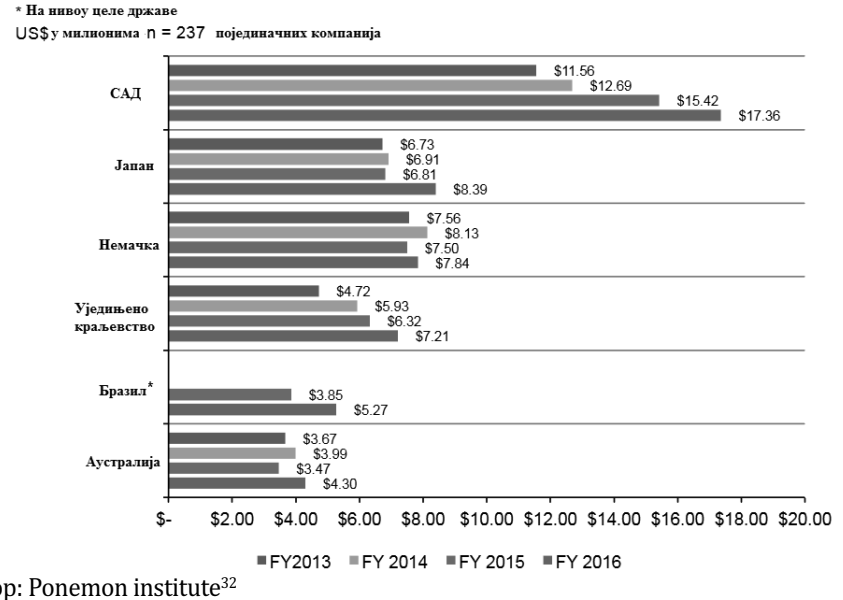
[29] R. Yeager: *Criminal computer forensics management*, Proceedings of the 3rd annual conference on Information security curriculum development – InfoSecCD'06, 2006, p. 168.

[30] Интернет: aicpa.org/InterestAreas/InformationTechnology/Resources/Privacy/GenerallyAcceptedPrivacyPrinciples/Pages/Generally%20Accepted%20Privacy%20Principles.aspx, датум прегледа: 19.3.2017.

3) ПОСЛЕДИЦЕ САЈБЕР НАПАДА НА ПРИВРЕДНЕ СУБЈЕКТЕ

Са порастом важности примене информационих система у пословању саветодавна функција ревизије информационих система постаје све присутнија. Користи се као независно тело које ће снимити стање, уочити критичне тачке, проценити ризике примене информатике у пословању и дати препоруке како тим ризицима управљати. Тиме се, поред статутарне ревизије која је у многим земљама обавезна, ревизија ИС све чешће користи и као аналитичка и саветодавна активност којом се жели побољшати постојећа пословна пракса.[31] Према истраживању *Ponemon* института из САД, у 2016. години повећани су трошкови сајбер криминала. Презентовање трошкова сајбер криминала треба да утиче на привредне субјекте да се определе на инвестирање у области спречавања и ублажавања последица сајбер напада. На слици испод су резултати истраживања из 2016. године. Они показују да у поређењу са претходним годинама постоји пораст сајбер криминала и да је највећи раст у 2016. години био у Бразилу.

Слика 2: Укупни трошкови сајбер криминала у шест земаља у четири године



Извор: Ponemon institute[32]

[31] Марио Спремић, *Сигурност и ревизија информацијских сустава у окружењу дигиталне економије*, Свеучилиште у Загребу, Економски факултет, Загреб, 2017, стр. 196-197.

[32] *2016 Cost of Cyber Crime Study & the Risk of Business Innovation*, Sponsored by Hewlett Packard Enterprise, Independently conducted by Ponemon Institute LLC, Michigan, USA, 2016, p. 4.

Према резултатима истраживања из 2014. године које је спровео Амерички институт овлашћених јавних рачуновођа (*AICPA*), потражња за услугама овлашћених јавних рачуновођа (*CPA*) у форензичком рачуноводству се убрзала. Чак 68% од 5.400 чланова *AICPA Forensics Valuation Services Section* испитаних 2014. године кажу да су се њихове форензичке услуге проширile током претходних година. Од испитаника који су навели повећану потражњу њих 67% је навело израчунате економске штете као водећи разлог за повећану тражњу њихових услуга. Већина испитаника у наредне две до пет година очекује раст потражње за њиховим услугама у овој области између 10 и 50%. Федерални истражни биро *Internet Crime Complaint Center* (IC3) у САД, од 2003. године (од 2000. године до 2003. године – *Internet Fraud Complaint Center*) прима жалбе у вези са *on line* преварама, укључујући преваре у области права интелектуалне својине, компјутер нападе (*hacking*), економску шпијунажу, међународно прање новца, крађу идентитета и друге облике интернет злочина. Да би рачуновође у Индији имале звање „форензички рачуновођа у дигиталној области" морају испутнити неколико захтева: да положе за сертификат (ACFE, огранак у Индији), да похађају курсеве превара *белих оковратника* који преовлађују у САД, на основу њихових закона. Ипак, у Индији не постоји формално тело које пружа образовање од превара. У Индији, према извештају *KPMG* из 2015. године, број сајбер инцидената расте и то доминантно у правцу повећања финансијског сајбер криминала. Испитаници у овом извештају, њих 63%, истичу да су њихови привредни субјекти претрпели финансијски губитак због сајбер криминала.[33] Сајбер криминалци редовно нападају привредне субјекте широм ЕУ. Немачка је највећа жртва ове врсте криминала у финансијском сектору, као и у енергетском и фармацеутском сектору.[34] На основу информација од Интернет провајдера у Великој Британији привредни субјекти су погођени 230.000 пута сајбер нападима у 2016. години.[35] Државна ревизија у Великој Британији процењује трошкове сајбер криминала у Великој Британији између 18 и 27 милијарди фунти годишње.[36] На основу изјаве Америчке агенције за националну безбедност *US National Security Agency* (*NSA*) глобални тршкови компјутерског

[33] *Cybercrime survey report 2015*, KPMG in India, November 2015, p. 8.

[34] *2015 Cost of Cybercrime Study: Global*, Sponsored by Hewlett Packard Enterprise Independently conducted by Ponemon Institute LLC Publication Date: October 2015, p. 10.

[35] Anmar Frangoul, "UK businesses were hit 230,000 times each by cyber-attacks in 2016, says internet service provider", Интернет: http://www.cnbc.com/2017/01/11/uk-businesses-were-hit-230000-times-each-by-cyber-attacks-in-2016-says-internet-service-provider.html, 25.05.2017.

[36] Emmanuel G. Baud et al. "Europe Proposes New Laws and Regulations on Cybersecurity." Jones Day, 1 Jan 2014. Web. 10 Jun 2014. Интернет: http://www.jonesday.com/europe-proposes-new-laws-and-regulations-on-cybersecurity-01-02-2014., 25.05.2017.

криминала процењују се на више од 385 милијарди долара.[37] Највећа глобална претња како наглашава *Ernst and Young* за опстанак приведних субјеката је високотехнолошки криминал. Функција информационе безбедности задовољава потребе само 17% привредних субјеката, 93% привредних субјеката одржава или повећава безбедност. Привредни субјекти морају бити окренути ка будућности и припремити се за нове технологије и заштиту од преварних радњи путем истих.[38] У оквиру PwC глобалног истраживања привредног криминала у 2016. години, интервјуисано је више од 6.300 привредних субјеката из 115 земаља. Три најчешћа облика привредног криминала према извештају из 2016. године су: проневера имовине (64%), сајбер криминал (32%) и на трећем месту подмићивање и корупција (24%).[39] Статистички подаци у овом истраживању обухватили су у Хрватској 47 водећих привредних субјеката из области финансијских услуга, осигурања, инжењеринга, грађевинарства, технологије и производње. У Хрватској 25% анкетираних привредних субјеката било је жртва сајбер криминала (глобални ниво 32%). Упркос наведеној чињеници 22% испитаних привредних субјеката сматра да ће имати сајбер нападе у наредне две године. Мање од половине испитаника (45% привредних субјеката) у Хрватској има припремљен план одговора на инциденте сајбер претњи, а сваки пети привредни субјект (њих 21%) нема ни најмању меру таквог плана. Интересовање привредних субјеката у Хрватској који би ангажовали форензичког истражитеља када се установи превара је само 9% од испитаника у PwC истраживању.[40] Резултати истраживања PwC из 2016. године сајбер криминала у Русији[41] су следећи: само 26% привредних субјеката има план за одговор на сајбер инциденте, 43% привредних субјеката директно брине о сајбер безбедности, 25% компанија сматра да ће бити погођено сајбер криминалом у наредне две године. Ови резултати су засновани на одговорима преко 120 привредних субјеката из Русије. Као најчешће врсте преваре наведене су проневера имовине (72%), преваре приликом набавки (33%), мито и корупција (30%) и сајбер криминал (23%). Како привредни субјекти постају све више ослоњени на информациону

[37] *Net Losses: Estimating the Global Cost of Cybercrime*, Center for Strategic and International Studies. Jun 2014. Web. 18 Jun 2014, p. 6. Интернет: http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf,: 25.05.2017.

[38] *Cyber-crime is greatest global threat to organizations' survival today*, Ernst & Young, 29 Oct 2013; Интернет: http://www.ey.com/lu/en/newsroom/news-releases/news_20131105_cyber-crime-is-greatest-global-threat-to-organizations-survival-today, 26.3.2017.

[39] *Global Economic Crime Survey,* PWC, 2016, p. 9.

[40] Per Sunbye, Martina Butković, Ivana Rapć, „Globalno istraživanje gospodarskog kriminala iz 2016. – Hrvatska Naoružani i spremni za bitku? (Vaši protivnici jesu!)", Интернет. http://www.pwc.hr/hr/forenzicke-usluge/Globalno-istrazivanje-gospodarskog-kriminala-iz-2016-za-Hrvatsku.pdf, 26.3.2017.

[41] *Russian Economic Crime Survey 2016,* PwC Russia 2016.

технологију и све више информација о свом пословању чувају електронски о клијентима, постоје велике могућности да сајбер криминал искористи слабости и недостатке у контролама. Ово је област у којој је Велика Британија испред тренда у свим истаживањима: 44% испитаника у Великој Британији је претрпело привредни криминал у последње две године и били су жртва неке врсте сајбер инцидента (овај проценат је много већи од светског просека од 32% за 2016. годину). Сем тога у 2014. години у Великој Британији тај проценат је био 24%. Овај податак је у складу са другим истраживањима која приказују велики пораст броја детектованих инцидената у Великој Британији у последњих неколико година. Више од половине испитаника у Великој Британији сматра да је вероватно да ће имати нападе сајбер криминалаца у наредне две године, а 71% испитаника виде да је овај ризик повећан током последње две године.[42] Ризик у Великој Британији од превара у економским трансакцијама према процени[43] националне агенције за криминал стално расте, са развојем електронске трговине. Г20 наводе да је Велика Британија највише сајбер зависна економија у групи Г20 земаља. Овај раст је довео до повећања опасности по Велику Британију од сајбер криминала. Сајбер криминал је транснационални феномен и претње у Великој Британији долазе и из унутрашњости и од међународних криминалаца. Према подацима из 2016. године мала правна лица постала су велика мета за сајбер нападе, ово истраживање је спровео Symantec's[44] – *2016 Internet Security Threat Report* је објављено је 2016. године.

Слика 3: Сајбер напади на мала правна лица

Извор: *Symantec's*

[42] *Global Economic Crime Survey 2016: UK report*, PwC UK, 2016.

[43] *National Strategic Assessment of Serious and Organised Crime 2015,* National Crime Agency UK, London, UK, 2051, p. 18.

[44] Symantec, Innovation, Sophistication, Organization – Producing Ominous Results. Интернет: https://www.symantec.com/security-center/threat-report, 26.3.2017.

Мала и средња правна лица у Србији, као и представништва неких иностраних компанија показују огромне недостатке или чак непостојање продецура за сајбер безбедност пословних система. У привредном окружењу наше земље уочава се потреба за систематизованим документом који би понудио решење за ситуације које се дешавају у привредним процесима,[45] везано за сајбер нападе и заштиту од њих од напада изван привредног субјекта и злонамерних упада у оквиру самог привредног субјекта. Према истраживању *Vault Top* R*anked* најбољих десет фирми које се препоручују за форензичку ревизију у 2017. години су:

1. PwC (PricewaterhouseCoopers),
2. Ernst & Young (EY),
3. Deloitte,
4. KPMG,
5. Grant Thornton,
6. BDO USA,
7. RSM US,
8. Crowe Horwath,
9. Baker Tilly Virchow Krause,
10. Moss Adams.[46]

У анализи из 2016. године компанија *Who`s Wholegal – WWL* наводи које су форензичке рачуновође и дигитални стручњаци најистакнутији у овој области.[47] Ови стручњаци су на глобалном нивоу препознати по својим знањима у решавању спорова и регулаторних питања, а неки су препознати по вештинама, *е-знањима*, компјутерској форензици, проналажењу података, анализама за клијенте, заједно са адвокатским фирмама и корпорацијама. Велики значај у овом истраживању имају *Big Four* ревизорске фирме, као и водеће међународне рачуноводствене и консултантске фирме: *FTI Consulting, Grant Thornton, Kroll* и *Berkeley Research Group*. У анализи се појединачно наводе искуства и препоруке стручњака из ове области, имајући у виду да ове компаније послују широм света и да су у стању да понуде клијентима услуге из области: истраживања превара у финансијским институцијама, јавним привредним субјектима, борбе против корупције,

[45] М. Д. Ђекић, „Сајбер процедуре за пословно окружење у Србији", *Техника,* 71(3), 2016, стр. 471-474.

[46] Vault, *2018 Best Accounting Firms for Forensic Accounting.* Интернет. http://www.vault.com/company-rankings/accounting/best-firms-in-each-practice-area?sRankID=418; 26.3.2017.

[47] *Forensic Accountants and Digital Forensic Experts Analysis,* Интернет: http://whoswholegal.com/news/analysis/article/32915/forensic-accountants-digital-forensic-experts-analysis; 26.3.2017.

форензичке истраге и експертизе за електронска открића, компјутерску форензику, питања о информацијама за управљање.

4) САЈБЕР ИНЦИДЕНТИ У МЕЂУНАРОДНИМ И НАЦИОНАЛНИМ И ПРАВНИМ ОКВИРИМА

Националне и међународне организације укључујући *The National Institute of Standards and Technology* (*NIST*)[48] и *The European Union Agency for Network and Information Security* (*ENISA*)[49] објавиле су смернице које имају за циљ да помогну привредним субјектима да реагују на сајбер инцидент. Они пружају детаљне информације за планирање процеса прикупљања и анализирања доказа о преварним активностима које је потребно да форензичар докаже. У Републици Србији Законом о потврђивању конвенције о високотехнолошком криминалу *Службени гласник РС, бр. 19/2009*, потврђена је примена Конвенције о високотехнолошком криминалу, која је усвојена од стране Савета Европе 2001. године у Будимпешти. Будипештанска конвенција представља први међународни споразум о високотехнолошком криминалу. Конвенција је закључена у циљу усклађивања националних права, унапређења истражних метода и сарадње међу државама на пољу сајбер криминала. Додатни протокол уз конвенцију о високотехнолошком криминалу који се односи на инкриминацију радње расистичке и ксенофобичне природе учињених преко рачунарских система, сачињен 2003. године у Стразбуру, Република Србија прихватила је Законом о потврђивању додатног протокола уз конвенцију о високотехнолошком криминалу који се односи на инкриминацију дела расистичке и ксенофобичне природе извшених преко рачунарских система – Службени гласник РС, бр. 19/2009. Европска комисија је донела Директиву 2013/40/ЕУ.[50] Директива о нападима на информационе системе од држава чланица захтева да предвиде својим законодавством кривична дела против информационо комуникационих технологија, да пропишу казнене одредбе, да се одреди кривична одговорност привредних субјеката, као и да се омогући размена корисних информација. ЕУ је 2013. године усвојила Стратегију сајбер безбедности.[51] У Стратегији се истиче да су међународни правни акти у области људских права примењиви и у мрежном, интернет свету. У Републици Србији Закон о инфомационој безбедности – *Службени гласник РС, бр. 6/2016*, дефинише стручне термине из информационо

[48] Интернет: https://www.nist.gov/, 26.3.2017.

[49] Интернет: https://www.enisa.europa.eu/, 26.3.2017.

[50] "Directive 2013/40/EU of the European Parliament and of the Council", Интернет:http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013 :218:0008:0014: EN:PDF , 26.3.2017

[51] *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace.* Интернет: *http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf*, 26.3.2017

комуникационих технологија, одређује безбедност ИКТ система од посебног значаја, препоручује превенцију и заштиту од безбедносних ризика у ИКТ системима у Републици Србији, регулише криптобезбедност и заштиту од компромитујућег електромагнетног зрачења, препознаје инспекцију за информациону безбедност и казнене одредбе. Осигуравајућа друштва у САД и нека у ЕУ увели су полисе за сигурност против сајбер напада. Ове врсте осигурања на захтев привредног субјекта могу садржати хакерске нападе који су довели да производња стагнира, или утичу на лошу репутацију фирме. Ово нас упућује на закључак да и осигуравајућа друштва морају одлично познавати проблематику сајбер напада и откривања друштвено недоличног понашања у сајбер окружењу.

5) ДИГИТАЛНА ФОРЕНЗИКА, ПРАЊЕ НОВЦА И САЈБЕР ТЕРОРИЗАМ

Сајбер тероризам је једна од највећих претњи данашњем савременом окружењу. У овом делу рада навешћемо модалитете прања новца које користе терористичке организације за стицање средстава у вези финансирања сајбер тероризма. За формирање инфраструктуре и извођење терористичких инцидената у сајбер простору један од најважнијих услова представља поседовање легалних финансијских средстава. Терористичке организације финансијска средства стечена различитим типологијама прања новца уводе у финансијски систем скривањем намене новца за организоване терористичке сајбер нападе. На светском нивоу због проблема прања новца у сајбер простору и финансирања тероризма, уводе се превентивни механизми кроз сарадњу финансијско обавештајних служби земаља које подржавају ову борбу и кроз њихову сарадњу са међународним оргнизацијама које се баве овом проблематиком. Финансирање сајбер тероризма пролази кроз процес прања новца. Процес прања новца за финансирање сајбер тероризма пролази кроз три фазе: улагање, раслојавање и интеграција. ОЕЦД идентификује ове три фазе прања новца, али фазу интеграције дели у две подфазе и то: оправдање и инвестиције.[52] Наведене фазе прања новца препознала је и *FATF* група (*the Financial Action Task Force*[53]) која је успоставила стандарде и бави се имплементацијом правних и оперативних мера за превенцију и сузбијање прања новца и финсирања тероризма. Широм света земље које подржавају борбу против прања новца прихватиле су смернице и међународне стандарде *FATF-a*. Манивал (*Moneyval*)[54] је регионално тело слично *FATF-y*. Бави се

[52] *Money Laundering Awareness Handbook for Tax Examiners and Tax Auditors*, OECD, 2009, p. 11.

[53] Интернет: http://www.fatf-gafi.org/, 26.3.2017.

[54] Council of Europe, Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism, Интернет: http://www.coe.int/t/dghl/monitoring/moneyval/, 26.3.2017.

проценом система за борбу против прања новца и финансирања тероризма у земљама чланицама Савета Европе, које нису чланице *FATF-a*. Од 2003. године Република Србија је члан система Манивал у оквиру борбе против прања новца и подлеже процени тог тела. Управа за спречавање прања новца Републике Србије, као финансијско обавештајна служба је чланица Егмонт групе (удружење финансијско обавештајних служби) од 2003. године.[55] Циљ Егмонт групе је унапређење међународне сарадње и размена података у области прања новца и финансирања тероризма. Ово је посебно важно за базе података регистрованих терориста и терористичких организација, за успешну борбу против прања новца и финансирања тероризма.[56] По питању сајбер криминала и сајбер тероризма огласио се и Интерпол (*INTERPOL*) препознајући их као једну од глобалних претњи и активно се прикључио у борбу против прања новца и финансирања тероризма.[57] Северноатлантски пакт (НАТО)[58] усвојио је Сајбер стратегију препознавши сајбер претње као објективну опасност по државе чланице, али и по саму организацију. У порасту је број билатералних споразума држава о сарадњи на овом пољу, попут Русије и Израела, или Бразила и Аргентине.[59] Истраживање по налогу немачког Министарства финансија које је спровео *Halle-Wittenberg* универзитет истиче да се у Немачкој износ прања новца у финансијском и нефинансијском сектору годишње креће око 100 милијарди евра.[60] Ова студија истиче да се на продручју трговине некретнинама и уметничким делима годишње идентификује од 15 до 28 хиљада сумњивих трансакција, којима се утиче на трансакције прања новца. Са аспекта прања новца у Републици Србији највећи ризик по питању имовинске користи проистекле од извршених дела у овом пољу, као високо ризична кривична дела окарактерисани су пореска утаја, неовлашћена производња и стављање у промет опојних дрога и кривично дело злоупотребе службеног положаја.[61] Према Националној процени ризика од прања новца у Републици Србији недостатак система чини нејединственост статистика (или се уопште не воде), непостојање електронског уписа података и неумреженост

[55] Интернет: https://www.egmontgroup.org/, 26.3.2017.

[56] Жаклина Спалевић, Жељко Спалевић, „Стање сервиса електронске управе базираних на рачунарству у облаку", *Култура полиса,* година XIV, посебно издање, Нови Сад, 2017, стр. 171-183.

[57] Интернет: https://www.interpol.int/, 26.3.2017.

[58] Интернет: http://www.nato.int/, 26.3.2017.

[59] К. Јонев, „Сајбер тероризам и употреба сајбер простора у терористичке сврхе", *Безбедност*, Београд, 58(2), 2016, стр. 206-222.

[60] Интернет: http://www.uni-halle.de/, 26.3.2017

[61] *Национална процена ризика од прања новца у Републици Србији,* Савет Европе, Канцеларија у Београду, 2013, стр. 15.

информационих система и база података на нивоу државних органа. Према овој процени најрањивији у оквиру финансијског сектора са високим ризиком прања новца су банке, а у нефинансијском сектору висок степен ризика је промет некретнина. Манивал је при Савету Европе објавио саопштење у 2016. години којим се Босна и Херцеговина ставља на „црну листу" заједно са Украјином, Северном Корејом и Ираном, због неиспуњавања обавеза према Акционом плану *FATF-a* у области мера увођења стандарда за спречавање прања новца и финансирања тероризма.[62] Из анализе прикупљених података у Хрватској следећа кривична дела представљају највећу претњу за кривично дело прања новца: корупција (злоупотреба поверења у привредном пословању, злоупотреба положаја), утаја пореза и царине, злоупотреба опојних дрога.[63] Према Националној процени ризика од прања новца и финансирања тероризма у Републици Хрватској, процена способности одупирања ризицима од прања новца на националном нивоу је средња. Главне рањивости према овој процени у националној способности да се супротстави ризицима од прања новца су: недостаци техничких (потребно је јачање информатичке инфраструктуре) и административних капацитета (повећање броја аналитичара у Уреду за спречавање прања новца Републике Хрватске, повећање броја финансијских истражитеља), мали број покренутих кривичних дела за прање новца, неадекватно вођење службене статистике о међународној сарадњи и кривичним делима. Сложеност и глобална повезаност данашњег пословног окружења резултирали су растућом потражњом за осигурањем информација које су обелодањене поштено и тачно.[64] Поред сталног праћења и преиспитивања ризика од прања новца и финансирања тероризма, потребно је да привредни субјекти поседују функцију интерне ревизије да би имали независну процену система управљања ризиком од прања новца и финансирања тероризма. Ову независну ревизију могу да спроводе интерни и екстерни ревизори, стручни консултанти или дуга квалификована лица која нису непосредно ангажована на примени или у функцији управљања ризиком од прања новца и финансирања тероризма у привредном субјекту.[65]

---

[62] Council of Europe, Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism, Интернет: http://www.coe.int/t/dghl/monitoring/moneyval/, 26.3.2017

[63] *Nacionalna procjena rizika od pranja novca i financiranja terorizma u Republici Hrvatskoj*, Međuinstitucionalne radne skupine za sprječavanje pranja novca i financiranja terorizma (MIRS), Zagreb, 2016, стр. 12

[64] Косана Вићентијевић, „Нова форма и садржај извештаја независног ревизора", *Ревизор,* година XX, бр. 77/2017, Институт за економику и финансије, Београд, 2017, стр. 37-48.

[65] *Смернице за процену ризика*, Савет Европе, Канцеларију у Београду, 2013, стр. 25.

6) ЗНАЧАЈ ЗА РЕПУБЛИКУ СРБИЈУ

Иако расту потребе за заштитом и превенцијом сајбер превара, привредни субјекти не ангажују довољно дигиталне форензичаре. Могући разлози су: услуге су захтевне и превазилазе финансијске могућности клијента да их исфинансира, недовољна је информисаност и сазнање о услугама које су доступне. Сем тога, све више привредних субјеката у својој организационој структури има *fraud* одељење, па је и то могући разлог мањег екстерног ангажовања дигиталног форензичара рачуновођа. Не треба занемарити ни чињеницу да у условима претрпљене штете по основу превара које нису материјално значајне правна лица су спремнија да прећуте ту информацију како не би нарушила своју репутацију. Поред откривања сајбер превара, израчунавања износа преварне радње, извештавања о истражном поступку, дигиталне форензичке рачуновође имају саветодавну улогу превентивног карактера да се сузбију незаконити поступци и преваре, да се сачува репутација компаније. У том правцу потврђујемо да је дигитална форензика у рачуноводству у сајбер окружењу интердисциплинарна јер обједињује знања из области рачуноводства, форензичког рачуноводства, интерних контрола, пореског и кривичног права, информационих технологија. Форензички експерти из рачуноводства у дигиталном окружењу спремни су да пруже следеће услуге корпоративним клијентима: истраге финансијских превара, превенцију и сузбијање превара, управљање ризицима преварних радњи, процене губитака и прорачуни опоравка од преваре, саветовања у вези спречавања превара и друге активности у правцу *anti-fraud* за компаније.