Review Scientific Paper/Pregledni naučni rad
Paper Accepted/Rad prihvaćen: 21. 1. 2019.
doi:10.5937/SJEM1901009L

UDC/UDK

004.738.5.056:316.62
159.9.019.4-057.87

Sajber maltretiranje, online ponašanje i psihološka dobrobit studenata: pristup inženjerskog menadžmenta

Nikolina Ljepava ^{1*}, Duško Tomić ², Dženana Nuhodžić ³ Marko Gnjatović ⁴

¹ American University in the Emirates, Dubai, UAE, nikolina.ljepava@aeu.ae;

² American University in the Emirates, Dubai, UAE;

³ Univerzitet Mediteran, Podgorica, Crna Gora;

⁴ Fakultet za inženjerski menadžment, Beograd, Srbija.

Apstrakt: Široko rasprostranjena upotreba informacionih i komunikacionih tehnologija postala je sastavni deo naših života u proteklih dvadeset godina, posebno u okviru mlade generacijske kohorte. Kako su tehnologije integrisane u naše svakodnevne rutine, kriminalna ponašanja su takođe prešla granice fizičkog sveta, stvarajući područje koje se pojavljuje na internetu. Sajber zlostavljanje je identifikovano kao jedan od kontinuirano rastućih problema u školama i univerzitetima širom sveta i brojne studije su pokazale značajne odnose između internetskog zlostavljanja i psihološkog zdravlja, posebno mentalnog zdravlja i problema u ponašanju. Teorija rutinskih aktivnosti (Cohen & Felson, 1979) sugerise da svakodnevne aktivnosti pojedinaca direktno utiču na viktimizaciju, što nekim pojedincima povećava rizik da budu žrtve. Sa obimnom, svakodnevnom upotrebom interneta i pametnih telefona, mladi ljudi su pod povećanim rizikom da budu izloženi nekom obliku internetskog zlostavljanja. Stoga, treba da se implementiraju preventivni programi na svim nivoima kako bi se mladi bolje obrazovali o bezbednom ponašanju na internetu i smanjili rizik da postanu žrtve internetskog nasilja.

Ključne riječi: internetsko zlostavljanje, online ponašanje, rizično ponašanje, teorija rutinskih aktivnosti.

Cyberbullying, online behavior, and the students' psychological well-being: An engineering management approach

Abstract: The widespread use of information and communication technologies became an integral part of our lives in the past twenty years, especially within the young generational cohort. As technologies are integrated in our daily routines, the criminal behaviors also crossed the boundaries of the physical world, creating an emerging area of online offenses. Cyberbullying has been identified as one of the continuously increasing problems in schools and universities worldwide and numerous studies have demonstrated significant relations between cyberbullying and psychological well-being, specifically mental health, and behavioral problems. Routine Activities Theory (Cohen & Felson, 1979) suggests that an individual's day-to-day activities have a direct impact on victimization, placing some individuals at increased risk of being victimized. With the extensive, daily use of the Internet and smartphones, young people are at increased risk to be exposed to some form of cyberbullying. Therefore, the prevention programs should be implemented at all levels to educate youth better about safe online behaviors and decrease the risk of becoming the victims of cyberbullying.

Keywords: cyberbullying, online behavior, risk behavior, routine activity theory

1. Introduction

The impact of the technological development on our everyday life and activities has been increasing in the past twenty years. Various Internet-enabled services are used daily by billions of individuals worldwide; we live in the continuously connected society with our mobile devices serving as the primary device for gathering information and communications (Kotler, Kartajaya, & Setiawan 2017). Cyberspace, the new social environment with numerous possibilities for various activities and social interactions was created, and in a relatively short period, the Internet became a place to communicate, interact, socialize, and entertain. Nevertheless, with these advancements, criminal behaviors also crossed the boundaries of the physical world, creating an emerging area of online offenses (Jaishankar, 2011; Reyns, Hanson, & Fisher, 2011; Whitaker & Kowalski, 2015, Weulen Kranenbarg, Holt, & van Gelder, 2019).

With the continuous increase in the use of the Internet and particularly mobile technologies and smartphones, the prevalence of technology-related crimes is also quickly increasing (Jones, Mitchell, & Finkelhor, 2011, Eustace et al., 2018). From online fraud, identity theft, and computer viruses to cyberbullying, cyber harassment, and cyberstalking, a whole new area of cyber-crimes has emerged in this new online environment.

According to Jaishankar (2011), there are two types of technology-related crimes: (a) "cyber crimes" that rely on specialized knowledge (e.g., bank frauds, identity thefts) and (b) "computer crimes," which are criminal offences facilitated by using technologies, but are unrelated to technological knowledge (e.g., cyberbullying, harassment, child pornography). To explain the occurrence of the technology-related crimes, Jaishankar (2007) argued that individuals behave differently in different spaces, and that, cyberspace gives individuals an opportunity to exhibit behaviors that would not otherwise be displayed in real life.

Bullying among school-aged children is not a new trend; it is a widespread social phenomenon that has been here for generations. According to Olweys (1994), bullying was not systematically studied until the late 1970s, when social scientists in Scandinavian countries started to research the incidence of bullying among elementary school students. Soon after that, bullying was recognized as an important social phenomenon in the school environment and became the topic of research in numerous countries. Bullying can cause intense physical, emotional and psychological harm to a victim, and emotional difficulties associated with bullying can have a potential long-term adverse outcome for the psychological health and self-esteem of the bullied individuals since in many cases effects of bullying do not disappear with time. Additionally, the number of studies has shown that bullies are more likely to express criminal and anti-social behavior later in life, comparing to their peers who never bully. Olweys (1984) argued that bullies have 37% more chance to commit offenses compared to their peers.

According to the US Department of education (2018), around 20% of the school-aged children are exposed to some type of bullying in school. This number decreased within the past ten years, indicating that the number of interventions conducted systematically in middle and high schools was successful. Nevertheless, according to the most recent Ipsos research (2018), performed with the parents of the school-aged children the prevalence of cyberbullying worldwide is continuously increasing, and more and more school-aged children have been exposed to some form of cyberbullying.

2. Cyberbullying: A New Form of Bullying

With the recent development of technology and the Internet and widespread usage of smartphones, an increasing number of young people is utilizing technology to communicate, socialize, and interact. In 2005 87% of the children in the USA, aged 12-17 years used the Internet daily and 45% owned cell phones (Lehart et al. 2005); since that time these numbers have increased both in the USA and globally. Mobile phones and social networking applications are becoming an integral part of youth and children everyday activities, used for communication, information and maintaining social relationships. According to Parasuraman et al. (2017), around 50% of teenagers think that they are addicted to their smartphones. The online environment became quickly one of the leading social settings for the youth, place where they communicate, interact and entertain. Consequently, both positive and negative social interactions crossed the boundaries of the physical to the virtual world, opening some new questions and dilemmas for parents, teachers, and researchers.

One of the anti-social behaviors that found its way into the virtual world is bullying; online activities of digital age bullying among youth, recognized in the literature as "cyberbullying." Cyberbullying is defined as "an aggressive, intentional act carried out by a group or individual, using electronic forms of contact, repeatedly against a victim who cannot easily defend him or herself." (Smith et al., 2006, pg 376). A variety of technological mediums provide some different opportunities for cyberbullying. Threatening or embarrassing emails, videos, instant messages, photos, and SMS can be sent through smartphones, tablets or computers. Additionally, social networks also provided a suitable environment for different ways of cyber-bullying. There is now the increased range of audience that can witness cyberbullying (e.g., on Facebook, YouTube, Twitter) leading to increased public embarrassment, that might intensify the impact of cyberbullying and harm inflicted on victims (Wright, 2017).

Having in mind that physical bullying is not a component of cyberbullying one can ask why cyberbullying is considered to be so dangerous. As with any other form of bullying, cyberbullying can cause emotional and psychological harm to the victim (Livingstone, Stoilova, & Kelly, 2016). However, while traditional bullying was usually limited to a particular physical environment, cyberbullying has a broader scope; with current technology devices such as cell phones and mobile Internet, a teenager can be continuously bullied.

Looking at the body of research dedicated to cyberbullying, it can be argued that cyberbullying can occur in two forms - verbal and social cyberbullying. Verbal cyberbullying is perpetrated by sending threatening, offensive, and aggressive verbal messages. Additionally, cyberstalking can also be viewed as a type of verbal cyberbullying. Social cyberbullying, on the other hand, is the form of cyberbullying targeted towards social defamation of the victim with the primary goal of either publicly humiliating the victim or inducing problems in the personal or social life of an individual. Social bullying can be perpetrated by rumours spreading, social exclusion, or by online dissemination of private photos and/or video materials of the victim. Both types of bullying can be perpetrated at the same time or separately, and they can be conducted by a single individual or by a group of individuals.

In addition to socio-demographic and psychological factors, some studies have also examined individuals' online behaviors as predictors of cyber victimization. Some online behavior such as online gaming was not found to increase the risk of cyber victimization significantly; however, participation in online social networking websites, especially Facebook, was predictive of cyberbullying (Mesh, 2009). Morrison and Gore (2010) found that individuals with symptoms of Internet addiction are more inclined to participate in social networks, online chats, and other types of online socializing. Additionally, they have found social networks users to be more likely to reveal their personal information and to engage in conversation with unknown individuals. Moreover, individuals using instant messaging (chat) programs were also more likely to become victims of cyberbullying (Maple, Short & Brown, 2011; Wright, 2017). Using a sample of 120 American undergraduate students, Walker, Sokhman, and Koehn (2011) found that the majority of respondents who had experienced cyberbullying reported that bullying was perpetrated via Facebook or instant messaging programs. Similarly, Lindsay and Krysik (2012) also reported that social network use among American university students in their sample increased students' risk of online harassment. Thus, as can be seen, the amount of time and how individuals use the Internet also need to be considered when assessing the risk of cyber victimization.

The Impact of Cyberbullying on Psychological Well-Being

In addition to associations with age, gender, education, and income, some studies have demonstrated significant relations between cyber victimization and psychological well-being, specifically mental health, and behavioral problems. Cyberbullying has, for instance, been linked with a higher incidence of depression and suicide attempt, especially among adolescents (Morrison & Gore, 2010). Research conducted by Schenk (2011) on college students similarly indicated that victims of cyberbullying scored higher on depression, anxiety, and distress scales, reported feeling sad and angry more often, and endorsed significantly more suicidal planning and ideations compared to those that did not experience cyberbullying. Results from the study further indicated that cyberbullying had a negative psychological impact on victims and that exposure to cyberbullying might have serious implications for individuals' psychological health (Schenk, 2011; Cowie 2013).

Other research by Zu, Lee, Ning, and Guan (2011) predicted participants' mental health status based on the individuals' web usage behaviour using Song and Mo's (1992) Psychological Health Inventory, which measures seven dimensions of mental health, including depression, anxiety, psychopathic deviate, hypochondria, being unrealistic, and hypomania. They found all seven dimensions of mental health to be predictive of participation in online discussions, such that higher scores on the mental health subscales predicted more usage of instant messaging programs and a greater overall amount of time spent online. Similarly, in a study of 2,114 Taiwanese high school students conducted by Yen et al. (2007), mental health symptoms were found to relate to increased levels of Internet use, with depression being an especially strong predictor for girls. These results are consistent with Morison and Gore's (2010) findings from an online study conducted in the UK that explored the relationship between excessive Internet use and depression in a sample of 1,319 young people and adults. Morison and Gore (2010) found that participants who showed signs of Internet addiction exhibited significantly more depressive symptoms compared to moderate Internet users.

When considering the stressful nature of cyberbullying, all types of cyberbullying have been found to inflict a considerable amount of stress on victims. For instance, research conducted by Ybarra and Mitchell (2007) showed that 38% of participants stated that cyberbullying caused them severe emotional distress. Why is cyberbullying so stressful? Whereas traditional bullying and stalking are usually limited to a specific physical environment (e.g., school playgrounds or school buses), cyberbullying has a broader scope. That is, with present-day technological devices such as cell phones and mobile Internet, an individual can be continuously bullied. This constant bullying can inflict additional stress and pressure on victims, causing feelings of helplessness and the perception that they have nowhere to hide from the abuse. Public defamation in an online environment can affect an individual's self-perception and self-esteem, causing depression and suicidal ideation (Ruedy, 2008). In recent years, cyberbullying has resulted in many suicides in North America as well as across the globe, opening discussions among law practitioners about the introduction of specific legal repercussions against cyberbullying.

Moreover, online environments do not provide bullies the opportunity to observe their victims' reactions to the bullying behavior, thus minimizing the sense that real harm has been inflicted on their victims, and in turn, potentially making the bullying behaviour even harder to stop (Bhat, 2008). Given that there is no physical contact between the victim and the cyberbully, the seriousness of the cyberbullying is sometimes underestimated; however, there are some indications that cyberbullying behaviors can, in some cases, lead to real life violence (Bocij, 2005).

In sum, numerous studies have demonstrated a relationship between various forms of cyberbullying, online user behaviours, and poor mental health outcomes. What is perhaps most concerning about these findings is the potential for mental health problems to have indirect effects on cyber victimization by influencing patterns of online behaviour and heightening individuals' risk of being victimized by increasing the amount of time spent online. Thus, in addition to the negative impact that cyber victimization might directly have on victims' mental health, there is the potential that victims' online behaviors might also be impacted by the victimization, which in turn, could place them at further risk of future victimization and subsequent mental health problems.

Routine Activities Theory and Cyberbullying

Routine Activities Theory (Cohen & Felson, 1979) has been applied to explain cyber victimization. This theory suggests that an individual's day-to-day activities have a direct impact on victimization, placing some individuals at increased risk of being victimized. Moreover, this theory also suggests that for victimization to occur, three preconditions need to be satisfied: there needs to be a motivated offender, the opportunity for victimization (suitable target), and the absence of a capable guardian. Proponents of Routine Activities Theory argue that for a crime to take place, all three factors need to be present; if even one element is missing, violent crime cannot be perpetrated (Cohen & Felson, 1979).

Routine Activities Theory explains criminal victimization based on direct physical contact between perpetrators and victims. It emphasizes that victimization happens when motivated offenders and suitable targets are placed in environments suitable for the criminal offense. It further states that due to the routine activities of some individuals, these individuals can be at increased risk of being victimized.

Thus, because daily use of Internet has become a routine behaviour for majority of young individuals in the modern world, it could be argued that regular Internet users are increasing their risk of online victimization (Jaishankar, 2011; Reyns, 2010). While conducting these routine activities online, an individual (i.e., the suitable target) can become a victim of a motivated offender in the absence of guardianship (i.e., lack of antivirus or antispy software).

Alshalan (2006) analyzed the National Cyber Crime Victimization Survey data collected in the USA in 2004. He found measures of the routine online activities to predict both computer virus victimization and cybercrime victimization. Reyns (2010) explored the relationship between several types of online behaviors and victimization on the Internet. He found that the number of online social networks that participants used, the number of daily updates participants made on social networks (e.g., status updates on Facebook, tweets on Twitter), communication with strangers online, and engaging in any deviant online behavior significantly predicted cyber victimization.

Navarro and Jasinski (2011) found the Routine Activities Theory to be the viable explanation for cyberbullying risk among teenagers, with suitability and availability being the highest risk factors for teenagers' exposure to cyberbullying.

3. Conclusion

Although cyber safety and cyberbullying seem to be essential issues in the modern information society, with the young people spending more and more time in online activities every year, there are still no official cyber safety and cyberbullying awareness programs in numerous countries. Primary education about cybersecurity and cyberbullying should be incorporated in school curriculums as suggested in the literature (Diamanduros & Downs, 2008), and specific prevention and intervention programs that would address those problems should be developed (Ljepava, 2011). Moreover, both school and university officials and parents should be provided with additional information and training about these issues, to raise awareness about cyberbullying and minimize its negative consequences.

Some successful examples of interventions in traditional bullying in literature have shown that with appropriate intervention programme the incidence of bullying in the school environment can decrease. Having in mind the same theoretical concepts behind both cyberbullying and traditional bullying, there is no reason for cyberbullying to be different. Bullying can be reduced if it is acknowledged as a problem and if there is a specific strategy to deal with it. In the case of cyberbullying, it is the lack of knowledge about the topic, about online communication and use of technology that is a problem.

Educational institutions should adopt cyberbullying prevention programs and parents, teachers, school and university psychologist, and councilors need to pay more attention to this kind of harassment. Wider society involvement in the prevention of all forms of bullying including the cyberbullying and to involve in the problem is crucial in order to make a difference in the next period and often prevent devastating consequences of cyberbullying.

Literature

1. Agathston, P., Kowalski, R., Limber, S. (2007). Student perspective on cyber bullying. *Journal of Adolescent Health* 41, 59-60.
2. Allen, K.P., (2010). A bullying intervention system: Reducing risk and creating support for aggressive students. *Preventing School Failure* 54(3), 199-209
3. Bhat, S. C., (2008). Cyber bullying: Strategies for school counsellors, guidance officers and all school personnel. *Australian Journal of Guidance and Counselling* 18(1), 53-66.
4. Campbell, M. (2005). Cyber bullying: An old problem in a new guise? *Australian Journal of Guidance and Counselling* 15(1). 68-76. Retrieved 01-10-2018 from: <http://www.atypon-link.com/AAP/doi/pdf/10.1375/ajgc.15.1.68?cookieSet=1>
5. Cowie, H. (2013). Cyberbullying and its impact on young people's emotional health and well-being. *The Psychiatrist*, 37(5), 167-170.
6. Diamanduros, T., Downs, E. (2008). The role of school psychologists in the assessment, prevention, and intervention of cyberbullying. *Psychology in the Schools*, 45 (8), 693-704.
7. Eustace, K., Islam, R., Tsang, P., & Fellows, G. (2018). Human Factors, Self-awareness and Intervention Approaches in Cyber Security When Using Mobile Devices and Social Networks.

- In *Security and Privacy in Communication Networks: SecureComm 2017 International Workshops, ATCS and SePrIoT, Niagara Falls, ON, Canada, October 22–25, 2017, Proceedings 13* (pp. 166-181). Springer International Publishing.
8. Hinduja, S., & Patchin, J. (2006). Bullies move behind schoolyard: A preliminary look at cyber bullying. *Youth Violence and Juvenile Justice*, 4 (2)148-169.
 9. Kotler, P., Kartajaya, H., & Setiawan, I. (2017). Marketing 4.0: Moving from traditional to digital.
 10. Kowalski, R. M., Limber, S.P., (2007). Electronic bullying among middle school students. *Journal of adolescent health* 41(6), 22 -30.
 11. Lenhart, A., Madden, M., & Hitlin, P. (2005). Teens and technology. Washington, DC: Pew Internet & American Life Project. Retrieved November 14, 2018, from <http://www.pewinternet.org/Reports/2005/Teens-and-Technology.aspx>
 12. Livingstone, S., Stoilova, M., & Kelly, A. (2016). Cyberbullying: incidence, trends and consequences.
 13. Ljepava, N. (2011). Realno zlostavljanje u virtuelnom okruzenju: Prevencija i intervencija u slucajevima zlostavljanja dece na Internetu. *Aktuelnosti* (1-2), 22-33.
 14. Mesch, G. (2009). Parental mediation, online activities and cyber bullying. *Cyberpsychology and Behaviour*, 12(4), 387-393.
 15. Navarro, J. N., & Jasinski, J. L. (2012). Going cyber: Using routine activities theory to predict cyberbullying experiences. *Sociological Spectrum*, 32(1), 81-94.
 16. Nansel, T. Overpeck, M. Pilla, R. Ruan, W., Simons-Morton, B. & Scheidt, P. (2001). Bullying behaviours among US youth: Prevalence and association with psychosocial adjustment. *Journal of the American Medical Association*, 285, 2094-2100.
 17. Olweus, D. (1994). Bullying at school: Basic fact and an effective intervention programme. *Promotion and Education*, 1(27), 27-31.
 18. Ruedy, M. (2008). Repercussions of My Space teenage suicide: Should anti-cyberbullying laws be created? *North Carolina Journal of Law and Technology*, 9(2), (323-346).
 19. Shariff, S. (2005). Cyber dilemmas in the new millennium: School obligation to provide student safety in a virtual school environment. *McGill Journal of Education*, 40(3)
 20. Smith, P.K., Mahdavi, J., Carvalho, M., Fisher, S., Russell, S., & Tippett, N. (2008). Cyberbullying: Its nature and impact in secondary school pupils. *Journal of Child Psychology and Psychiatry*, 49(4), 376–385.
 21. Whittaker, E., & Kowalski, R. M. (2015). Cyberbullying via social media. *Journal of School Violence*, 14(1), 11-29.
 22. Wright, M. F. (2017). Cyberbullying: Bullying in the Digital Age. In *Handbook of Research on Individualism and Identity in the Globalized Digital Age* (pp. 50-70). IGI Global.
 23. Weulen Kranenbarg, M., Holt, T. J., & van Gelder, J. L. (2019). Offending and victimization in the digital age: Comparing correlates of cybercrime and traditional offending-only, victimization-only and the victimization-offending overlap. *Deviant Behavior*, 40(1), 40-55.

IT rešenja u upravljanju ljudskim resursima

Brankica Pažun¹, Irena Rašević², Ognjen Rakić²

¹ School of Engineering Management, University Union – Nikola Tesla, Belgrade,
brankica.pazun@fim.rs;

² INAT Centre, Belgrade.

Sažetak: Informacioni sistemi imaju sve veći uticaj na moderno poslovanje. Brzo menjaju poslovne sisteme i postojeće poslovne modele. Upravljački pristup je od suštinskog značaja za sve poslovne sisteme i podsisteme, kao npr. ljudske resurse, ako žele da opstanu, ali danas sve faze procesa upravljanja ne mogu da se odvijaju bez podrške informaciono-komunikacionih tehnologija. Brze i velike promene u okruženju u kojem je poslovanje praćeno neizvesnošću i rizikom, dovode do potrebe za primenom adekvatnih tehnologija u cilju povećanja fleksibilnosti, preciznosti, kao i eliminisanju ili smanjenju pojave grešaka koje umanjuju vrednost poslovne aktivnosti. Sve upravljačke aktivnosti se zasnivaju na razmeni podataka između eksterne i unutrašnje sredine, tako da na osnovu tačnih informacija menadžeri mogu da kontrolišu postizanje cilja. Proces globalizacije nameće pravila igre, dok znanje i informacije određuju poslovni sistem unutar organizacija. Informaciona tehnologija je ključni faktor koji omogućava menadžerima da upravljaju rizikom i zadovolje zahteve turbulentnog okruženja. Ovaj rad ukazuje na mogućnosti primene savremenih IT rešenja u upravljanju ljudskim resursima, analizirajući njihove prednosti i nedostatke.

Ključne reči: HR softver otvorenog koda, informacione tehnologije, poslovni sistemi, upravljanje ljudskim resursima

IT solutions for human resources management

Abstract: Information systems have a growing impact on modern business. They rapidly change business systems and existing business models. Management approach is essential to all business systems and subsystems, i.e. human resources, if they want to survive, but today all phases of the management process cannot take place without the support of information and communication technology. Rapid and large changes in the environment in which business is accompanied by great uncertainty and thus a huge risk, lead to necessity for applying adequate ICT that would increase flexibility, precision and eliminate or reduce errors' occurrence that diminish the value of business activity. All management activities are based on information flow of external and internal environment, so on the basis of accurate information managers could control the attainment of the objective. Globalization process imposes game rules; further, knowledge and information determine business system within organisations. Information technology is the key factor that allows managers to manage risk and meet demands of a turbulent environment. This paper emphasizes the possibility of applying contemporary IT solutions in human resources management, analyzing their advantages and disadvantages.

Key words: business systems, open source human resource management systems, human resource management, information technologies

1. Introduction

It is a common fact that everyone in the business system should work together to meet needs of the customer (beside profit), which means that profitable business, among other things, requires money, information, human resources and ways for obtaining or producing goods and services. Information technology plays an important role because it affects the business system as a whole, as well as many other functions within the company.

With the advent of the information society, human resources management with performing managerial tasks related to personal issues, employment, training, assessment etc. (Dessler, 2015), has undergone major changes. First of all, due to the emergence of the Internet and new jobs, human resources had to evolve and transform themselves digitally. Software solutions have become an indispensable part of human resources management and have greatly accelerated the recruitment process and reduced the need for additional paperwork.

Open source software today is an ideal solution for newly-opened business ventures, as well as for small or medium-sized enterprises. Open source software (according to Opensource) are most often free solutions, i.e. (according to Free), but they can be partially free, (according to Freemium). Nowadays, the difference in the benefits provided between the licensed software and the open source software is being reduced.

Cloud computing does not represent a passing mode, nor a revolution in electronic commerce. Instead, most companies are likely to use a combined IT environment in which applications, infrastructure, and business processes will be implemented through public and private CCs, and possibly using a hybrid cloud model. In any case, the undeniable fact is that CC changes existing business models.

2. New technologies in business environment

The growth rate of data is large, so economy i.e. the business environment presents a very large amount of data that creates the need for strong and modern information systems. The upper layers of information systems are directly related to functions of business systems, therefore, concepts' relations Big Data, Cloud computing and IoT system, are defined.

Cloud computing is present everywhere in the modern business environment. Cloud-based HR systems give businesses the computing power and the ability to survive today. There are advantages in using cloud HR software, such as less paperwork, fast deployment of HR systems, security issues, increased employee engagement, real-time and accurate performance assessments, 24/7 access to pay and benefit information, giving companies easy access to innovation, predictive analytics that promotes employee retention and loyalty, etc.

In the business environment Big Data concept represents vast and complex amounts of data. One of infrastructure solutions of above mentioned concept is a combination of the analytical platform Hadoop with NoSQL system. Big Data provides the ability to process data in real time, with searching option using the Map Reduce framework. For example, Big Data systems allow analytical processing of data collected on planning, organizing, staffing, directing, controlling, recruiting, placement, performance appraisal, compensation and training, etc. The resulting knowledge is transferred to managers, in order to define decisions/ strategies. Big data could be a part of a complex advanced analytical system, which is a solution.

Figure 1: Big Data - holistic approach

Source: (VMware, 2016)

Further, according to the Economist Intelligence Unit, the research and analysis division of the Economist Group and the world leader in global business intelligence, it is found that 82% of organizations planned to either begin or increase their use of big data in HR before the end of 2018. (Economist Group, 2018)

As Cloud and Big Data platforms, the IoT concept (Internet of Things) becomes increasingly common in the business environment. These are devices called „things“ which in their structure have processor systems and other components, with the possibility of data exchanging. Predictions of the International Corporation for data analysis (International Data Corporation - IDC) are that by the year 2018 about 40% created IoT data will be stored, manageable and used by systems that are near or at the network edge. (Langovic, Pazun, 2016)

3. Open source software for human resource management

Nowadays open source human resource management systems (HRMS) become very popular concept even still relatively young. They give a lot possibilities or alternatives for human resource management, as well as become more competitive to Oracle and SAP, market leaders in this field.

Following open source business software applications for human resource management will be explained.

Orange HRM software. Orange HRM software is open source software, web-oriented. It has a user-friendly experience and a very wide range of tools that facilitate the work of human resources management. Given software has a trial period of thirty days, after which it should be paid. This software solution uses over 3,500,000 users. Many users state that its main advantage is its user-friendly experience.

Open source ERP software. Open source ERP software is also an open source software that is web-oriented and there is no need for installation, as well as it is designed for all types of businesses. Given software is free. Its advantages are the database and transparency of personal data. This software is mainly used by companies that are only starting up and whose number of employees is up to 100.

Odoo software. Odoo software is open source web-oriented software, which is partially free, that is, the first wanted application is free, and others are paid. In other words given software is an example of a freemium model. For human resources, it offers several solutions which cover recruitment, staffing, costs, assessment, fleet, and absenteeism. Each of these solutions has its own application. This software is ideal for all types of companies. It has 3,000,000 users.

HR.my software. HR.my open source software is completely free. This software does not require installation and it is web-oriented. It has a pleasant user experience, as well as excellent opportunities, such as electronic tracking of absenteeism, enhanced visibility of arrivals and departures from work, which greatly facilitates human resources management.

Teamdeck software. Teamdeck software is open source software that is partially free. In other words, it is free for a company that has up to 6 members, otherwise it should be paid for, and it represents a freemium form. Its advantages are that it has an excellent solution for resource planning, supervision of employee employment, etc. This tool facilitates human resources management in planning and organizing optimum work performance of employees.

4. Comparative analysis of HR software solutions

Each of these software solutions provides some benefits. Table 1 shows the most significant advantages of given five software solutions for human resources management.

Table 1. Comparison of benefits of HR software tools

Orange HRM	Open source ERP	Odoo	HR.my	Teamdeck
Role adjustment	Database resource	Planning departure	Role tracking Organization	Time tracking
Employee information	Employee information	Complete business software	Job planning	Job optimization
Time management	Time management and attendance monitoring	Salary management	Improve attendance at work	Schedule management

Source: (Pat Research, 2018 (authors' adjustment))

Introducing software solutions requires certain resources, primarily financial. If the company is small or just entering the market, ERP software such as SAP or DynamicNav can cause high costs. Each of these solutions has the option of free trial and it is recommended to test them, so that the company can identify for one of the above.

Requirements for introducing the aforementioned software solutions are presented in a comparative way in the following table.

Table 2: Comparison of requirements for the introduction of HR software solutions

Orange HRM	Open source ERP	Odoo	HR.my	Teamdeck
- Open source software - Professional license - on request - License for the company - on request	- Open source software – completely free	- Free - one application - Online plan - paid - Company plan – paid	- Open source completely free	- Startup plan – free up to 6 - Business plan - \$3.99 monthly per user

Source: (Pat Research, 2018 (authors' adjustment))

In order to select the software, it is necessary to be analyzed, or to find out whether it visually responds to human resources managers, as well as its easiness to use. The user experience should be as good as it is, therefore, the software solution is more appealing to users. In this paper four aspects of user experience are presented and compared: easiness to use, additions and functionality, performance and customer support. Based on rates, final grade is generated for each software solution.

Graph 1 shows average user ratings of the five software listed. Ratings are generated from 1 to 10, where 1 represents the worst user experience, and by grade 10 the best user experience is presented.

Graph 2. Four parameters comparison of user experience

Source: (Authors, 2018)

Easiness to use aspect shows that Odoo software with rate 8.2 is the best choice for users, following by Orange HRM (7.4), as well as Teamdeck application (7.1). According to the second parameter, additions and functionality, it can be seen that the same software is leader with rate 9.1, as well, but close to it HR.my application has been noticed (8.8). Again, the best software performance, according to users' opinion and experience, is provided by Odoo and Orange HRM, both rated by 10. Finally, graph 1 shows that all presented solutions are almost equal, due to the characteristics customer service functionality (7.6-7.8). It can be concluded that due to given parameters, Odoo software is predominant.

At last, a graphical presentation of final users' grades is provided, relying on four parameters.

Graph 3. The average grades by four parameters

Source: (Authors, 2018)

Graph 2 shows that Odoo software has the best score of 8.77, three applications are almost even, while the worst average rating has Open source ERP (7.17).

5. Conclusion

Generally speaking, business systems represent a set of interrelated resources and one or more controlled operations which transform inputs into outputs. Mentioned technologies Cloud computing, Big Data and IoT represent a part of a modern information system which nowadays allow the company to survive on the market.

The human resources management, as a business subsystem, performs a wide range of tasks. For this reason, it is necessary to modernize or digitize it, so that the jobs can be done quickly and easily. The solutions presented in this paper show that in modern society there is a wide choice of open software solutions for human resources, which increasingly represent a serious competition between SAP and DynamicNav.

Open software solutions have the following benefits:

- Affordable solutions for small and medium enterprises.
- Some of them, more or less, have all the functions that are necessary for a modern manager of human resources.
- There is no need for additional investment in implantation and education of personnel.
- They can contribute to the improvement of human resources.
- The first step towards business modernization.

In this paper 5 open source software was analyzed and evaluated in four aspects in a comparative way. The average score shows that software solutions have very good grades (between 7 and 9). Finally, according to user ratings, Odoo has the best rating, while the worst one is Open source ERP.

Although the software solutions presented in this paper can be used in companies of all sizes, they are most often used in small and medium-sized enterprises, except the Odoo software solution, which is the most complete software of the offered ones, because it can be used in every function of the company.

Literature

1. Benson, G.F. (2011). *Emerging Themes in International Management of Human Resources*: Information Age Publishing.
2. Curtis, B., Hefley, E.W., Miller, A.S. (2010). *People CMM: A Framework for Human Capital Management*: Addison-Wesley.
3. Dessler, G. (2015). *Human Resource Management*. Florida International University: Pearson.
4. Langović, Z., Pažun, B. (2016). *Virtualization of information resources in tourism organizations*, 1st International Scientific Conference, Tourism in Function of Development of the Republic of Serbia, Spa Tourism in Serbia and Experiences of Other Countries, 2-4 June, 2016, Vrnjačka Banja, Serbia, Thematic Proceedings - II, University of Kragujevac, Faculty of Hotel Management and Tourism in Vrnjačka Banja, pg.536-552 [ISBN 978-86-89949-09-4; ISBN 978-86-89949-10-0].
5. Pankl, E., Theiss-White, D. (2010). *Recruitment, Development, and Retention of Information Professionals: Trends in Human Resources and Knowledge Management*: IGI Global.
6. Pat Research. (2018). Retrieved on November, 2018 from <https://www.predictiveanalyticstoday.com/compare/hr-my-vs-teamdeck-vs-open-source-erp-vs-orangehrm-vs-odoo/>
7. Simmers, C., Anandarajan, M. (2003). *Personal Web Usage in the Workplace: A Guide to Effective Human Resources Management*: Information Science Publishing.
8. The Economist Group, The Economist Intelligence Unit. (2018). Retrieved on December, 2018 from <http://www.eiu.com/home.aspx>
9. Torres-Coronas, T., Arias-Oliva, M. (2004). *E - Human Resources Management: Managing Knowledge People*: IGI Global.
10. VMware. (2016). *4 Key Architecture Considerations for Big Data Analytics*. Retrieved on November, 2018 from <http://blogs.vmware.com/vfabric/2012/08/4-key-architecture-considerations-for-big-data-analytics.html>