VYSOKÁ ŠKOLA OBCHODNÍ A HOTELOVÁ

Studijní obor: Management hotelnictví a cestovního ruchu

Nataliia LEMESHKO

SELECTING A WEB SERVER FOR HOTEL AREA

BAKALÁŘSKÁ PRÁCE

Vedoucí bakalářské práce: Mgr. Tomáš Jeřabek, MBA.

Brno, 2019

VYSOKÁ ŠKOLA OBCHODNÍ A HOTELOVÁ

Katedra ekonomie, ekonomiky a managementu

Akademický rok: 2018/2019

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Jméno a příjmení studenta: Nataliia Lemeshko

Osobní číslo: 14632364

Studijní program: Gastronomie, hotelnictví a turismus (B6503)

Studijní obor: Management hotelnictví a cestovního ruchu (6501R027)

TÉMA PRÁCE: VÝBĚR WEBOVÉHO SERVERU PRO OBLAST HOTELNICTVÍ

TÉMA PRÁCE V AJ: SELECTING A WEB SERVER FOR HOTEL AREA

Cíl stanovený pro vypracování BP

1. Teoretické část BP:
   - definujte základní teoretická východiska práce, základní pojmy a modely využitelné v rámci zvoleného tématu.

2. Praktická část BP:

   Analytická část:
   - charakterizuje vybrané ubytovací zařízení a představte metodiku výběru webového serveru. Metodiku aplikujte a prezentujte získané výsledky.

   Návrhová část:
   - na základě výsledků v analytické části navrhněte implementaci vybraného serveru v daném ubytovacím zařízení.

Při zpracování BP vycházejte z pomůcky vydané VŠOH Brno.

Rozsah bakalářské práce bez příloh: 2 AA

Forma zpracování bakalářské práce: tištěná i elektronická

Seznam doporučené literatury:
[1] LUDVÍK, M., ŠTĚDROŇ, B. *Teorie bezpečnosti počítačových sítí*. Brno: Computer Media, 2008. ISBN: 978-80-8668-635-3.
[2] KUNDA, D., CHIHANA, S. MUWANEI, S. Web Server Performance of Apache and Nginx: A Systematic Literature Review. *Computer Engineering and Intelligent Systems*. 2017, vol. 8, no. 2, pp. 43-52. ISSN 2222-1719.
[3] Šefčík, V. a kol. *Management hotelnictví a cestovního ruchu*. Brno: Akademické nakladatelství CERM, s.r.o., 2015. ISBN 978-80-7204-928-8.

Další literatura dle doporučení vedoucí/ho bakalářské práce.

Vedoucí bakalářské práce: Mgr. Tomáš Jeřábek, Ph.D., MBA
Katedra ekonomie, ekonomiky a managementu

Datum zadání bakalářské práce: 1. září 2018

Termín odevzdání bakalářské práce: 12. dubna 2019

V Brně dne: 1. září 2018

L. S.

VYSOKÁ ŠKOLA
OBCHODNÍ A HOTELOVÁ s.r.o.
Bosonožská 9, 625 00 Brno

Mgr. Tomáš Jeřábek, Ph.D., MBA
vedoucí katedry

Ing. Zdeněk Málek, Ph.D.
prorektor pro vzdělávací činnost

Jméno a příjmení autora:	Nataliia Lemeshko
Název bakalářské práce:	Selecting a web server for hotel area
Studijní obor:	Management hotelnictví a cestovního ruchu
Vedoucí bakalářské práce:	Mgr. Tomáš Jeřabek, MBA
Rok obhajoby:	2019

Abstract

On the basis of conducted investment analysis of improvement of information security and efficiency by change of its web servers realized by chosen international hotel from Ukraine to make a set of recommendations for hotels from other international hospitality chains which operate in Ukraine and which plan to improve their information security and efficiency by change of their web servers.

Key words

Information security, cyber security, hotel information system, web server, investments, finance.

Prohlašuji, že jsem bakalářskou práci Bezpečnost IT/IS v hotelovém provozu vypracovala samostatně pod vedením pana Mgr. Tomáš Jeřabek, MBA. a uvedla v ní všechny použité literární a jiné odborné zdroje v souladu s aktuálně platnými právními předpisy a vnitřními předpisy Vysoké školy obchodní a hotelové.

V Brně dne 12. 4. 2019

vlastnoruční podpis autora

Poděkování:

Na tomto místě bych ráda poděkovala vedoucímu bakalářské práce panu Mgr. Tomáš Jeřabek, MBA. za cenné informace a rady, které významně dopomohly ke vzniku bakalářské práce. Dále bych chtěla poděkovat řediteli hotelu Hyatt Regency Kiev panu Winklerovi a jeho personálu za ochotu a vstřícnost. V neposlední řadě chci poděkovat rodině za podporu.

CONTENT

INTRODUCTION……………………………………………………………………….….9

CHAPTER I. FUNDAMENTALS OF INFORMATION SECURITY IN HOSPITALITY….11

1.1. Conceptual framework for information security per se and in context of hospitality……..11

1.2. History of information security per se and in context of hospitality………………………15

1.3. IT and information security in hospitality business in Ukraine………………………...…18

1.4. Web server as one of the fundamentals of information security…………………………..22

1.5. Legislative framework of information security in EU and in Ukraine ……………………24

CHAPTER II. EVALUATION OF INVESTMENT OF HYATT REGENCY KIEV INTO ITS INFORMATION SECURITY

2.1. Profile of Hyatt Regency Kiev and its growth and innovation strategy 2018-2022…….…28

2.2. Methodology of conducted technical, economic and investment evaluation of migration of Hyatt Regency Kiev databases located at Apache-based to Nginx-based servers………......…31

2.3. Results of conducted technical, economic and investment evaluation of migration of Hyatt Regency Kiev databases located at Apache-based to Nginx-based servers……………..……..37

2.4. Recommendations for hotels from international hospitality chains which operate in Ukraine and other CIS countries planning to improve there IS security and efficiency by change of web servers…………………………………………………………………………………...42

CONCLUSION…………………………………………………………….........................46

BIBLIOGRAPHY……………………………………………………….………………...48

INTRODUCTION

Information is important. It is often depicted as the lifeblood of the growing electronic economy. Reliable and secure operation of data networks, computer systems and mobile devices is the most important for the functioning of the state and for maintaining the economic stability. Safe operation of all information systems is influenced by many factors: cyber attacks, disorders caused by physical impact, failure of software and hardware, human errors. These events demonstrate that information security of information systems needs to be managed and controlled properly. The purpose of thesis is to study this topic, that is, information security, from perspective of hospitality business. Every day millions of users around the world book and pay for hotel rooms. All hotel stakeholders (e.g. internal users and external users) involves computer networks. Internal use includes reservation systems, hotel stock management system, payroll, accounting, marketing and many other systems composing hotel information system (HIS). External users browse make reservations storing their personal data and credit card details at hotel web sites. In this way both external and internal users of hotel information systems are exposed to high risk of either system outage and/or data breach.

In light of stated above thesis aims to measure the impact of information security on performance of Hyatt Regency Kiev through investment evaluation of migration of its databases from Apache-based to Nginx-based servers and on the basis of obtained results to make a set of recommendations for similar hotels from international hospitality chains which operate in Ukraine and other CIS countries and which plan to improve their information security and efficiency of their information systems by change of their web-servers.

Thesis is structured into two parts – theoretical background and practical evaluation. Theoretical fundamentals reviewed in Chapter I include definitions of basic concepts and principles of information security, brief overview of history of information security in general and in hospitality, role of web servers in improvement of information security of the organization. Also general legislative framework at EU level and in Ukraine is outlined in this chapter.

Practical part presented in Chapter II contains brief presentation of Hyatt Regency Kiev together with key points from its growth and innovation strategy 2018-2022. In essence, Hyatt's management strives to make hotel as attractive investment target for national and international investors through increase of hotel's earnings per share and boost its image as one of the most luxury and secure hotels not only in Ukraine but also abroad. After conducting complex analysis, which included computation of a set of technical, financial and investment indicators by hotel’s top management, the decision was made to upgrade its data protection system by migrating of hotel databases to another web server. After financial analyze obtained results indicate that highest positive variance (i.e. growth in hotel server-apportioned profit) after migration of Hyatt’s web servers from Apache to Nginx is observed for such technical characteristics as count of threads and error rate.

Methodological part of thesis is based on literature review as well as comparative analysis which in its turn is based on computation of a range of key technical, financial and investment indicators.

Based on the obtained results thesis contributes with providing of a set of recommendations which can be used as guidance when changing web servers by other hotels from international hospitality networks that operate in Ukraine and other CIS countries. The main recommendation is to conduct complex analysis aimed to measure in monetary terms the impact of individual technical parameters of web servers (or any other components of hotel information system over which there is a plan to conduct an improvement) on hotels’ profit before and after realization of planned improvement.

CHAPTER I. FUNDAMENTALS OF INFORMATION SECURITY IN HOSPITALITY

Information is a fundamental asset for any business and protection of this asset, through a process known as information security, is of equal importance. Ensuring of information security is main objective of information security risk management which, in its turn, is one of five components of corporate risk management strategy[1].

Nowadays information security is espoused to a wide range of cyber threats resulting in data breach (e.g. malware and phishing) and/or business servers outage (e.g. DDoS attacks and SQL injections). However, it is not correct to state that information security is some modern trend. It had become a subject of public concern already in the first century when Julius Caesar devised a secret code to protect his confidential messages sent to his friends from being intercepted. During the past 21 centuries it has evolved into complex system with many variables and interdependencies with other hard and soft systems of organization (marketing, accounting, reporting, customer relationship management etc.). As for role of information systems and information security in hospitality, so they started to play an important role in this business since 1980 when first hotel management computer-assisted techniques were introduced.

As for legislative framework which regulates information security of organizations, so it has two levels – international (e.g. EU Regulation 2016/679 shortly known as GDPR) and national (e.g. Information Security Concept and National Cyber Security Program in Ukraine). Most of national legislative acts in area of information security are results of harmonization process with international legislation, that is, a process when international legislative acts are adopted at national level with some local particularities and/or exceptions.

All presented above are the key points which are discussed in details in theoretical part of thesis.

1.1 Conceptual framework for information security per se and in context of hospitality

Generally, the accepted notion of **information security** means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. Information security also refers to the condition

[1] Other four compoenets are: business environment, risk assessment, control activities, monitoring.

of continuous administration of information by protecting it from internal and external risks.[2] This universal concept is used no matter what form the data may have (electronic or physical).

The term **cyber security** is often used interchangeably with the term information security. Although there is a substantial overlap between cyber security and information security, these two concepts are not totally analogous. Cyber security goes beyond the boundaries of traditional information security to include not only the protection of information resources, but also that of other assets, including the person – customer - him/herself. To summarize: while information security assums protection of all aspects of the information itself, cyber security spreads over a wide range of assets that need to be protected starting from the person him/herself to common household appliances, to the interests of society at large, including critical national infrastructure. In fact, such assets include absolutely anyone or anything that can be reached via cyberspace.[3]

It is well-known fact that information security is one of fundamental components of corporate governance. Information is an organisational asset, and consequently the security thereof needs to be integrated into the organisation's overall management plan. Effective corporate governance should dictate this overall management plan. Sir Adrian Cadbury, in the foreword of Corporate Governance: A Framework for Implementation has the following description of corporate governance. He states that corporate governance deals with establishing a balance between economic and social goals and between individual and mutual goals. The framework for governance is there to promote the competent use of resources and, in the same way, to involve accountability for the stewardship of those resources. Information is a vital asset to most organisations, and because the Board of Directors have ultimate responsibility and accpuntability for the welfare of their organisation they should ensure that the organisational asset of information is protected to ensure the well-being of the organization.[4] This is done throught risk management, particularly throught one of its components called **information security risk management (ISRM).** ISRM enables an organization to identify vulnerabilities and threats, and then to decide which countermeasures to choose to address potential threats[5]. Moreover, those threats are becoming increasingly sophisticated, and more

[2] HONG-BUMM Kima, DONG-SOO Leeb, HAMC Sunny. *Impact of hotel information security on system reliability. Journal of ScienceDirect* vol.35, 2013, 369-379 pp.

[3] SOLMS von Rossouw, NIEK van Johan. *From information security to cyber security. Journal of ScienceDirect* vol.38, 2013, 97-102 pp.

[4] THOMSON Kerry-Lynn, SOLMS von Rossouw. *Information security obedience: a definition. Journal of ScienceDirect* vol.66, 2004, 36-40 pp.

[5] SHAMELI-SENDI Alireza, AGHABABAEI-BARZEGAR Rouzbeh, CHERIET Mohamed. *Cyber threats – approaches to cyber risk assessment. International Journal of Computer Science and Network Security*, vol. 12, no. 1, pp. 1-14.

resources than ever before are required to neutralize them. Organizations which do not conduct risk assessment properly and regularly may experience severe consequences, like loss of reputation, legal issues, or even a direct financial impact.

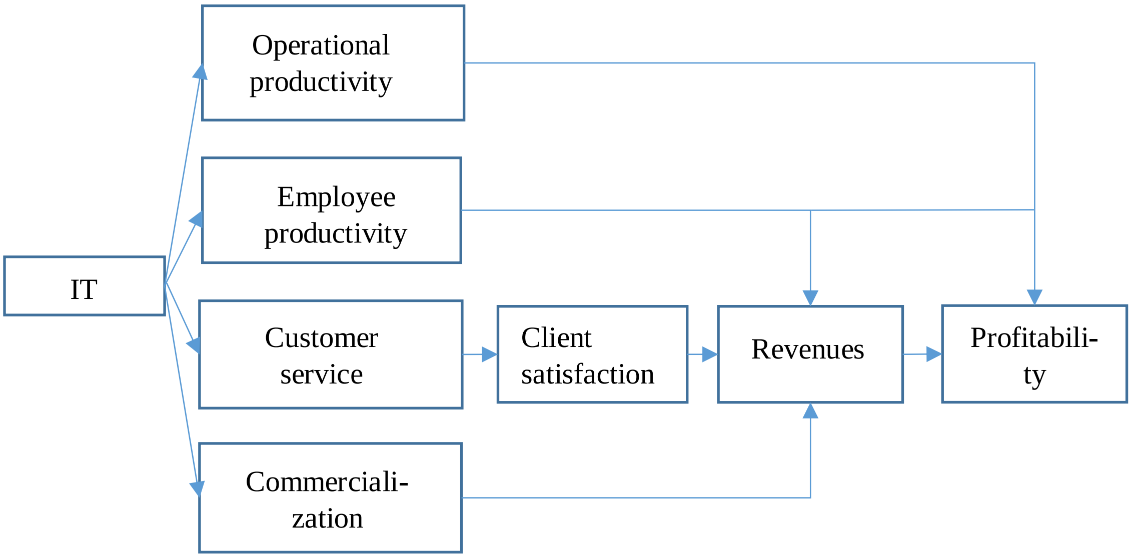
And what do we know about information security in such companies as hotels? First of all, it is necessary to give a brief overview of **information technologies and systems** used **in hospitality business.** The intense competition in today's business environment means that tourism and hospitality businesses have to work hard to maintain and develop their competitiveness. The success of a business, to certain extent, depends on its ability to acquire and utilize updated information to assist its management and marketing processes. Hence, information technology (IT) assists organization to manage information dynamically and influences business competitiveness through assisting decision makers to make appropriate investments and decisions. IT helps to meet the demands for timely and accurate information by customers and the IT diffusion in the tourism and hospitality industries has recently increased at an unprecedented rate. This is evident by the ubiquitous presence of IT systems that work cooperatively to assist managers to deliver quality service to their customers and to enhance operational efficiency and control costs. Researchers have stated that IT, by acting as a protector and enhancer, directly influences the experiences and behavior of tourists.[6] More strategically, IT is gradually reshaping the nature of tourism and hospitality products, processes, businesses, and competition, and that tourism and hospitality organizations that have failed to master the right IT systems would find difficult to direct and manage their information-intensive business damaging their competitiveness.

Hotel information system (HIS) stands for a system of computer-assisted techniques which supply information about that hotel's business operations. HIS typically includes all computerised systems, which are used to collect and process data (often 'big data') continuously both for internal and external use. HIS plays a crucial role in hospitality as it facilitates hotel' planning, management, and investments. In short, impact of information technology on hotel performance can be shown on Fig. 2.

To use HIS effectively, establishment of ISRM have become increasingly important. It is possible to say that **information security in hotel industry** developed from general safery principles, which assume preventing employees and customers within the hotel property from

[6] LAW Rob, LEUNG Rosanna, BUHALIS Dimitrios. *Information technology applications in hospitality and tourism: a review of publications from 2005 to 2007. Journal of Travel and Tourism Marketing* vol.26, 2009, 599-623 pp.

Figure 1. Impact of IT on hotel performance



Source: MELI-AN-GONZALEZ Santiago, BULCHAND-GIDUMAL Jacques. *A model that connects information technology and hotel performance.*

potential death and injury, such as from accidental slips, falls, cuts, burns and so forth, as well as preventing related property damage.[7] To improve safety, many hotel companies have installed electronic locks, fire sprinklers, smoke detectors, and closed circuit televisions. As time passed the traditional security responsibilities of guarding and loss prevention have been broadened to include health and safety, IT security, disciplinary action, fire safety and insurance.

Today, ISRM in hotel operation, the security of information that the hotel (produces, transmits or receives) from unauthorized access, destruction, modification, disclosure, and acceptance delays. Information security includes measures to protect data creation processes, their input, processing and output. The main objective of ISRM is to ensure the sustainable operation of the facility by preventing threats to its security, protecting the customer's legitimate interests from unlawful interventions, to prevent theft of funds, disclosure, loss, leakage, distortion or destruction of proprietary information to ensure the normal production activity of all object divisions . Another objective of the information security system is to improve the quality of the services provided and to ensure the security of the property rights and interests of the clients. With proper risk management, a balance between potential risks and acceptable

[7] CHAN Erik, LAM Doris, (2013). *Hotel safety and security systems: Bridging the gap between managers and guests. International Journal of Hospitality Management* vol.32, 2013, 202-216 pp.

risks can be achieved. In other words, risk management processes should be repeatable, measureable, and auditable, and it should be possible to model them as well.

1.2 History of information security per se and in context of hospitality

Reflecting upon the past two decades, it is obvious that we cannot separate history of information security in hospitality from the global, societal view of development of IT.

It is possible to say that information security came into existence even before the invention of a computer. .Dlaminia et al. (1991) argues that information security is as old as information itself. From the time when information began to be transmitted, stored and processed, it required protection.[8] This dates back to the time when human beings first learned how to write. Anderson and Choobineh (1999?) takes us back to the first century when Julius Caesar devised a secret code to protect (confidential) messages sent to his friends from being intercepted.[9]

With development of mail, government organizations began to withold, decrypt, read, and re-write letters. In this way in England a Secret Office was established in 1653. In Russia since the times of Peter I, i.e. from 1690s, all foreign letters were opened and examined in Secret Office (later renamed into 'Black Office') in Smolensk.

In the 1840s when the telegraph was invented, an encryption code was developed to safeguard the secrecy of the transmitted telegrams. The first recorded attack on information security ('hack') actually took place in 1903, when inventor Nevil Maskelyne disrupted a public demonstration of secure wireless telegraphy technology, by sending insulting Morse code messages through the auditorium's projector.[10] Luckily for Maskelyne, the wireless had no firewall, but this was the catalyst for increasingly complex and disturbing attacks, and with it, increasingly secure software designed to counter the threats.

The 1940s up to the 1950s marked the dawn of computing, when the first-generation computers came into existence. This was followed by the era of mainframe computers when only a few operators were permitted to use these computers. Other users would submit their jobs to the operator through protected slots (batch processing). The key security issue during this era was ensuring that only the privileged computer operator (one user one computer) would

[8] DLAMINIA Mloses, ELOFFA Mariki, ELOFF Jan. *Information security: The moving target. Journal Semantic Scholar* vol.10, 2009, 32-35 pp.

[9] ANDERSONA Evan, CHOOBINEHA Joobin. *Enterprise information security strategies. Journal of ScienceDirect* vol.27, 2008, 22-29 pp.

[10] MAULE-FFINCH Bradley. *Cyber Security Europe. Key trends in information Security*. *Journal of Cyber Security,* vol.13, 2017, 113-118 pp.

have access and that the physical computer was not stolen or damaged by outsiders. The scope of security gradually increased from the protection of secrecy or confidentiality of information, businesses' reputationructure (mainframe computers) that processed the information and storage media. Physical security was the basic principle underlying all security of computer systems.

The late 1960s until the early 1970s mark the beginning of dumb terminals. These enabled users (multiple users – one computer) to access and use remote data. This innovation introduced a new risk to remotely held data. Data could be accessed by unauthorized people or outsiders. Elementary physical security could not deal with this new risk. Therefore, user identification and authentication came into play in the early 1970s. Physical access to terminals was screened by a security officer before the user could start the identification and authentication process. Since there were few terminals it was easy to keep track of all logged-in users and their activities.

However, since there were no security policies in place to enforce the use of strong passwords, password cracking was a big threat at this time. Password sharing posed another major problem. Guest and anonymous logins were still acceptable, as outsiders without much identification and authentication could access only limited resources inside the network.

Also in the early 1970s public key cryptography came into existence. The Data Encryption Standard (DES) was adopted by the then National Bureau of Standards (NBS) of USA,. This is around the same time that the ARPANET began, which aimed at providing a reliable and robust network to ensure the availability of computer systems[11]. This innovation introduced a new dimension for the protection of information. In response the US government passed the Privacy Act of 1974 to safeguard personal information recorded in government systems.

The 1980s marked the introduction of personal computers and suddenly every user had his/her own computer. The number of people with computer know-how increased. Companies began to automate their operations and new security threats emerged as critical corporate data was now stored on easily accessible secondary storage. The scope of information security further widened. Hence, the 414 gang, the intruder (Markus Hess) who broke into computers at Stanford campus in the USA and the West German programmer who broke into the US military computers to steal documents were reported to be among the first intruder break-ins.

[11] DLAMINIA Mloses, ELOFFA Mariki, ELOFF Jan. *Information security: The moving targetю Journal Semantic Scholar* vol.10, 2009, 32-35 pp.

This decade marked the rise of computer viruses, which spread through the use of diskettes. Viruses called ‘‘Elk Cloner’’ and ‘‘The Brain’’ to be among the first viruses ever created. Robert Morris created the first worm in 1988, which despite its general harmless, it produced a massive scare. By the end of 1990, there were approximately nineteen anti virus software environments including Symantec’s Norton Anti Virus, ViruScan by McAfee; and IBM’s Anti Virus.

Towards the end of the 1990s attackers changed from using worms and viruses to more sophisticated attacks. The introduction of distributed denial of service and malicious code attached to business emails and web pages shifted the focus to gateways. This saw the introduction of filtering firewalls. Perimeter security came into existence to provide a wall around networks and keep outsiders out. But as the use of the Internet intensified, network boundaries disappeared and perimeter security vanished.

As we entered the 21st century, things changed. Attackers started hacking for financial gains and not just to show-cast their skills. IT infrastructure became pervasive in almost all industries (known as the era of pervasive computing). Every second word now began with an E, for example E-commerce, E-voting, E-business, E-government, etc., because everything had gone electronic. As all sorts of devices came on-board (Personal Digital Assistants, Smart phones, Laptops, Tablet PCs, etc.), it became difficult to clearly define a computer. Mobile computing (Bluetooth and Wi-Fi) also emerged to complicate things even further. Online payment systems and the usage of credit cards became highly popular and webbased applications intensified. However, the fact remains that all these new developments in technology were vulnerable and like all other good things came with side effects (risks).

From what we found about information security in hospitality it is possible to say that only starting from the mid of 1980s information security became important component of hotel management and academic research. Before that time information security was represented only by general safety, such as quality of food and beverages, installed electronic locks, fire sprinklers, smoke detectors, and closed circuit televisions.

However from the mid of 1980s with intorudction of computer-assisted hotel management techniques (currently known as HIS – hotel information system) the range of security ares has widen substantially. HIS refers to all the computing software programs and hardware used in the hotel operations, consisting of many subdivisions, such as front office, reservations, restaurant services, housekeeping, engineering, sales, accounting and guest services. And all these operations need proper protection against unauthorized access and misuse.

Rapid development and wide application of Internet in 1990s increased number of customers who access hotels via the Internet and employees permissible accessing HIS through outside intranets, the importance of security for customer information has become greater than ever[12]. Hotel websites collect customers' personal data when providing hotel services and other information. While such collected information greatly contributes to the hotel's marketing and promotional strategies, the hotel must preferentially protect customers' data to sustain integrity. For this purpose, already from the mid of 1990s hotels started to establish protocols pertaining to customers' privacy.

As by the end of 1990s hotels' websites expanded their functions from providing general information to customers to registering reservations and related transactions through e-commerce, the security of the payment system has come into play. Despite almost twenty years of software developments in this area up until now the information security for e-commerce transactions reamints a critical element of hotel information security risk management (ISRM).

Since 2000s cyber-attacks have become a significant concern in the hospitality industry. The hotel industry, with the considerable volume of credit card transactions, online payments for reservations, accounts to loyalty programs, and Wi-Fi usage at the property, provide a considerable footprint for potential cyber-attacks.[13] As respond to this from 2010s ISRM of hotels was extended with cyber crisis management aimed to take immediate actions by hotel management in order to decrease the negative effects of cyber attack. Such actions include not only rebudting HIS but also communicating with hotel customers whose personal data were stolen. This can eventually result in less lawsuits filed against the hotel, lower financial losses, and less damaged reputation.

1.3 IT and information security in hospitality business in Ukraine

Travel, Hospitality, and Leisure (THL) sector in Ukraine is faced with significant changes. Businesses operating in this sector are struggling to adapt themselves to the new environment, given the current strained state of the economy. The industry today faces a number of tasks related to the operational excellence, customer loyalty and the development of new technologies.

[12] HONG-BUMM Kima, DONG-SOO Leeb, HAMC Sunny. *Impact of hotel information security on system reliability. Journal of ScienceDirect* vol.35, 2013, 369-379 pp.

[13] HSIANGTING Shatina Chena, JAIB Tun-Min (Catherine). Cyber alarm: *Determining the impacts of hotel's data breach messages. International Journal of Hospitality Management* vol.73, 2018, 100-103 pp.

The development of hospitality market in Ukraine in the 1990s and at the beginning of 2000s can be characterized by several multidirectional trends. Despite precense of international hotel chains in Ukriane local hotel industry still remains the Soviet past: until the early 2000s foreign operators did not open their hotels outside Kiev, Lvov and Odessa. In small cities it was a typical situation when major hotels remained in state ownership and with traditional Soviet approach to management. In many regions there continues to be a lack of hotels from the middle price segment. And it is this sector – middle price hotels – that generates most of revenues in country's hotel market and that is the driver of new brands and innovations.

Currently as per beginning of 2019 the total market value of hospitality in Ukraine is estimated at 0.1 billion US dollars and the number of hotels is 10,000 including 75 branded hotels (Hyatt, Intercontinental, Fairmont, two Radisson, Holiday Inn, Park Inn, Ramada Encore and Ibis).[14] The average annual market growth rate is estimated at 5-8%. Such high rate of growth is connected with rapidly movement of customer support services towards applications such as Viber, Telegram and Facebook as popular platforms for client communication. Also more people are now flying to Ukraine and within the country. The largest regional increase in air traffic this year has been in western Ukraine, with Lviv International Airport recording a 29% rise in passenger numbers. The figure for Kyiv currently stands at 19%, while Odesa has welcomed 9% more airline passengers.

As for information systems used by hotels in Ukraine, despite powerful IT basis of Ukraine, its hospitality uses mainly foreign software[15]:

- Front-office information system 'Fidelio'. The system facilitates registering of tourists, inventory and management of rooms, marketing of tourist products or record of income;
- Information systems dedicated to bookings 'Worldspan' and 'Amadeus'. These systems get together booking and sales services The two systems are used by both hotels and customers.
- Hotel management information systems:
  - Medallion Property Management System (Medalion PMS) – it is the system in Windows version that comprises all modules required to carrying the work of a hotel, regardless the number of rooms and its structure;
  - Expressoft Interface Manager – it is a system used for an accurate control of inventories;

[14] Ccdcoe report - Cyber security srtategy of Ukraine .

[15] N-IX report - Information technology and information security in hotel operation in Ukraine. Available from WWW:<https://www.n-ix.com/is-ukraine-safe-software-development-offshoring-data-protection-information-security/>

- Customer Relationship Management (CRM) aimed to attract new and retain existing customers. It integrates processes and internal functions as well as external networks in order to create and provide value to customers. The development of a CRM application requires serious knowledge about consumption needs of customers, behaviour and preferences, and the new technologies are the main factor that fosters change in the hotel industry.

Using by hotels in Ukraine of such leading world-known information technologies as the ones mentioned above is another contributor to fast growth of Ukraine’s hospitality market.

While discussing HIS used by Ukraine’s hotels it is worth mentioning about local information security. According to Bloomberg as many as 1.4 million and 0.85 million people visited Ukraine during European Football Cup in 2012 and Eurovison Song Contest in 2017. And it might sound like hyperbole, but it was also official guidance from National Counterintelligence and Security Center in the United States, that anyone traveling to Ukraine to attend to these event (Euro 2012 ad Eurovision 2017) should be clear-eyed about the cyberrisks involved. Visitors planning to take a mobile phone, laptop, PDA, or other electronic device with them were notified that any data on those devices could be accessed cybercriminals. Probably such worrning from leading counterintelligence agency in the world was not an exaggeration since Ukrainian government together with the national special services ad conducted special checks on hotel IT systems where the visiting teams and officials should stay. This resulted in the issue of report stating that event infrastructure is a highly possible target of cyber attacks[16].

It is necessary to mention that information security in Ukraine’s hotels varies greatly from hotel to hotel. In the same report, we can find information that hotels within global chains pay a lot of attention to data protection, but the level of IT security at the majority of other hotels remains relatively weak.

In those hotels where management is carried out directly by the operator with a worldwide reputation, there are high requirements for information security ranging from installation of electronic locks and computer surveillance systems to implementing anti-terrorism procedures. The most common ways how such hotels improve their information security are the following:

As electronic locks and computer surveillance systems to implementing anti-terrorism procedures

[16] Cyber attacks in Ukraine. Available from WWW:< https://www.politico.eu>

- Building connection between IT and security departments. The two departments should work together. To foster this relationship, some hotels place the two departments under the same manager and same budget. And the two departments should conduct regular security meetings, perhaps as often as once a week. Ukrainian hotels mostly make a joint security department. Usually he is in the hotel and also has its own server.
- Upgrading to servers with VLAN. A LAN, or local area network, is a network that connects computers. For many businesses that includes a WiFi access point for customers. However, WiFi that's directly connected to hotel servers can pose a risk and provide easy access for savvy hackers. One way to add more cybersecurity is to install what's called a VLAN, or virtual network. Relatively inexpensive, VLANs often don't require additional hardware. Installing this software adds another layer of security between hotels servers and potential hackers. Also, a common feature of VLANs is the ability to set up multiple wireless network names, which can have varying levels of security. Computers used for business and staff can have a high level of security, and guest WiFi networks can have a lower, easy-to-access level of security and be separated from the property's network.
- Discovering threats of of social engineering. Not all cyber threats occur online. Social engineering and physical hacking of hotel computers pose a significant risk. Employees should have an awareness about the physical security of computers, access control, and passwords. Many of the big hacking schemes we hear about start with someone conning a password out of an employee. Change passwords every three months. Also, employees should monitor the physical access points to a property's computers and servers. Make regular patrols to look for people who are in staff-only areas of a property. Hyatt creates chip cards for employees who have access to computers. Also, every three months, the system generates new passwords.

1.4 Web server as one of the fundamentals of information security

As per CISCO report the most common types of cyberattacks are the following[17]:

[17] CISCO report - Cisco Annual Cybersecurity Repor. Available from WWW:<https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html>

- Malware - malicious software, including spyware, ransomware, viruses, and worms. Malware breaches a network through a vulnerability, typically when a user clicks a dangerous link or email attachment that then installs risky software. Once inside the system, malware can block access to key components of the network (ransomware), installs malware or additional harmful software, covertly obtain information by transmitting data from the hard drive (spyware).
- Phishing – it is the practice of sending fraudulent communications that appear to come from a reputable source, usually through email. The goal is to steal sensitive data like credit card and login information or to install malware on the victim's machine.
- Man-in-the-middle attack (MitM) - also known as eavesdropping attacks, occur when attackers insert themselves into a two-party transaction. Once the attackers interrupt the traffic, they can filter and steal data.
- Denial-of-service attack - it floods systems, servers, or networks with traffic to exhaust resources and bandwidth. As a result, the system is unable to fulfill legitimate requests. Attackers can also use multiple compromised devices to launch this attack. This is known as a distributed-denial-of-service (DDoS) attack.
- SQL injection – it occurs when an attacker inserts malicious code into a server that uses SQL and forces the server to reveal information it normally would not. An attacker could carry out a SQL injection simply by submitting malicious code into a vulnerable website search box.
- Zero-day exploit - it hits after a network vulnerability is announced but before a patch or solution is implemented. Attackers target the disclosed vulnerability during this window of time. Zero-day vulnerability threat detection requires constant awareness.

According to Cisco Annual Cybersecurity Report, almost in 75% of cyberattacks mentioned above happen via unsecure web servers. Web server security is important for any organization that has a physical or virtual Web server connected to the Internet. It requires a layered defence and is especially important for organizations with customer-facing websites (like hotels). A leaky server can cause a vital harm to an organisation.

In light of the above it it can be concluded that by enhancing security of their web servers hotels decrease by 50% their risks of being a target for cyber attackts and leakage of their customers personal data.

Before going into details of particular types of web servers it is necessary to give brief definition of web server by itself. Web servers are big computers that serve as website hosts for a particular organization. The common characteristics that web servers have are public IP addresses and domain names. There are those based on Microsoft Windows and those based on Linux, which are respectively named Microsoft IIS Server and Apache (the most common one although there are others like Nginx, Cherokee, and Zeus).

After hearing about all the problems with Microsoft's Internet Information Server (IIS)[18], most of organizations, including those in hospitality business, consider Apache and similar ones as substantially easier to secure. This assumption is to some degree true - although Linux-based servers are by no means perfect from a security perspective, it is not needed to do as many things to secure Linux-based server as in case of IIS-based one. In fact, there are two groups of actions which can be undertaken to secure Linux-based servers: (1) to monitor that scripts that run on web server are secure; and (2) to upgrade servers with VLAN. And running ahead it is necessary to say that both actions are undertaken by hotels from world-known chains.

As mentioned earlier, the two main types of Linux-based servers are Apache and Nginx. Here are some brief descriptions of both:

- Apache HTTP Server was developed by Robert McCul in 1995 and has been under the management of the Apache Software Foundation, Apache Software Development Foundation since 1999. It now operates around 46% of sites worldwide. Due to its popularity with Apache, there is strong documentation and integration with third-party software. Administrators often choose Apache because of their flexibility, strength, and prevalence. It can be extended with a dynamically loaded modular system and run programs in a large number of interpreted programming languages without using external software. In the hotel operation system helps to process received data from different locations, such as Booking.com, Facebook, store data from passports, bank cards. And also encrypt this information.
- In 2002, Igor Sysoev began working on Nginx to address the C10K problem - a software requirement to work with 10,000 simultaneous connections. The first public version was released in 2004, the goal was achieved thanks to asynchronous event-driven architecture. Nginx began to gain popularity from release due to its ease (light resource utilization) and ability to easily measure to minimal hardware. Nginx is excellent in providing static content and is designed to transmit dynamic requests to other software for processing. Administrators often choose the Nginx algorithm for resource efficiency and load response, as well as the ability to use it as a web server and proxy server.

[18] Microsoft's Internet Information Server. Available from WWW:<https://www.iis.net/>

General comparison of Apache and Nginx servers can be found in Table 1.

Table 1. Comparion of Apache and Nginx by key technical and economical characteristics

Criterion	Apache	Nginx
Static speed	Second to Nginx	2.5x faster than Apache
Dynamic speed	Both score same in this area	
OS support	Unix, Windows, MacOSX	Unix- like OS, not so with Windows
Security	Both have excellent security track record	
Flexibility	Highly customizable architecture	Difficul to customize modules suitable for the server due to complex base architecture
Support	Excellent community with widespread user base. Lots of support provided online	Provides community support through mailing lists, IRS, stack overflow and forum
Cost	Open source hence free to download and use	Open source license available along with paid license for advanced features like Nginx plus

Source: Sagar Khillar. *"Difference between Apache and Nginx."*

1.5 Legislative framework of information security in EU and in Ukraine

In recent years, the information security has gained a lot of attention in business and governmental circles. Study of many sources[19] indicated that there is requirement for additional regulation to lift the information risk management across various essential services, such as critical national infrastructure (utilities, telecommunication, banking etc.). During last 10 years, we can observe how national goverments all over the world are working on national and international legislative frameworks aimed to deal with the growing threat from various cyber attacks with direct implications for consumer confidence, public protection as well as economic growth. Alongside with national governments international professional organizations like International Auditing and Assurance Standards Board and Corporate Governance Committee (part of OECD) are working on standards and codes aimed to enhance security of IT infrastructure used by business and customers[20]. All these initiaves and projects resulted in a wide range of national and international legal acts and authoritative pronauncements (standards) aimed to enhance information security within business and public. For the purposes

[19] OECD Better Regulation in Europe- 2018

[20] Legislative Activities in Ukraine. [online]. 2019. Available from WWW:<https://rada.gov.ua/en>

of this bachelor thesis we will focus only on the main legal acts and standards mandatory in EU member states and in Ukraine.

Information security apparatus in the European Union was built upon an informal but largely technical, engineering-driven governance system between various national teams responsible for network and computer security. With extending of scope of work of individual teams the following key bodies have been formed:

- European Cyber Security Organisation (ECSO) - non-for-profit organization which is contractual counterpart to the EU Commission for the implementation of the cyber security initiatives. ECSO members include a wide variety of stakeholders such as large companies, SMEs and start-ups, research centres, universities, end-users, operators, clusters and association as well as European Member State’s local, regional and national administrations.21 Guidance and strategies worked out by Board and subsequently used by EU Parliament are Strategic Research and Innovation Agenda (SRIA) and a Multiannual Roadmap in Information Security, Research and Innovation (R&I) in cybersecurity.
- European Union Agency for Network and Information Security (ENISA) - an advisory body of EU Parliament actively contributing to a high level of network and information security within the Union. This includes the pan-European cyber security exercises, the development of national cyber security strategies, studies on secure cloud adoption, addressing data protection issues.22 In general, ENISA advice in development and implementation of the European Union's policy and law on matters relating to information security. Guidance and strategies worked out by Board and subsequently adopted by EU Parliament are Network Information Security Good Practice Guide, Network Information Security: An Implementation Guide, National Information Security Strategies, An Evaluation Framework for Network Information Security.
- European Data Protection Board (EDPB) - an advisory body of EU Parliament made up of a representative from the data protection authority of each EU member state. The Board provides expert advice to the states regarding data protection, promotes the consistent application of the Data Protection Directive in all EU state members, gives to EU Commission an opinion on community laws (first pillar) affecting the right to protection of personal data, makes recommendations to the public on matters relating to the protection

[21] European Cyber Security Organisation. Available from WWW:< https://ecs-org.eu>

[22] European Union Agency for Network and Information Security. Available from WWW:<https://www.enisa.europa.eu>

of persons with regard to the processing of personal data and privacy in the EU.23 Legislative acts worked out by Board and subsequently adopted by EU Parliament are: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR); Directive (EU) 2016/680 - On the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data; Information note on data transfers under the GDPR in the event of a no-deal Brexit - 12/02/2019.

Taking into consideration crucial role of Regulation (EU) 2016/679 (GDPR) in personal data security here it is worth to summarize its key points:

- The companies that process personal data are asked to process the personal data in a lawful, fair and transparent manner.
- The companies are expected to limit the processing, collect only that data which is necessary, and not keep personal data once the processing purpose is completed
- The data subjects have been assigned the right to ask the company what information it has about them, and what the company does with this information.
- As and when the company has the intent to process personal data beyond the legitimate purpose for which that data was collected, a clear and explicit consent must be asked from the data subject. Once collected, this consent must be documented, and the data subject is allowed to withdraw his consent at any moment.
- The organisations must maintain a Personal Data Breach Register and, based on severity, the regulator and data subject should be informed within 72 hours of identifying the breach.
- Companies should incorporate organisational and technical mechanisms to protect personal data in the design of new systems and processes.
- The controller of personal data has the accountability to ensure that personal data is protected and GDPR requirements respected, even if processing is being done by a third party.
- When there is significant processing of personal data in an organisation, the organisation should assign a Data Protection Officer.

[23] European Data Protection Board. Available from WWW:<https://edpb.europa.eu>

- Organisations must create awareness among employees about key GDPR requirements, and conduct regular trainings to ensure that employees remain aware of their GDPR responsibilities.

All these international organizations have brought information security and data protecition in EU memebre states to the new level. As for similar agencies and boards in Ukraine so they are represented by National Security and Defence Council of Ukraine and National Coordination Center for Cyber Security. Both are designated to develop and enhance Ukraine's information security through protection of national information space against information threats and the promotion of its sustainable development to satisfy vital information interests and needs of a citizen, society and the state.[24] These two governmental boards issue drafts of national programmes, doctrines, laws of Ukraine, decrees of the President of Ukraine, directives of the Supreme Commander-in-Chief of the Armed Forces of Ukraine, international treaties and other regulations and documents relating to information security of Ukraine. The major of them are Ukraine Information Security Concept, National Cyber Security Programme, and National Information Security Specialist Training and Retraining Programme.

[24] National Security and Defence Council in Ukraine. Available from WWW:<http://www.rnbo.gov.ua/en/>

CHAPTER II. EVALUATION OF INVESTMENT OF HYATT REGENCY KIEV INTO ITS INFORMATION SECURITY

Being one of the most frequent targets for cyber attacks, improvement of security of web servers has become one of the most popular types of investments into IS infrastructure of any business. Also besides their substantial contribution to information security of the business, web servers also represent quite material portion of total business costs and allocated profits. Thus by improving its web servers any business achieves two objectives: (1) increased protection against cyber attacks and internal fraud; and (2) reduction in operating costs, thus increase into profit margin of whole business. Especially it is important for companies which have become or are planning to become public.

With respect to all stated above, practical part of thesis will be focused on evaluation of efficiency of investment into its web servers undertaken by Hyatt Regency Kiev as part of realization of its growth and innovation strategy 2018-2022. Particularly we will evaluate the pay off of migration of Hyatt's databases from apache-based to Ngnix-based web servers. This will be done by means of conducting a complex analysis comprising technical, financial and investment components. As final output based on Hyatt's experience we will summarize briefly core recommendations for other hotels from international hospitality chains which operate in Ukraine and other CIS countries planning to improve there IS security and efficiency by change of web servers.

2.1. Profile of Hyatt Regency Kiev and its growth and innovation strategy 2018-2022

2.1.1. Hyatt Regency Kiev

Hyatt Regency Kiev (here and after 'Hyatt') is part of Hyatt Regency Ukraine, which is Ukrainian subsidiary of Hyatt Hotels Corporation, an American multinational hospitality company that manages and franchises luxury hotels, resorts, and vacation properties. Construction of Kiev property started in 1998 and finished in 2001 and over following 17 year Hyatt Regency Kiev has become the first largest hotel and the second after Intercontinental Hotel most luxury hotel in Ukraine.

Hyatt Regency Kiev is located in the city center of Kiev, political and business capital of Ukraine. Overlooking the breath-taking Old City, which features many of Kiev's main historical and cultural sights, Hyatt is within walking distance of Saint-Sophia's Cathedral, Saint-Michael's Monastery and the boutiques of famous Kreshchatyk Street. The hotel offers 234 comfortable rooms and suites, some of the most luxurious accommodation in Kiev. This 5-star hotel is one of the top business addresses in Ukraine and is the host to the unique Spa center "Naturel" and the fitness center "Club Olympus", with modern gym facilities and 20m-long indoor pool. Hotel is also known for its exquisite restaurants and bars. Price for 1 night per 1 person- from 300 USD till 900 USD. Hotel is holder of many prestigious international awards such as "For a high level of service" in 2015-2018 from Booking.com, "Quality certificate" in 2010-2018 , from TripAdvisor, World Travel Awards 2017-2018, "Best new hotel in Europe 2002-2005" from The Sunday Times and many others25. As per December 2018, during 17 years of its existence 1,000,000 foreigners and about 2,000,000 Ukrainians visited Ukraine's Hyatt.

2.1.2. Hyatt Regency Kiev growth and innovation strategy 2018-2022

To keep the pace of race with its competitors from other international hospitality chains, in 2017 hotel's board of directors adopted 'Hyatt Regency growth and innovation strategy 2018-2022' (here and after Strategy). This was shortly after initial public offering of hotel's shares at Kiev International Stock Exchange in December 2016.

The adopted Strategy is aimed to make Hyatt Regency Kiev as attractive investment target for national and international investors through increase of hotel's earnings per share (EPS) and boost its image as one of the most luxury and secure hotels not only in Ukraine but also abroad. As it is well known from fundamentals of finance[26], EPS increases with growth of company's profit, which in its turn is achieved by maximization of its sales and decrease of its costs. According to Hyatt's top management vision growth in sales should be achieved via massive marketing campaign and offer of new type of accommodation[27]. These actions are aimed to stimulate hotel sales. On the other hand, such increase in sales should be based on adequate infrastructure (hotel capacities), which means some changes in its building plan as well as changes in its information systems. As part of the latter ones (i.e. changes in information system), Strategy lays down the transfer of Hyatt's databases from Apache-based to Ngnix-based web servers described further. Such transfer will help Hyatt to achieve several objectives, two of which are creation of adequate infrastructure to support Hyatt's growing sales and reduction in unit based costs per hotel web server.

[25] Available from WWW:<https://www.kievcheckin.com/kiev-bars-restaurants-summer-terraces>

[26] BREALEY Richard, MYERS Stewart. *Principles of Corporate Finance. 233-240 pp.*

[27] New type of accommodation to be offered by Hyatt Regency Kiev are micro suites which should be nearly twice lower in price than normal suites and more customized for needs of those guests who stay in the hotel during their business trips.

As for hotel security, so as it was already mentioned in theoretical part of thesis, it is very complex system with many components, and information security being one of them. Nowadays not only direct armed terroristic attacks like that of September 11, currently impact occupancy of hotels. Cyber attacks become equally dangerous for hospitality industry. Every year hotel industries in major tourist destinations suffer significantly low occupancy rates due to massive hacker attracts and theft of personal and financial data of the hotels and their guests[28]. That is why, there is nothing surprising that hotels from world known hospitality chains started to take actions to improve their information security. Hyatt Regency Kiev is not an exception. As it is clear from its title the second core stone of Hyatt's Strategy 2018-2022 is reinforcement of hotel's information security. As it had already been mentioned in theoretical part, according to Cisco Annual Cybersecurity Report almost in 75% of cyberattacks mentioned above happen via unsecure web servers. And this statistics is confirmed by Hyatt internal evidence. That is why one of the main directions for improvement of Hyatt's information security was decision to migrate hotel's databases located on Apache-based to Nginx-based servers. Such migration would help to increase working capacities of hotel servers for their internal and external users as well as decrease a range of operating costs directly connected with server operation, particularly server outage costs, server maintenance costs and costs caused by breach of personal and financial data in result of hacker attacks.

Hyatt's Strategy 2018-2022 in area of growth in sales, decrease in costs and improvement of its information security can be summarized in following bullet points:

- Decrease in total hotel operating costs by 5% from 2018:
    - Server-dependent decrease in costs – 10% of planned decrease in costs[29] to be decreased through:
        - Decrease in outage costs
        - Decrease in maintenance costs
        - Decrease in personal data breach penalties
- Increase in total hotel sales by 7% in 2020 and contestant annual growth of 2% after 2020:
    - Server-dependent increase in sales – 15% of planned increase in sales[30] to be increased through:
        - Increase in number of concurrently processed requests

[28] CHAN Erik, LAM Doris. Hotel safety and security systems: Bridging the gap between managers and Guests. *International Journal of Hospitality Management* vol.32, 2013, 202-216 pp.

[29] that is, 10% from total planned decrease in costs in amount of 5% stands for 5%*10% = 1% of decrease in total hotel costs due to lower hotel's server related costs

[30] that is, 15% from total planned decrease in costs in amount of 7% stands for 7%*15% = 1.05% of increase in total hotel sales due to higher operating capacities provided by Ngnix-based web servers compared to Apache-based ones.

- Increase in speed of one request cycle and, thus, total number of cycles

2.2. Methodology of conducted technical, economic and investment evaluation of migration of Hyatt Regency Kiev databases located at Apache-based to Nginx-based servers

2.2.1. Data and methodology

Thesis aims to measure the impact of information security on performance of chosen hotel through investment evaluation of migration of Hyatt Regency Kiev databases from its Apache-based web servers to Nginx-based servers and on the basis of obtained results to make a set of recommendations for similar hotels from international hospitality chains which operate in Ukraine and other CIS countries and which plan to improve their information security and efficiency of their information systems by change of their web-servers. Following established practice, there have been conducted three types of analysis - technical, economic and investment – all based on data collected from hotel's management reports for 2017-2018 and Hyatt Regency growth and innovation strategy 2018-2022. Output of technical analysis served as input for economic analysis, particularly obtaining estimated average monthly cash flow generated under two scenarios: Scenario A – planned growth in sales with concurrent decrease in costs due to achieved economy of scale; and Scenario B – decrease in costs (cost saving) with no change in sales (i.e. sales remain at the same level after launching the Strategy as they were before it). Obtained cash flows will be used as input for further investment analysis and creation of average profile of the most possible outcome of migration of Hyatt's Regency Kiev databases from Apache-based to Nginx-based web servers.

2.2.2. Technical, economic and investment indicators

The following technical indicators are the main tools to measure performance of web servers[31]:

- Requests per Second (RPS) - is the evaluation of how many requests per second are processed at web server. Usually, this is calculated as a count of the requests received during a measurement period, where the period is represented in seconds. All else being equal, higher RPS is preferable to lower RPS since higher RPS stands for larger coverage of external and internal users of web server. In economic terms, it means higher number of requests from clients (customers as external clients and company stuff

[31] Indicators of web server. Available from WWW:<https://www.softwaretestinghelp.com/performance-testing-tools-load-testing-tools/>

as internal clients) to be responded concurrently. It implies higher sales and lower number of man-days to perform certain work tasks by company stuff.

- Error Rates - is calculated as a percentage of problem requests relative to all requests. Problem requests are the ones which never get a response (i.e. timed out requests). Error Rate measures how many failed requests have occurred at a particular point in time. Obviously, lower error rates are preferable to higher ones. Economical implication of lower error rate is similar to RPS: lower timed out requests bring less lost potential customers and help to minimize system outage for its internal users, meaning lower number of idle working hours.
- Average Response Times (ART) and Peak Response Time (PRT) - both measure the duration of every request/response cycle. They evaluate how long it takes the target web application to generate a response: ART measures average cycle, while PRT measures the longest one. The resulting metric is a reflection of the speed of the web application – perhaps the best indicator of how the target site is performing, from the users' perspective. Lower ART and PRT are preferable to higher ART and PRT, implying less lost potential customers and less working time spent on waiting for result from query sent to various databases (e.g. the ones used in producing financial reports by hotel's financial department).
- Uptime - is the amount of time that a server has stayed up and running properly. It reflects the reliability and availability of the server and, obviously, this value should be as large as possible. In economic terms, it implies less lost potential customers and helps to minimize system outage for its internal users, meaning lower number of idle working hours.
- CPU utilization and memory utilization - are the amount of CPU time used and memory used by web server while processing a request. Usually, it is the percentage of CPU usage and percentage of memory utilization (i.e. space for text, data) that is calculated, which indicates how much of the processor's and memory capacity is currently in use by particular web server. Lower value is preferred to higher one: when percentage of CPU usage begins to max out at 100%, additional action may need to be taken because that points to the existence of capacity deficiency of the host machine. Economical implication of lower CPU utilizations is as follows: lower utilization of CPU of each individual virtual server in the group of interconnected virtual servers helps to increase the number of requests from clients (customers as external clients and company stuff as

internal clients) to be responded concurrently. It implies higher sales and lower number of man-days to perform certain work tasks by company stuff.

- Count of threads – number of generated threads to process requests. If some web server generates too many threads it can be an indicator that there is a problem in the web server. Obviously, the count of existing threads is proportional to the load and inversely proportional to the processing time of the requests. Hence there should be reasonable number of threads, which would be proportionate to number of CPUs: increasing number of threads under the constant number of CPUs indicate problem with web server while decreasing number of threads (under the constant number of CPUs) indicate at the existence of idle time (for processing of both external and internal requests to web server).

The following financial indicators are the main tools used to measure change in key technical parameters of web server from monetary perspective[32]:

- Sales (bookings) – comparison of original sales (i.e. before change in any of technical parameters described above) and new sales (i.e. after change in any of technical parameters described above). Sales are good approximation for number of potential clients: higher sales caused by improvement of any of technical parameters of hotel web server indicate at the lower number of lost potential customers and, thus, lower unrealized gains for hotel.

Average hotel monthly sales =
Average number of reservations per month *
Average duration of stay (nights) *
Average daily rate of reservation *
Apportionment rate for monthly sales to utilization of
hotel web server
(1)

- Costs (web server maintenance costs and costs of idle working hours) – comparison of original costs and new costs. Web server maintenance costs and costs of idle working hours stand for a combination of: (1) labor costs of certain number and of certain qualification IT stuff responsible for maintenance of hotel web server (system administrators); and (2) labor costs of idle working hours of non-IT stuff whose work

[32] Financial indecators. Available from WWW:<https://www.investopedia.com/terms/>

is dependent on performance of web server (e.g. financial and business analysts extracting data from hotel databases located on its web server for reporting and management purposes). Web server maintenance costs are calculated as average daily wage of one system administrator multiplied by daily number of system administrators required to maintain hotel web server. Labor costs of idle working hours are calculated as average daily wage of one financial or business analyst using data from web server multiplied by daily number of such analysts and pro rated to number of idle working hours (days) due to server outage.

Average monthly hotel system outage costs =
Average number of timed out stuff requests per month *
Average duration of timed out request (minutes) * (2)
Average monthly payroll costs per FTE from finance
and/or marketing department

Average monthly hotel server maintenance costs =
Average monthly payroll costs per web admin (3)
* Number of web servers

Average monthly hotel data breach costs =
Average number of data breaches per month (incl. DDoS attacks) * (4)
Average penalty per breach (cost of outage due to DDoS attack)

Summary of Hyatt's key economic parameters before Strategy implementation, that is, before migration of hotel's databases from Apache-based to Nginx based servers as well as before launching marketing campaign and introduction of new type of product, is presented in Table 1.

- Investment – usually investment includes: (1) acquisition cost of new system/server, which is purchase price plus installation costs; (2) cost of disposal of original system/server; and (3) costs of training of employees to operate new system/server. Installation and disposal costs for change of web server are called migration costs and in case of shift from Apache-based to Nginx-based server, which are open source systems, migration costs will be the only pure IT costs since there is no purchase price for Apache and Nginx web codes.

Summary of Hyatt's key investment parameters connected with Strategy implementation is presented in Table 2.

The following investment ratios are the main mathematical ratios used to evaluate the efficiency of an investment[33]:

Table 2. Monthly profit input parameters for Hyatt Regency Kiev under Apache-based servers during 2017-2018

Monthly profit parameter	Amount
Panel A. Average monthly hotel sales (apportioned to hotel web server utilization)	
Average number of reservations per month	15
Average duration of stay (nights)	4
Average daily rate of reservation (UAH)	7,800
Apportionment rate for monthly sales to utilization of hotel web server	11,5%
Average monthly sales (UAH)	**53,820**
Panel B. Average monthly hotel web server outage costs	
Average number of stuff requests per month	510
Average duration of timed out request (minutes)	10
Average monthly payroll costs per reporting by FTE from finance and/or marketing department (UAH)	1,100
Average monthly hotel web server outage costs (UAH)	**11,688**
Panel C. Average monthly hotel server maintenance costs	
Average monthly hotel payroll costs per administration of one server (UAH)	1,304
Number of web servers	10
Average monthly hotel web server maintenance costs (UAH)	**12,783**
Panel D. Average monthly hotel data breach costs	
Average number of data breaches per month	0.67
Average penalty per breach	37,500
Average monthly hotel data breach costs (UAH)	**25,000**

Source: Author's own computations based on HRK annual reports 2015-2017

- Return on investment (ROI) - is performance measure used to evaluate the efficiency of an investment. It measures the amount of return on a particular investment relative to investment cost. Higher and/or positive ROI means that investment generates gains

[33] Financial indecators. Available from WWW:<https://www.investopedia.com/terms/>

relative to its cost. Lower and/or negative ROI means that investment generates loss relative to its cost. It is calculated as follows:

$$\text{ROI} = \frac{(Return - Cost\ of\ investment)}{investments} \times 100\% \qquad (5)$$

- Payback period (PP) – is the length of time required to recover the cost of an investment or to reach the break-even point. It intuitively measures how long investment takes to pay for itself. All else being equal, shorter payback periods are preferable to longer payback periods. It is calculated as follows:

$$PP = \frac{Costs\ of\ investment}{Annual\ Cash\ Inflows} \qquad (6)$$

- Net present value (NPV) – is the difference between present value of cash inflows and present value of cash outflows over a period of time. Positive net present value indicates that the projected earnings generated by investment exceed the anticipated costs. It is assumed that an investment with a positive NPV will be profitable, and an investment with a negative NPV will result in a net loss. It is calculated as follows:

$$NPV = -CI \quad + \frac{CF_1}{1+r} + \frac{CF_2}{(1+r)^2} + \cdots + \frac{CF_t}{(1+r)^t} \qquad (7)$$

where: $-CI$ = Cost of Investment

CF = Cash flows (inflows)

r = Discount rate

t = Time

Table 3. Investment parameters for transferring from Apache-based to Nginx-based servers of Hyatt Regency Kiev

Investment parameter	**Amount**
Release (time of web admins to switch from Apache to Nginx)	2 man days
Hourly rate (UAH)	1,100
2 months support	262,400
Total investment	280,000
Discount rate p.a.	35%

Source: Author's own computations based on HRK budget 2018.

2.3. Results of conducted technical, economic and investment evaluation of migration of Hyatt Regency Kiev databases located at Apache-based to Nginx-based servers

The obtained results indicate that highest positive variance after migration of Hyatt's web servers from Apache to Nginx is observed for such technical characteristics as count of threads (+67%) and error rate (-13%) (see Table 3, panel A). The highest negative variance is observed for change in such technical parameter as memory utilization (+22%). Practically this means that Hyatt's web servers can process by 67% more concurrent requests and that there are by 13% less timed out requests from internal and external users, meaning lower number of idle working hours and less lost potential customers. Opposite to this, increased number

Table 4. Comparison of impact of Scenario A and Scenario B during the transfer from Apache-based to Nginx-based servers of Hyatt Regency Kiev on hotel's monthly profit

Technical parameter	Impact on profit by Apache-based server (UAH)	Impact on profit by Nginx-based server (UAH)	Variance (UAH)	Variance (%)
Panel A. Comparison of technical parameters of Apache-based and Nginx-based servers of Hyatt Regency Kiev				
RPS (requests/sec)	60	65	5	8%
Error rate (%)	24	21	(3)	-13%
ART (sec)	548	552	4	1%
PRT (sec)	685	717	32	5%
Uptime (%)	99	99	-	0%
CPU utilization (%)	98	98	-	0%
Memory utilization (MiB)	14	17	3	22%
Count of threads	6	10	4	67%
Panel B. Comparison of impact on hotel monthly of transfer from Apache-based to Nginx-based servers of Hyatt Regency Kiev with sales growth and economy of scale (Scenario A)				
RPS (requests/sec)	8,290.45	13,477.90	5,187.45	63%
Error rate (%)	(4,512.20)	2,434.34	6,946.54	-154%
ART (sec)	2,908.45	2,473.68	(434.77)	-15%
PRT (sec)	217.45	(2,565.42)	(2,782.87)	-1,280%
Uptime (%)	2,908.45	2,908.45	-	0%
CPU utilization (%)	(2,256.10)	(2,256.10)	-	0%
Memory utilization (MiB)	(14,623.85)	(27,774.14)	(13,150.29)	90%
Count of threads	11,416.35	51,443.42	40,027.07	351%
Total impact on monthly profit	**4,349.00**	**40,142.12**	**35,793.12**	**823%**

Panel C. Comparison of impact on hotel monthly of transfer from Apache-based to Nginx-based servers of Hyatt Regency Kiev with cost saving (Scenario B)				
RPS (requests/sec)	8,290.45	14,478.01	6,187.56	75%
Error rate (%)	(4,512.20)	(3,589.20)	923.00	-20%
ART (sec)	2,908.45	3,471.45	563.00	19%
PRT (sec)	217.45	2,342.45	2,125.00	977%
Uptime (%)	2,908.45	-	-	
CPU utilization (%)	(2,256.10)	-	-	
Memory utilization (MiB)	(14,623.85)	(14,377.85)	246.00	-2%
Count of threads	11,416.35	20,044.35	8,628.00	76%
Total impact on monthly profit	**4,349.00**	**22,369.21**	**18,672.56**	**429%**

Source: Author's own computations based on HRK forecast for Strategy 2018-2022 implementation

of threads results in increase of idle time by 22%. As for characteristics which had not changed with transfer from Apache to Nginx are uptime and CPU utilization.

As for financial impact of change in technical parameters due to transfer from Apache to Nginx there have been done worked out two scenarios: Scenario A – planned growth in sales with concurrent decrease in costs due to achieved economy of scale; and Scenario B – decrease in costs (cost saving) with no change in sales. If we take a look first at Hyatt's profit margin

Table 5. Comparison of monthly profit parameters for Hyatt Regency Kiev under Apache-based servers (before the project) and under Nginx-based server (after launching of project)

Financial indicator	**Apache-based servers (UAH)**	**Nginx-based servers with sales growth and economy of scale (UAH)**	**Nginx-based servers with cost saving (UAH)**
Average hotel monthly sales	53,820	64,046	53,820
Average monthly hotel system outage costs	(11,688)	(5,647)	(8,940)
Average monthly hotel server maintenance costs	(12,783)	(6,177)	(9,777)
Average monthly hotel server data breach costs	(25,000)	(12,080)	(12,080)
Net impact on profit, monthly	**4,349**	**40,142**	**23,023**
Change in profit, monthly		**+35,793**	**+18,674**

Source: Author's own computations based on HRK annual reports 2015-2017 and underlying forecast for Strategy 2018-2022 implementation. Notes: for Apache-based server the average hotel monthly sales and average hotel server costs are actuals as per management reports 2015-2017 i.e. before launching implementation of Strategy; for Nginx-based server average hotel monthly sales and average hotel server costs are as estimates as per underlying forecast 2018-2022 i.e. after implementation of Strategy.

Table 6. Net value and net present value of transfer from Apache-based to Nginx-based servers of Hyatt Regency Kiev with sales growth and economy of scale

Month	Based on CF not discounted		Based on CF discounted	
	CF not discounted (UAH)	Net value (UAH)	CF discounted (UAH)	Net present value (UAH)
1.	0	(280,000.00)	0	280,000.00)
2.	35,793	(244,207.00)	33,793	(246,207.01)
3.	35,793	(208,414.00)	32,835	(213,371.71)
4.	35,793	(172,621.00)	31,905	(181,466.96)
5.	35,793	(136,828.00)	31,001	(150,466.40)
6.	35,793	(101,035.00)	30,122	(120,344.40)
7.	35,793	(65,242.00)	29,268	(91,076.06)
8.	35,793	(29,449.00)	28,439	(62,637.19)
9.	35,793	**6,344.00**	27,633	(35,004.27)
10.			26,850	(8,154.47)
11.			26,089	**17,934.40**

Source: Author's own computations based on HRK annual report 2015-2017 and underlying forecast for Strategy 2018-2022 implementation.

behavior under scenario A, we will see that financial impact of major technical parameters is in line with technical trend described in previous paragraph: the most significant positive impact on Hyatt's profit is observed from count of threads (+UAH 51k or 351% to Hyatt's server-dependent profit) and error rate (+UAH 6k or +154% to profit) (see Table 3, panel B) . Likewise memory utilization has the highest negative impact on Hyatt's profit: +UAH 13k (or -1,260%) to server costs which means -UAH 13k to its profit. Additionally to these technical parameters significant impact in financial terms have such parameters as RPS and PRT with +UAH 5k and -UAH 2k to Hyatt's profit respectively. It is interesting that materiality of these two parameters started to show themselves only after putting Nginx-based servers into production and this effect was not expected when they were in design and under testing.

If we take a look at Hyatt's profit margin behavior under scenario B, we can see that in general the significance and direction of impact of technical indicators described under scenario A remains more or less the same even under condition of no growth in sales: the most significant positive impact is done by count of threads (+ UAH 8k or +76% to Hyatt's server-dependent profit) and error rate (+ UAH 923 or +20%) (see Table 3, panel C). However, different to scenario A, under condition of sole cost saving without corresponding growth in sales, such technical parameter as memory utilization is no longer impacting negatively Hyatt's profit and the financial impact of PRT has changed completely: under scenario B, PRT is contributing to hotel's monthly profit in amount of +UAH 2k on average. Such change in direction of impact on profit by PRT and partially memory utilization can be explained by exceeding of technical capacities of these two parameters under such growth in sales as expected under scenario A. This is in line with microeconomic theory of cost behavior: fixed costs have U-shape, implying that after certain point in growth in scale, fixed costs stop demonstrating cost saving behavior but start to increase at growing rate.

Summary of total financial impact of migration Hyatt's servers from Apache to Nginix under both scenarios is presented in Table 4. Here we can see that despite overcoming by some fixed costs of their minimum point (particularly PRT), the highest cost saving is still reached under scenario A: +UAH 25k to average monthly server-dependent profit. To compare: under

Table 7. Net value and net present value of transfer from Apache-based to Nginx-based servers of Hyatt Regency Kiev with cost saving

Month	**Based on CF not discounted**		**Based on CF discounted**	
	CF not discounted (UAH)	**Net value (UAH)**	**CF discounted (UAH)**	**Net present value (UAH)**
1.	0	(280,000.00)	0	(280,000.00)
2.	18,674	(261,326.00)	17,631	(262,369.45)
3.	18,674	(242,652.00)	17,131	(245,238.55)
4.	18,674	(223,978.00)	16,645	(228,593.14)
5.	18,674	(205,304.00)	16,174	(212,419.46)
6.	18,674	(186,630.00)	15,715	(196,704.14)
7.	18,674	(167,956.00)	15,270	(181,434.20)
8.	18,674	(149,282.00)	14,837	(166,597.01)
9.	18,674	(130,608.00)	14,417	(152,180.31)
10.	18,674	(111,934.00)	14,008	(138,172.18)
11.	18,674	(93,260.00)	13,611	(124,561.03)
12.	18,674	(74,586.00)	13,225	(111,335.63)
13.	18,674	(55,912.00)	12,851	(98,485.04)
14.	18,674	(37,238.00)	12,486	(85,998.64)
15.	18,674	(18,564.00)	12,133	(73,866.10)
16.	18,674	**110.00**	11,789	(62,077.40)
17.			11,455	(50,622.79)
18.			11,130	(39,492.81)
19.			10,815	(28,678.25)
20.			10,508	(18,170.17)
21.			10,210	(7,959.90)
22.			9,921	**1,961.02**

Source: Author's own computations based on HRK annual reports 2015-2017 and underlying forecast for Strategy 2018-2022 implementation.

scenario B total cost saving is +UAH 18k. Also it should be noticed that regardless of growth in sales Nginix-based servers offer higher protection against hacker attracts: average monthly data breach costs, including costs of server outage due to DDOS attacks, under both scenarios are by almost +UAH13k lower than the ones under Apache. This can be explained by combined positive effect including costs of server outage due to DDOS attacks, under both scenarios are by almost +UAH13k lower than the ones under Apache. This can be explained by combined positive effect of technical parameters, particularly count thread and error rate, allowing increase in bandwidth capacity of Hyatt's servers, that is, increase in number of concurrently processed requests meaning more time for conducting additional data breach checks and DDOS attack checks such as additional traffic filters in Nginx using IP addresses, user agents, country or other data for each submitted external request.

To perform investment analysis we need to compose time-series for cash flows given by estimated increases in average monthly Hyatt server-dependent profit under scenario A and scenario B, which are +UAH 35,793 and +UAH 18,674 respectively.

Table 8. Investment indicators for transferring from Apache-based to Nginx-based servers of Hyatt Regency Kiev under Scenario A and Scenario B

Indicator	**Amount under Scenario A**	**Amount under Scenario B**
Panel A. Non-discounted CF		
ROI at the end of 1st year (%)	41%	-27%
ROI at the end of 2d year (%)	194%	53%
Payback period (months)	9 months	16 months
Net value at the end of 1st year (UAH)	113,723 UAH	(74,586 UAH)
Net value at the end of 2d year (UAH)	543,239 UAH	149,502 UAH
Panel B. Discounted CF		
ROI at the end of 1st year (%)	15%	-40%
ROI at the end of 2d year (%)	106%	7%
Payback period (months)	11 months	22 months
Net value at the end of 1st year (UAH)	43,284 UAH	(111,356 UAH)
Net value at the end of 2d year (UAH)	296,873 UAH	20,957 UAH

Source: Author's own computations based on HRK annual reports 2015-2017 and underlying forecast for Strategy 2018-2022 implementation.

Table 9. Average profile: moderate growth in sales with moderate cost saving based on discounted CF

Investment indicator	Amount
ROI at the end of 1st year (%)	-6%
ROI at the end of 2d year (%)	80%
Payback period (months)	13.5 months
Net value at the end of 1st year (UAH)	(15,651 UAH)
Net value at the end of 2d year (UAH)	223,188 UAH

Source: Author's own computations based on HRK annual reports 2015-2017 and underlying forecast for Strategy 2018-2022 implementation.

As it is stated in methodology, the investment indicators used for evaluation of efficiency of transfer from Apache to Nginx for Hyatt are ROI, Payback period and NPV. Table 5, 6 and 7 provide results of calculation of Payback period and net value of Hyatt's servers transfer based on non-discounted and discounted CF for both scenarios. As we can see from completed tables it will take Hyatt 9 months to reach break-even-point for its server-related part of Strategy 2018-2022 with assumption of constant growth in sales in combination with economy of scale (i.e. Scenario A) under non-discounted increase in its server-related monthly profit and 11 months in case when increase of server-related monthly profit is discounted (Table 5 and Table 7). Alternatively it will take Hyatt 16 months and 22 months respectively to pay back its investment into switch from Apache to Nginx with assumption sole cost saving (i.e. Scenario B) under non-discounted and discounted increase in its server-related monthly profit (Table 6 and Table 7). It is reasonable to assume that both cases when payback period is 9 months (i.e. outcome under scenario A with non-discounted CF) and 22 months (i.e. outcome under scenario B with discounted CF) are kind of outliers and the most close approximation to reality falls within 11 and 16 months and NPV at the beginning of 2020 in amount of UAH 223k (Table 8). This average estimated investment profile is in line with average value for ROI, payback and NPV for investments into IT/IS in Ukraine and other developing economies of CIS[34].

2.4. Recommendations for hotels from international hospitality chains which operate in Ukraine and other CIS countries planning to improve there IS security and efficiency by change of web servers

Based on obtained results of conducted technical, financial and investment analysis it is possible to make following recommendations for hotels from international hospitality chains

[34] CIS. Available from WWW:<http://renewablemarketwatch.com/country-reports>

which operate in Ukraine and other CIS countries planning to improve there IS security and efficiency by change of web servers:

1. Before making investment decision about improvement of any of their IS components, hotels need to undertake a complex analysis aimed to measure in monetary terms impact of individual technical parameters of that component (e.g. web servers) which will effected by the planned improvement on hotels' profit. This analysis should be based on actuals (i.e. impact of existing technical parameters on hotels' profit before realization of improvement) and on estimates (i.e. impact of new technical parameters on hotels' profit after realization of improvement). If variance in profit before and after realization of improvement is positive it means that improvement is value adding and it should be realized. If variance is negative it means that new technical parameters will not pay out and such improvement either needs to be rejected or changed.
2. Accuracy of investment analysis by approximately 70% depends on quality of input financial information regarding apportionment of hotel's operating costs and profit margin to its individual cost and profit centers. In case of Hyatt Regency Kiev there was available accurate calculation of server-dependent costs and sales (apportionment rates). Such kind of information is dependent on quality of hotel's managerial accounting.
3. As it is observed on example of Hyatt Regency Kiev the best outcome for realization of improvement in one of the components of hotel's IS, particularly its web servers, can be achieved under combination of planned cost saving brought by operation of new web server in combination with planned growth in sales. This will help to maximize value adding effect of using of new type of servers.
4. Replacement of one web server by another one allowing higher bandwidth capacity, that is, increase in number of concurrently processed requests will pay out for those hotels whose total users of their web servers for substantial extent are composed from internal users (i.e. external users and external users are approximately in equal proportion). Internal users cover marketing, accounting, reporting, customer relationship management departments. Such departments are internal users of hotel's web servers only when they are located inside particular hotel, that is, when they are not outsourced by third party company or located in the hotel headquarter (for Hyatt Regency Kiev it is Hyatt Hotels Corporation in Chicago, USA) or brought aside in form of shared service center. Only under such condition replacement of

one server by another one offering better bandwidth capacity will allow to decrease idle time of its internal users due to decreased time of server outage.

5. When estimating the cost of investment into most of components of hotels' IS, particularly their web servers, it is necessary to keep in mind that for purposes of internal control and year end audit after installation of new IS component it is required that old component and its replacement should run concurrently for some time. It is done in order to ensure that new component works as it is expected to work, that is, that all data is displayed by it correctly and in full extent (i.e. there are no missing data or duplicated data). Such concurrent operation of two component – old one and new one – imposes additional costs for the hotel and these costs need to be added to cost of investment. Usually they are included into costs of support of new system. Depending on impact of component over which there is conducted improvement, on hotels' profit, duration of such concurrent operation may vary from 2 months (like for web servers) and up to 2 years (in case of change in accounting software like transfer from old SAP to new SAP).
6. Depending on type of server - stateful server (containing databases) or statetless server (acting as transmitter of data for databases) – backup for period of database migration may be required. In case of Hyatt Regency Kiev its web servers are stateless that is why no backup was required. But in case of stateful servers backup will be required. That will impose additional costs for investment.
7. It is recommended for hotels which plan to change their web servers, in their strive to minimize investment costs not to refuse from after-production support. Besides providing backup in case of stateful servers, such support is aimed to ensure that external users keep using hotel web server as well as to be certain that hotel's web server is performing as planned. This includes many activates the major of which are: (1) informing of users that corresponding web site and /or database located at the impacted web server will be under migration; (2) change of DNS – once migration is started it is necessary to attach hotel's existing DNS record to its new server; (3) monitoring uptime of new server; (4) conducting complex checks of database migrated hasn't become corrupted during such migration.
8. Migration of databases from one web server to another one always requires good timing and high synchronization between hotels IT department with its other departments (e.g. marketing, accounting, reporting, customer relationship management) since with high probability there will be servers outage impacting

activities of server internal users from other departments. Definitely, it is not desirable to conduct such migration closely before, during or closely after interim and yearend financial closings.

CONCLUSION

Information is a fundamental asset for any business and protection of this asset, through a process known as information security, is of equal importance. Hospitality business has passed a long way to building its information security to that state as it is known today. Being one of the most frequent targets for cyber attacks, improvement of security of web servers has become one of the most popular types of investments into IS infrastructure of any business. Also besides their substantial contribution to information security of the business, web servers also represent quite material portion of total business costs and allocated profits. Thus by improving its web servers any business achieves two objectives: (1) increased protection against cyber attacks and internal fraud; and (2) reduction in operating costs, thus increase into profit margin of whole business. Especially it is important for companies which have become or are planning to become public.

With respect to all stated above, thesis aims to provide complex evaluation of efficiency of investment into its web servers undertaken by Hyatt Regency Kiev as part of realization of its growth and innovation strategy 2018-2022. Particularly, practical part of thesis provides evaluation of pay off of migration of Hyatt's databases from apache-based to Ngnix-based web servers. This is done by means of conducting a complex analysis comprising technical indicators (e.g RPS, error rate, ART, uptime etc.), financial indicators (e.g. monthly server-apportioned sales and server-apportioned costs such as maintenance costs, outage costs and data breach costs) and investment indicators (e.g. ROI, payback period, NPV).

As main contribution of thesis based on obtained results there is provided a set of recommendations which can be used as guidance when changing web servers by other hotels from international hospitality networks that operate in Ukraine and other CIS countries. These can be summarized as follows:

(1) Before making an investment decision about improvement of any of their IS components, hotels need to undertake a complex analysis aimed to measure in monetary terms impact of individual technical parameters of that component (e.g. web servers) which will effected by the planned improvement on hotels' profit.

(2) Accuracy of investment analysis to large extend depends on availability of accurate calculation of server-dependent costs and sales (apportionment rates), which in its turn depends on quality of hotel's managerial accounting.

(3) Replacement of one web server by another one allowing higher bandwidth capacity will pay out for those hotels who received requests from external users and internal users approximately in equal proportion.

(4) When estimating the cost of investment into most of components of hotels' IS, particularly their web servers, it is necessary to keep in mind that for purposes of internal control and yearend audit after installation of new IS component it is required that old component and its replacement should run concurrently for some time.

(5) Depending on type of server - stateful server or statetless server – backup for period of database migration may be required. That will impose additional costs for investment.

And as bottom line, the main recommendation is to conduct complex analysis aimed to measure in monetary terms the impact of individual technical parameters of web servers (or any other components of hotel information system over which there is a plan to conduct an improvement) on hotels' profit before and after realization of planned improvement.

LIST OF USED RESOURCES

BOOK SOURCES PAPER SOURCES

1. ANDERSONA, Evan, JOOBIN, Choobineha (2008). *Enterprise information security strategies. Journal of ScienceDirect* vol.27, 2008, 22-29 pp.
2. ANDRESS, Jason, (2011). *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice 1st Edition, Kindle Edition.* 240 pp. ISBN 0128007443.
3. BOLZONI, Damiano, (2006). *A Business Goal Driven Approach for Understanding and Specifying Information Security Requirements*. 96-98 pp.
4. Brealey, Richard, Myers, Stewart, 2011. *Principles of Corporate Finance.* 969 pp. ISBN 9781259144387
5. DLAMINIA, Mloses, ELOFFA, Mariki, ELOFF, Jan, (2009). *Information security: The moving target. Journal Semantic Scholar* vol.10, 2009, 32-35 pp.
6. FORTE, Dario, 2000. *Information Security Assessment: Procedures and Methodology." Computer Fraud & Security.* 100 p. ISSN 1361-3723.
7. HONG-BUMM, Kima., DONG-SOO, Leeb, SUNNY, Hamc, (2013). *Impact of hotel information security on system reliability. Journal of ScienceDirect* vol.35, 2013, 369-379 pp.
8. HSIANGTING, Shatina, Chena, JAIB Tun-Min (2018). *Cyber alarm: Determining the impacts of hotel's data breach messages. International Journal of Hospitality Management* vol.73, 2018, 100-103 pp.
9. KERRY-LYNN, Thomson, SOLMS, von Thomson, 2016. *Information security obedience: a definition. Journal of Computers and Science,* vol.24, 2005, 69-75 pp.
10. KIM, David, 2016. *Fundamentals of Information Systems Security (3rd Edition).* 570 pp. ISBN 978-1284116458
11. LAM, Doris, CHAN, Eric, (2013). *Hotel safety and security systems: Bridging the gap between managers and guests. International Journal of Hospitality Management* vol.32, 2013, 202-216 pp.
12. LAW, Rob, LEUNG, Rosanna, BUHALIS, Dimitrios, (2018). *Information technology applications. Journal of Travel and Tourism Marketing* vol.26, 2009, 599-623 pp.

13. LAW, Rob, LEUNG, Rosanna, BUHALIS, Dimitrios, (2009). *In hospitality and tourism: a review of publications from 2005 TO 2007. Journal of Travel and Tourism Marketing* vol.26, 2009, 599-623 pp.
14. MAULE-FFINCH, Ashleigh, (2018). *Cyber Security Europe. Key trends in information Security. Journal of Cyber Security*, vol.13, 2017, 113-118 pp.
15. MELI-AN-GONZALEZ, Santiago, BULCHAND-GIDUMA, Jacques, (2016) *A model that connects information technology and hotel performance. Journal of Information Management & Computer Security vol.53*, 2016, 30-37 pp.
16. SCHOU, Corey, 2014. *Information Assurance Handbook: Effective Computer Security and Risk Management Strategies (1st Edition).* 480 pp. ISBN 9780071821650
17. SHAMELI-SENDI, Alireza, EZZATI-JIVAN, Naser, JABBARIFAR, Masoume, (2012). *Intrusion Response Systems: Survey and Taxonomy, International Journal of Computer Science and Network Security*, vol. 12, no. 1, pp. 1-14.
18. SHAMELI-SENDI, Alireza, ROUZBEH, Aghababaei-Barzegar, CHERIET, Mohamed, (2014). *Cyber threats – approaches to cyber risk assessment. Journal of Ernst and Young*, vol.5, 2015, 17 pp.
19. SMITH, Richard, 2015. *Elementary Information Security 2nd Edition.* 866 pp. ISBN 978-1284055931.
20. SOLMS von Rossouw, NIEK van Johan, (2013). *From information security to cyber security. Journal of ScienceDirect* vol.38, 2013, 97-102 pp.
21. SOLMS, Reight, 1999. *Information security management (1): why information security is so important. Journal of Information Management & Computer Security vol.7*, 1999, 50-57 pp.
22. STAMP, Mark, 2011. *Information Security: Principles and Practice 1st Edition, Kindle Edition.* 606 pp. ISBN 0470626399.
23. THOMSON, Kerry-Lynn, SOLMS von Rossouw, (2004). *Information security obedience: a definition. Journal of ScienceDirect* vol.66, 2004, 36-40 pp.
24. WATKINS, Steve, 2013. *An Introduction to Information Security and ISO 27001:2013 – A Pocket Guide*. 48 pp. ISBN 9781849285261

ELECTRONIC RESOURCES

25. Cisco Annual Cybersecurity Repor. [online]. 2018. Available from WWW:<https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html>
26. Cyber security srtategy of Ukraine. [online]. 2018. Available from WWW:<https://ccdcoe.org/2018/10/NationalCyberSecurityStrategy_Ukraine>
27. European Cyber Security Organisation. [online]. 2018. Available from WWW:<https://ecs-org.eu>
28. European Data Protection Board. [online]. 2017. Available from WWW: <https://edpb.europa.eu>
29. European Union Agency for network and Information security. [online]. 2018. Available from WWW:<https://www.enisa.europa.eu>
30. Hyatt's international awards. [online]. 2018. Available from WWW:<https://www.kievcheckin.com/kiev-bars-restaurants-summer-terraces>.
31. In hospitality and tourism: a review of publications from 2005 to 2007. [online]. 2018. Available from WWW:<https://www.researchgate.net/publication/247495283A-Review-of-Personality-Research-in-the-Tourism-and-Hospitality-Context>
32. Information technology and information security in hotel operation in Ukraine. [online]. 2018. Available from WWW:<https://www.n-ix.com/is-ukraine-safe-software-development-offshoring-data-protection-information-security/>
33. Investments formulas. [online]. 2010. Available from WWW: <https://www.investopedia.com/terms/>
34. Legislative Activities in Ukraine. [online]. 2019. Available from WWW: <https://rada.gov.ua/en>
35. The technical indicators are the main tools to measure performance of web servers. [online]. 2015. Available from WWW: <https://www.softwaretestinghelp.com/performance-testing-tools-load-testing-tools/>

TABLE NAME

1. Comparion of Apache and Nginx by key technical and economical characteristics.
2. Monthly profit input parameters for Hyatt Regency Kiev under Apache-based servers during 2017-2018.
3. Comparison of impact of Scenario A and Scenario B during the transfer from Apache-based to Nginx-based servers of Hyatt Regency Kiev on hotel's monthly profit.

4. Comparison of monthly profit parameters for Hyatt Regency Kiev under Apache-based servers (before the project) and under Nginx-based server (after launching of project).
5. Net value and net present value of transfer from Apache-based to Nginx-based servers of Hyatt Regency Kiev with sales growth and economy of scale.
6. Net value and net present value of transfer from Apache-based to Nginx-based servers of Hyatt Regency Kiev with cost saving.
7. Investment indicators for transferring from Apache-based to Nginx-based servers of Hyatt Regency Kiev under Scenario A and Scenario B.
8. Average profile: moderate growth in sales with moderate cost saving based on discounted CF.
9. Average profile: moderate growth in sales with moderate cost saving based on discounted CF.

NAME OF FIGURE

1.Impact of IT on hotel performance

LIST OF ABBREVIATIONS

1. HIS – Hotel information system
2. ISRM - Information security risk management
3. Medalion PMS - Medallion Property Management System
4. CRM - Customer Relationship Management
5. MitM - Man-in-the-middle attack
6. DDoS - Distributed-denial-of-service
7. ECSO - European Cyber Security Organisation
8. SRIA - Strategic Research and Innovation Agenda
9. ENISA -European Union Agency for Network and Information Security
10. EDPB -European Data Protection Board