Stanclik Miłosz

Walkowiak Tomasz
Wrocław University of Technology, Wrocław, Poland

Risk in systems with virtualization – test case analysis

Keywords

virtualization, risk analysis, threats

Abstract

The paper presents an approach to risk analysis of exemplar test case information systems. Authors point out the common practice to implement virtualization and put away security considerations for future[5]. The overview of virtualization techniques, focusing on server virtualization is given. Next, authors present risk analysis of exemplar GIS system. First of all identification of threats is taken out focusing on virtualization aspects, but it also includes common threats for both that could have a significant impact on safety when using a virtualization. The risk assessment for the test case system was performed using qualitative method. Assessment of the likelihood and magnitude of impact of identified risks was performed on the basis of the expert's knowledge and experience. The obtained results were used to develop risk rankings, which indicate the risks that need special attention when designing and managing a virtual system.

1. Introduction

IT industry is nowadays affected by virtualization trend. Increasing popularity of virtualization was born since it became clear that virtualization is supposed to help companies save money on IT costs. Virtualization advantages encourages business owners to invest in it. However, they should also take in consideration the risks, dangers and weaknesses of this technology. Report [5] indicates that only 29% of examined organizations claim that security of virtual systems is a major concern for future development. In general, people believe that virtualization is secure technology without the requirement of any additional protection. This is the result of insufficient knowledge of technology and its characteristic [5]. It is a common practice to implement virtualization and put away security considerations for future [17]. Although, it is true that virtualization has a lot of advantages in terms of security. Virtual machines running in isolated manner with limited direct access to underlying hardware. Virtualization supports the backups and rollback feature, which allows to recover virtual machine after security breaches [10]. Most common result of faith that virtualization is a secure technology by itself is fact that virtual infrastructure security is not adopted to the real needs [7]. Another consequence, is using the same security measures as for physical systems [5].
Therefore, it is important to apply risk analysis in virtualized IT systems. And this is the main goal of the paper: risk analysis of exemplar information system. Risk analysis is used to ascertain the consequences of making a decision, when these cannot be a priori determined. It is now used in all major planning activities. The term "risk" is used in decision-making, when the results of the decisions cannot be predicted [15][16]. Therefore, in any cases where decision is made to implement new technology, risk analysis should be performed as a part of risk management process. By identifying and assessing potential risks and issues, it is possible to take appropriate actions to reduce the effects of those risks.
The paper is organised as follows. First of all, review of virtualization techniques is presented, it is followed by description of the risk assessment method. Next, the test bed system is presented and threats are identified. It is followed by the risk assessment based on a qualitative approach [3], [16]. In addition, the risk ranking [11] is drawn up. It provides information of the risks in the system that should be given special attention.

2. Virtualization techniques

The term virtualization refers to methodology of dividing the computer (or server) resources (the CPU, memory, disk drives, network interface cards and so forth) in to multiple separate execution environmental achieving by many mechanisms such as hardware partitioning, time-sharing, partial or complete machine simulation, emulation and others. The resulting environments which are called virtual machines, should ensure efficiency as high as possible[30]. Virtual machine can provide illusion of hardware or hardware configuration that is not installed on the host computer. In spite of being a kind of abstraction, a virtual machine operates the same as a physical computer. It behaves the same as physical machine, includes the same components (CPU, RAM, hard disk, network interface card), runs its own operating system and applications, but is made entirely of software. That ability is purpose why virtual machines are completely independent from their underlying physical hardware. The virtual machine will be working properly independent of its configuration and types of virtual components. Virtual machines residing on the physical server can run different kinds of operating systems (guest operating systems), but they are isolated from each other. Even if one of virtual machine is broken it has no impact on the other which still remain available. Isolation results in a higher level of security and availability than in traditional, non-virtualized systems [18]. What is more virtual machine is encapsulated in to a set of files. It consists of a configuration file, virtual disk file and other necessary files, all in the one directory what is essence of encapsulation [26]. Virtual machine files can be manage like other files what makes it easy to portable.

2.1. Hypervisor

The software (virtual machine monitor) that provides the abstraction of a virtual machines [18] is called nowadays hypervisor. It is intended to manage multiple operating systems and to provide resources which each OS requires [23]. Additionally virtual machine monitor must fulfill three obligatory conditions: equivalence, resource control, efficiency. Because of the way of deployment and acting, there are two types of hypervisors: Type 1 and Type 2 [8].

Type 1 hypervisor is installed directly on top of the physical hardware without any operating system beneath it. Hypervisor acts like a layer, which controls the underlying hardware, manages resources and monitor the guests. It typically has components found in nowadays operating systems, for example device drivers. It is responsible for running a guest OS, which means that it has to partition and share the CPU, memory and I/O devices to successfully virtualize the system. Type 1 hypervisor is generally recommended solution for virtualization, as it provide higher virtualization performance by dealing directly with hardware resources. Higher efficiency is also provided by using hardware assisted technology which is introduced to the latest Intel's (Intel VT) and AMD's (AMD-V) processors [2]. VMware ESXi and Citrix XenServer are being Type 1 hypervisors.

Type 2 hypervisor called also hosted hypervisor is under the control of the host operating system like any other application. The virtualization software depends on the host operating system which provides and handles access to underlying hardware. Using Type 2 hypervisor allow to support a wide range of hardware which is inherited from operating system. Usually installation and deployment is easy since a lot of configuration work is done by operating system [31].

Unfortunately, there are several disadvantages from the point of view of enterprise. Architecture with hosted hypervisor is not as efficient as Type 1[1]. Additional layer in form of operating systems causes that more operations have to be performed when guest's resource request is serviced. Performance may also suffers from memory footprint of hosting operating system. Type 2 hypervisors are also less reliable by more points of failure. Any affection of operating system impacts the hypervisor and guests it supports. A simple example may be situation when standard operating system patches require reboot. Then except the host operating system all virtual machines are forced to reboot [25]. The most popular products using Type 2 hypervisor are Microsoft Virtual PC, VMware Workstation and Oracle VM VirtualBox.

2.2. Virtualization benefits

Moving business into virtualization brings undoubtedly many benefits. First, server consolidation allows to increase the utilization of physical servers. Many servers use only 10 to 15% of hardware resources [25], thus other resources are wasted. Such a solution is very unprofitable. Virtualization gives the way to better utilization of resources. Moving processing environments to virtual machines decreases the number of physical machines with utilization ratio up to 90% [25]. Fewer servers also reduce the costs of power consumption as well as money spend on hardware maintenance while organization becoming more green.

Each guest operating system deployed on the server running in isolation manner, which is crucial for a secure and reliable environment. Any guest's fault appearing in the virtual system cannot be spread on the others while virtual machines' operations are separated from each other. This feature keep virtual environment safer. Additionally to increase security level, during configuration security settings can be assigned to virtual machines rather than to the server. It relates especially to the access privileges. In standard operating system each application in general run with administrator access. However under virtualization applications can be run on the designated virtual machines, each may be configured with different credentials and different privilege access.

Hardware management is one of the biggest challenge that organizations are faced with. Each failure or hardware upgrade can take hours to restore server operability. Virtualization makes the virtual infrastructure management more convenient and efficient. Since operating systems are independent from the hardware they can be easily moved to another server. This is key feature when server's memory capacity gets low especially it takes only a few minutes. A storage virtualization gives also better way for data management. Data centralization makes data access much easier when it can be assigned as a single logical entity instead of being separated along several individual physical servers.

To protect business continuity virtualization provides also disaster recovery mechanism. Disaster recovery ensure that when virtualized system crash, it will be restored as quick as possible. With system allows to take snapshots of current state of system each virtual machine can be backup from any time, for example from last week. What is more such mechanism is used for data replication keeping data consistent and up to date.

3. Risk analysis

The risk analysis is the process of identifying and assessing risks. Identification of risk is based on gathering and analyzing information about company assets, threats and vulnerabilities that could potentially affect the breach of security. Risk estimation is related to determination of the possibility of potential event occurrence and losses which may be caused by it. There are various alternative approaches to risk assessment [16]: qualitative and quantitative. Most popular is the qualitative approach, based on expert opinions [3]. The basis of this analysis is to classify the identified threads in accordance to the probability of their occurrence and the gravity of their consequences.

We propose to use a common approach: a scale from 1 to 5 when assessing the likelihood and magnitude of impact associated with a given threat. Therefore, the level of risk is estimated with the formula [21]:

$$Risk\_level = likelihood \times magnitude \quad (1)$$

The resulting value will is mapped to the adopted scale describes the size of the risk in linguistic values. The level of risk will be described using the following scale:

- 1 – 4: low risk,
- 4 – 12: medium risk,
- 15 – 25: high risk.

In addition, the designated risk level is the main criterion in drawing up the risk ranking [10], based on which one can classify threads.

4. Test case system threats identification

4.1. Testbed overview

The object of performed risk analysis is geographic information system (GIS). IT infrastructure, on which geographic information system operates is based on virtualization technology. GIS is a computer system intended to store, manage and present geospatial information – information specific for particular location [4]. The infrastructure consists of 8 servers, disk array, tape library and network equipment (router and 3 switches). From a pool of physical servers eight virtual machines are created, on which Windows Servers are installed. All eight servers are connected in a VMware HA cluster, under control of VMware ESXi hypervisor. The purpose of this solution is unbreakable high availability of the system, regardless of the efficiency of each server. The use of such a solution results from VMware policy, which assumes that if all servers are available, is best to keep each virtual machine separate on the server, which delivers high performance. The advantage is that if a server failure occurs, hosted virtual machine is moved up and running on the server that is the least loaded at the time. Servers and virtual machines are managed in fact from another virtual machine, VMware vCenter Server.

In case of any failure in the system D2D2T (disk-to-disk-to-tape) backups are generated. It is the most popular backup strategy based on storing of the same data simultaneously on disk array and tape. This type of backup assumes that a backup is stored on the disk, and then stored on a magnetic tape media. As a result two backup copies are created. It is a protection in case something goes wrong during

the data restoring. Then a second equivalent of a copy, stored on the tape, can be used. Access to the network from the outside is protected by router with a firewall. Device is accessible only from the local network. Outside traffic is monitored by IDS (Intrusion Detection System) and IPS (Intrusion Prevention System) mechanisms which provide protection against DoS (Denial of Service) and Flood Attacks.

4.2. Threats identification

Described virtualized system is a subject to the same risks as any physical system. It exposures to the risks associated with the environment flooding, lightning and various types of accidents caused by external factors is on the same level. However, the use of virtualization technologies in the described system introduces new threats and new surface of attack, unique to this technology. The threats identification took into account only those of the common threats to physical and virtual systems, which can have a significant impact on the proper operation of the system.
We have divided threads into three groups:

- human mistakes - all threats that are a consequence of unawareness or errors related to activities designed to manage the entire virtual infrastructure;
- malware-based - it includes all activities intended to harm the system;
- failures - all threats related to hardware or equipment failures.

4.3. Human mistakes

Human operators have a huge impact on the proper and secure operation of the system. Therefore, especially in systems with virtualization, it is recommended to pay special attention to the training of personnel. Such actions are designed to prevent committed errors and their consequence. One of the biggest mistakes made in systems with virtualization, also in the analyzed system is the lack of adequate protection for the virtual infrastructure [24]. Use of the same security controls as for physical systems does not guarantee security for virtual machines running on servers. Following human mistakes were identified:

- Inadequate protection - system using virtualization will be secure if appropriate and comprehensive protection for each of the virtual components are ensured. The analyzed system, like most of the virtual systems used safeguards characteristic for standard physical system [5]. There is no additional protection for both the hypervisor and virtual machines, which makes the acquisition of the system to be not a difficult tasks.
- VM sprawl - should be understood as the expansion of virtual environment, in which there is a large number of virtual machines [9]. It can lead to disorder in the system. Lack of control over the virtual machines results that they are not updated and patched, which makes them an easy target [28].
- Misconfiguration - virtual machines are created from the default. Configuration intended to ensure the safety of virtual system components must involve many more options than the default configuration [9][28]. Omission of additional configuration makes possible to take control of the system is a simple task.
- VM rollback - although virtual machine rollback is consider as security benefit, it should also be treat as a threat [6]. Administrator of the system using virtual machine snapshots can revert the virtual machine to previous state at any time [10]. This may cause that also all changes, updates or patches made for improving security of virtual machine will be discarded.
- Dormant VM - is a virtual machine that is not used actively, so it can be easily overlooked and omitted in security procedures[24]. This causes that dormant virtual machines are more exposed to threats, by not being patched and updated [6]. Thus it creates a potential back door to the system.
- Deletion files in virtual file system, reformat - accidental deletion of data is the threat, which is considered as an unintentional human error [20]. In the case of the analyzed system, we can take into account the removal of virtual machines with all data. Such mistake not only disturb the integrity of the data, but also to disable the whole system.
- Damage of virtual disk files - can be caused by improper administration of the infrastructure and ignoring the messages sent by the system management software. Virtual infrastructure is managed from within VMware vCenter as a high-availability cluster. It is recommended to manage the infrastructure as a cluster rather than single virtual machine. Any such attempt is preceded about information that this may cause damage to the virtual disks. However, it is most often overlooked.
- Loss of performance - threats associated with the limited resources of the server on which virtual machines are hosted. The system architecture assumes one virtual machine on a single server, to ensure high performance. However, if you need to create new machine/machines, resource utilization rate will grow, which can adequately reflect on the performance.

4.4. Malware-based threats

Systems with virtualization, just like any others are exposed to malicious human action. It is not specified that it must be a hacker who breaks into the play to a virtual machine, or a cyber-criminal who wants to steal the stored data. Systems can be threaten as well by malicious employees, former or current, who can take advantage of the privilege and the lack of adequate safeguards to harm the company. Following malware-based threats were identified:

- Hyperjackig - the attack aimed at taking control of the server. The attack can be performed by installing rogue hypervisor beneath or on the top of the original hypervisor and by direct acquisition hypervisor [14]. An attacker can not only steal all the data, but also leave himself the opportunity to come back as soon as he wanted to steal more data. The usual safety measures are ineffective, because the guest operating systems running on the hypervisor will not have any awareness that the server was taken.
- VM escape - one of the most common virtual systems security issues [28]. The attack is based on malicious code running in a virtual machine. It allows the operating system to work directly with the hypervisor. In consequence is virtual machine encapsulation failure. Moreover, such an attack can give the attacker access to other virtual machines on the server.
- VM hopping - the attack similar to VM escape. In general, this is a process of "jumping" from one virtual machine to another [14]. If an attacker gets access to one virtual machine, it can be used to gain access to other virtual machines hosted on the same server.
- VM poaching - attack similar to a Denial-of-service attack. The aim of the attacker is to overload the hypervisor, so it eventually can stop working [13]. VM poaching involves one of the guest operating system to use resources (CPU, memory) remaining for other guests running on the same server. In this way, the hypervisor is completely consumed, so the other virtual machines "starving". The attack can cause degradation of performance. In the worst case, vm poaching resulting a total loss of system availability.
- VM theft - theft of a virtual machine, which then can be run anywhere. This is equivalent to theft of physical server. Virtual machines consist of several files and can be moved from one server to another even on a portable memory device [6]. Then it can be imported to and executed under VMware Player [29]. To steal virtual machine files the attacker must have access to the disk array storing the images of virtual machines or to the hypervisor. For this purpose, remote access may also be used. In the worst case, after copying, virtual machines can be removed by attacker.
- vCenter compromising - as the virtual machines are managed by VMware vCenter, it creates an additional point of attack in the system. VCenter is implemented as an additional virtual machine, so attacker could potentially try to take control over this machine to obtain an advantage or harm.
- Unauthorized access - occurs when an unauthorized person gains access to the system [24]. No matter if it will be access to VMWare vCenter, to single virtual machine or to the hypervisor. The effect and consequences in each case are the same - the whole system, as well as stored and processed in the data will be intercept.
- Abuse of privileges - the issue concerning on administrators and those having the highest level of privileges to the system and infrastructure [9]. In the worst case, they can use their permissions to harm the organization for example, by deleting data, or creating a back door to the system for themselves or others.
- Sniffing the traffic between virtual machines - virtual machines running on the server are able to communicate with each other using the virtual network. Virtual switch is the hypervisor's component that has the ability to monitor traffic between virtual machines and the hypervisor [24]. Unfortunately, the lack of additional mechanisms for protecting the traffic between virtual machines cause that it is transparent to the standard network devices[22]. This gives the opportunity to the attacker, who can take over the traffic and use it to compromise the whole system.
- Sniffing the transmission during virtual machine migration - migration is the process of moving virtual machines from one physical server to another. This is a significant feature of a virtual environments facilitating the system's maintenance [10]. Most often during the migration, the data is transmitted using plain text, which makes it very easy to intercept. What is more, attacker can manipulate the transmission and change the state of virtual machine that being moved [12].
- Virtual machine image modification - an attacker having access to the virtual machine images (stored on the disk array) can make some modifications, for example by injecting malicious code or infected files [12].
- Physical damage of server - a person with physical access and intended to harm the organization can destroy the servers that are running virtual machines. This can lead to both the loss of data, as

well as interruption of the entire system, which causes the loss of the system availability.

4.5. Failures

Failures are critical to business continuity and system availability, while difficult to predict their occurrence. The analysed system has already experienced several failures within last year. It was twice the power failure and failure of the disk array. In particular, the effects of the latter have a significant impact on the system. Since the virtual machines' disks are stored in the matrix of virtual machines, the failure resulted in temporary (1 day) disability of the system.

Following failures were identified:

- Disk array failure - disk array, as a central data storage subsystem is a critical resource. Failure results in disabling and interrupting continuity and availability of the whole system. In the worst case disk array failure can even cause data loss.
- Virtual disk file failure - damage to the virtual disk files is a very common case [20]. Most often associated with a temporary loss of availability associated with the restoration of a virtual machine because backuping is performed on an on-going basis.
- Server failure - failure of a single server has no significant impact on the continuity of the system. The use of high-availability cluster solutions, ensure that virtual machine hosted on the server, after server's failure will be transferred to the least loaded server. However it may be associated with a decrease in performance.
- Power supply failure- threat that can disrupt the system operation. By applying the redundant power suppliers and UPS the system can work for some time in spite of failure. Detected quickly will not cause longer interruptions in a computer system.
- Cooling failure - air conditioning is an integral part of each server room. Its failure could lead to the exclusion of servers when the temperature is above accepted level [27].

5. Risk assessment results

The risk assessment was performed by experts with years of experience in the administration of systems, both physical and virtual. The risk assessment results are placed in three tables (Table 1-3), following threads identified in previous chapter. Columns marked L present the likelihood values assessed by experts. Columns marked by M give value of magnitude, RL – risks level and RP - the threat ranking within a given group.

Table 1. Risk assessment for threats based on human mistakes

Threat	L	M	RL	RP
Inadequate protection	5	4	20	1
VM sprawl	4	3	12	3
Misconfiguration	5	4	20	1
VM Rollback	3	3	9	4
Dormant VM	2	3	6	5
Deletion files in virtual file system	3	4	12	3
Damage of virtual disk files	4	4	16	2
Loss of performance	2	2	4	6

Table 2. Risk assessment for malware-based threats

Threat	L	M	RL	RP
Hyperjackig	2	5	10	3
VM escape	3	5	15	1
VM hopping	3	5	15	1
VM poaching	2	4	8	4
VM theft	3	5	15	1
VMware vCenter compromising	3	5	15	1
Data leakage from virtual machine images	2	4	8	4
Unauthorized access	2	5	10	3
Abuse of privileges	3	5	15	1
Sniffing the traffic between virtual machines	2	4	8	4
Sniffing the transmission during migration	1	5	5	5
Virtual machine image modification	3	4	12	2
Physical damage of server	1	5	5	5

Table 3. Risk assessment for failure threats

Threat	L	M	RL	RP
Disk array failure	2	4	8	2
tual disk file failure	3	5	15	1
Server failure	2	2	4	4
wer supply failure	3	2	6	3
Cooling failure	2	4	8	2

As presented in the *Table 1*, the system is particularly exposed to two types of risk from human mistake group: inadequate protection and misconfiguration. By making use of the mechanisms designed primarily to protect the physical layer virtualization system is not adequately protected. This issue can be especially important if the attacker would gain access to the system. As there are no additional mechanisms to protect both hypervisors and virtual machines, an attacker could have possibly opened door to all system assets. Another risk, occupying first place in the risk ranking is misconfiguration. The most frequent causes of poor configuration is use of the default vendor's settings and a lack of knowledge of the people involved in the system management. Therefore, if the organization decides to use virtualization of servers, this should go hand in hand with administrators training. Misconfiguration could be bypassed due to creation of library containing ready-made, securely configured virtual machine templates. In other hand, loss of performance risk is at the bottom of the risk ranking. System availability is well protected by implementation of high-availability cluster as well as the assumption that single virtual machine is running on single server. This significantly reduces the likelihood of system downtime and loss of performance.

While analyzing the assessment and ranking of risk associated with malware-based threats it is easy to see (*Table 2*) that they pose a serious risk to the system. This is especially in two elements: the unpredictability and the size of damage that can be done. The unpredictability of the risks is linked to the fact that it is not possible to estimate when the system may be attacked. Therefore, administering both the virtual and physical systems all duties must always be performed with awareness that some adverse event may potentially occur. Chance to overcome the safeguards according to assessment performed by expert, is not especially large. However, if such an attempt would be successful the attacker would have full access to system assets, which can result in huge losses. Threats from the top of the ranking – vm escape, vm hopping, vm theft or vCenter compromising – could be done by lack of security for virtualization layer. However, implemented safeguard is enough to decrease the likelihood of system compromising. Least possible risk threaten to the system is physical damage of servers. Similarly to the risks associated with malware-based threats, likelihood of failure (*Table 3*) is average at best, but is also characterized by unpredictability. Risk associated with physical hardware has been greatly reduced by the use of redundant power supplies and storage. However, it should be remembered that handling as well as utilizing the equipment should carried with carefulness. The highest value of risk is calculated for risk related to virtual disk file failure. Often there is no reason for this, or it is done during attempts to transfer the virtual machine. Thus, when performing backups or migrate virtual machines, it must be assurance that the machine is still operational.

6. Conclusion

Summarizing, we have presented the risk analysis for the test case GIS system. The risk assessment was performed using qualitative methods of risk analysis with expert knowledge. Carrying out risk analysis using quantitative methods was not possible due to the small amount of historical data concerning on the test case system operation. The analysed system was a specific one, having specific safeguards and using particular solutions. Thus, risk analysis results could be considered as limited and deficient. However, systems, such as analysed, using typical security measures designed for physical systems represents about 60% of all virtualized ones [5], [7]. Therefore, the identified threats may be served as a benchmark for those who respond for virtualized systems' security.

The most dangerous identified threads are connected with human mistakes: inadequate protection and misconfiguration, the second level of importance includes: VM escape, VM hopping, VMware vCenter compromising, abuse of privileges and virtual disk file/disk failure.

The results show that some significant security risks are not directly related to the virtualization technology, but to the operational and management factors. It is worth mentioning here misconfiguration or abuse of privileges. This shows how important the functionality of the virtual system plays a human factor. Staff errors are mainly

due to a lack of knowledge and experience. The results of the risk analysis can provide the input for the next stage of the risk management process - risk treatment.

Acknowledgment

The presented work was supported by the Polish National Science Centre under grant no. N N516 475940.

References

[1] Barrett, D. (2010). *Virtualization and Forensics: A Digital Forensic Investigator's Guide to Virtual Environments*. Waltham: Syngress. 10-12.

[2] Fisher-Ogden, J., *Hardware Support for Efficient Virtualization*, University of California, San Diego. Available at http://cseweb.ucsd.edu/~jfisherogden /hardwareVirt.pdf (access: 15.03.2013).

[3] Flyvbjerg, B. (2006). From Nobel Prize to Project Management: Getting Risks Right. *Project Management Journal* 3, 37. 5-15.

[4] Folger, P. (2011). *Geospatial information and Geographic Information Systems (GIS): An Overview for Congress*. Congressional Research Service, Raport 41825.

[5] Forrester Research (2012). Virtual Security in the Data Center. Available at http://www.cisco.com/en/US/solutions/collateral/ns224/ns945/tap_virtual_security_032012.pdf (access: 15.03.2013).

[6] Garfinkel, T. & Rosenblum, M. (2005). When Virtual is Harder than Real: Security Challenges in Virtual Machine Based Computing Environments. *Proc. 10th Workshop on Hot Topics in Operating Systems*. 121-126.

[7] Gartner Press Release, Gartner Outlines Six Most Common Virtualization Security Risks and How to Combat Them, http://www.gartner.com/newsroom/ id/1322414 (access: 15.03.2013).

[8] Goldberg, R.P. (1973). *Architectural Principles for Virtual Computer Systems*. Harvard University.

[9] Hietala, J. (2009). *Top Virtualization Security Mistakes (and How to Avoid Them)*, SANS. Available at http://www.sans.org/reading_room/analysts_program/McAfee_Catbird_Virtualization_Jul09.pdf (access 07.03.2013).

[10] Hoopes, J. (2009). *Virtualization for security: including sandboxing, disaster recovery, high availability*. Waltham: Syngress. 10, 20-25.

[11] Hopkin, P. (2010). *Fundamentals of Risk Management*. London: Kogan Page Limited. 28-31.

[12] IBM, (2010). IBM X-Force 2010 Trend and Risk Report. Available at http://public.dhe.ibm.com/common/ssi/ecm/en/wgl03007usen/WGL03007USEN.PDF (access 07.03.2013).

[13] Information Security Blog (2010). Attacks with Virtualization, http://shobhajagathpal.blogspot.com/2010/02/attacks-with-virtualization.html (access: 18.03.2013)

[14] ISACA, (2010). Virtualization: Benefits and Challenges. Available at http://www.isaca.org/KnowledgeCenter/Research/ResearchDeliverables/Pages/Virtualization-Benefits-and-Challenges.aspx (access: 18.03.2013).

[15] Kahneman, D. & Tversky, A. (1979). Prospect theory: An analysis of decisions under risk. *Econometrica* 2, 47. 313–327.

[16] Kaplan, S. & Garrick, B.J. (1981). On the Quantitative Definition of Risk. *Risk Analysis* 1, 1. 11-27.

[17] Kaspersky Lab, (2012). Implementing Virtualization and Providing IT Security in Virtual Environments. Available at http://media.kaspersky.com/documents/business/brfwn/en/GCC-trends-in-the-corporate-market-sector-white-paper.pdf (access: 18.03.2013).

[18] King, S.T., Dunlap, G.W. & Chen, P.M. (2003). Operating System Support for Virtual Machines. *Proc. of the 2003 Annual USENIX Technical Conference.*

[19] Kragh, E., Faber, M.H. & Guedes Soares, C. (2010). Framework for integrated risk assessment. *Safety and Reliability of Industrial Products, Systems and Structures*. London: Balkema.

[20] Kroll, O. (2011). *Data Loss in a Virtual Environment.* Available at http://www.krollontrack.com/library/odrdataloss_krollontrack2011.pdf (access: 15.03.2013).

[21] Landoll, D. (2011). *The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments*. Boca Raton: Auerbach Publications. 436-446.

[22] Lynch, D.M. (2008). *Understanding VirtSec: An executive overview of server virtualization security issues including best practices for maintaining your security profile*. Embotics Corporation.

[23] Neiger, G., Santoni, A., Leung, F., Rodgers, D. & Uhlig, R. (2006). Intel Virtualization Technology: Hardware support for efficient processor virtualization. *Intel Technology Journal*. 167-177.

[24] PCI Security Standard Council, (2011). PCI Data Security Standard. Available at https://www.pcisecuritystandards.org/documents/Virtualization_InfoSupp_v2.pdf (access: 15.03.2013)
[25] Portnoy, M. (2012). Virtualization Essentials. Indianapolis: *Sybex.* 9, 20-27.
[26] Rosenblum, M. (2004). The reincarnation of virtual machines. *Queue* 2, 5. 34-40.
[27] Seymour, M., Aldham, Ch., Warner, M. & Moezzi, H., (2011). The Increasing Challenge of Data Center Desing and Management: If CFD a Must? *Electronics Cooling*, December 2011. 28-33.
[28] Shackleford, D. (2012). Virtualization Security: Protecting Virtualized Environments. Indianapolis: *Sybex*.
[29] Siebert, E., *How to steal a virtual machine and its data in 3 easy steps*, http://searchvmware.techtarget.com/news/1378347/How-to-steal-a-virtual-machine-and-its-data-in-3-easy-steps (access 07.03.2013).
[30] Smith, J.E. & Nair, R. (2005). The Architecture of Virtual Machines. *Computer* 5, 38. 32-38.
[31] Victor, J., Savit, J., Combs, G., Hayler, S. & Netherton, B. (2011). *Oracle Solaris 10 System Virtualization Essentials*. New Yersey: Prentice Hall.