A Review of Information Security Preparedness Evaluation Mechanisms in Law Enforcement Agencies

Article *in* IOSR Journal of Computer Engineering · April 2016

DOI: 10.9790/0661-1804055863

2 authors:

s. Ndichu
National Institute of Information and Communications Technology
12 PUBLICATIONS **120** CITATIONS
SEE PROFILE

Patrick Ogao
Makerere University
43 PUBLICATIONS **365** CITATIONS
SEE PROFILE

IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 18, Issue 4, Ver. V (Jul.-Aug. 2016), PP 58-63
www.iosrjournals.org

A Review of Information Security Preparedness Evaluation Mechanisms in Law Enforcement Agencies

Samuel W. Ndichu[1], Prof. Patrick J. Ogao[2]
[1](Department of Computer Science, Maseno University, Maseno, Kenya)
[2](School of Computing & I.T, Technical University of Kenya, Nairobi, Kenya)

Abstract: *Law enforcement agencies being the primary security organs in a country are highly prone to information and network attacks due to the sensitivity nature of the information they deal with in their day to day operations. Information security preparedness requires a consideration of both technical and nontechnical solutions to information security. This paper presents a review of information security preparedness evaluation frameworks, approaches, methods and models available today which the law enforcement agencies and other organizations can use to quickly and reliably evaluate the current security state of their information and or network. The paper also highlights the weakness in each of these mechanisms and points towards a more comprehensive framework for information security preparedness evaluation in law enforcement agencies.*

Keywords:*Information security, preparedness, framework*

I. INTRODUCTION

Law enforcement agencies are institutions that provides justice platform for the citizens of a country for the purpose of peace and tranquility in the society. They play an important role in upholding the law and investigating, apprehending and prosecuting breaches of the law [1].The functions of the law enforcement agencies are: provision of assistance to the public when needed; maintenance of law and order; preservation of peace; protection of life and property; investigation of crimes; collection of criminal intelligence; prevention and detection of crimes; provision of specialized stock theft prevention services; apprehension of offenders; enforcement of all laws and regulations with which they are charged and performance of any other duties that may be prescribed [2].In performing their duties, they collect a lot of sensitive and classified data and information from different citizens. These data include crime reports; wanted persons; operation details; forensic evidence; witness identity; etc. These data and information is in turn stored in data centers and accessed from different locations through their network and sometimes through the Internet. Hence there is the need to safeguard these data and information in storage and when being transmitted from one point to another to ensure confidentiality, integrity, availability, identification and authentication, authorization and nonrepudiation. Lawenforcement agencies being the primary security organs experience several information security breaches to their information systems, they are highly prone to attacks, and have been a popular target for hackers resulting in them being hacked several times annually. Other government websites have also been hacked and this raises the question about the safety of data held by the government as the government and its agencies continue to adopt e-government strategies. This has prompted the question of how prepared the law enforcement agencies as one of the government agencies, are in terms of the security of their information systems.

Public and private organizations are facing a wide range of information threats. Information security is a crucial component in their information systems. With their increasing reliance on technologies connected over open data networks, effective management of information security has become one of the most crucial success factors for public and private organizations [3].Law enforcement agencies are high-profile targets of information systems attacks due to the high criticality of the data and information they hold and transmit in their day-to-day operations. This shows the importance of adequate information security preparedness in law enforcement agencies since their information systems are open and prone to information security risks, for example, unauthorized access and changes. Law enforcement agencies rely on network connections to provide the widest possible functionality. Hence, all the information security risks related to networks and to the access to networks, are also applicable to such information systems. If law enforcement agencies' information systems are compromised in any way because of lack of information security, this might have serious impact on the credibility and status of such an agency. Any organization should therefore realize the potential risks which can arise if proper counter measures are not implemented [4]. Therefore, it is important to be able to determine the information security capabilities in law enforcement agencies in order to ensure that their systems are protected against such risks. To do this, some type of information security evaluation framework is needed, such that this framework can be used to summarize all implemented concepts. Extended model for information security, an internationally accepted model for information security in Information and Communication technologies (ICT)systems [5][6] provides information security criteria. These information security services that must be enforced in order to create a secure environment are;

1) Confidentiality to ensure that data stored in databases and transmitted over a network, cannot be read by unauthorized third parties
2) Integrity to ensure that data stored in databases and transmitted over a network cannot be changed by unauthorized third parties
3) Availability to ensure that data is available to authorized parties at all times
4) Identification and authentication to ensure that a user is properly identified and verified during the log-on process
5) Authorization (logical access control) to ensure that the user only has access to that data which is relevant to him or her, and not to other data
6) Nonrepudiation to ensure that a user can be held individually responsible for any action performed on the system

Definition of Terms

1) Information security is the protection of information and its critical elements, including the systems and hardware that use, store, and transmit that information, through the application of policy, training and awareness programs, and technology [7].
2) Information security is the protection of information and information systems against unauthorized access or modification of information, whether in storage, processing or transit and against denial of service to authorized users [8].
3) Preparedness refers to activities and measures designed or undertaken to prepare for or minimize the effects of a natural or man-made hazard upon the information systems, to deal with the immediate emergency conditions that would be created by the hazard, and to effectuate emergency repairs to, or the emergency restoration of, vital aspects destroyed or damaged by the hazard; is a continuous operationally focused process for establishing guidelines, protocols, and standards for planning, training and exercises, personnel qualification and certification, equipment certification, and publication management [9].
4) Law enforcement agencies are institutions that provides justice platform for the citizens of a country for the purpose of peace and tranquility in the society. They play an important role in upholding the law and investigating, apprehending and prosecuting breaches of the law [1].

II. INFORMATION SECURITY PREPAREDNESS

2.1 Information security

Information security is becoming an area of increasing importance especially with the increasing dependency of humans and businesses on computers and computer networks [10]. Recent trends show a sharp increase in computer security breaches and incidences of virus and worm attacks [11].Information security covers many issues such as security policy development and implementation, user education, encryption, system administration, network firewall, intrusion detection, and programming practice etc.[12]. To secure an information infrastructure, which consists of the involved computer systems and network devices, many efforts from different areas should be taken. The information infrastructure is an integrated entity and so it should have security management [10].It is important to evaluate information security preparedness of information systems in order to be able to determine the security measures implemented and their adequacy at a particular time since technology is dynamic and so are the information security threats to such systems. This is also of importance when an organization wants to determine their level of security for their information systems or assets. It is important to evaluate network vulnerability to ensure its robustness and reliability since there is a large scale trend toward increasing reliance on large volumes of data and this increases the overall reliance on the networks that carry this data and translates into an increased vulnerability to network disruptions [13]. Common issues such as training for system administrators, risk assessment, physical security, security policies, and proper system administration are identified as part of important steps to secure a law enforcement network [14]. Better equipment, training, and awareness are part of the basis for law enforcement information security assessment [15].

2.2 Preparedness

Preparedness refers to activities and measures designed or undertaken to prepare for or minimize the effects of a natural or man-made hazard upon the information systems, to deal with the immediate emergency conditions that would be created by the hazard, and to effectuate emergency repairs to, or the emergency restoration of, vital aspects destroyed or damaged by the hazard; is a continuous operationally focused process for establishing guidelines, protocols, and standards for planning, training and exercises, personnel qualification and certification, equipment certification, and publication management [9].For effective Information security preparedness, it is important to safeguard both the physical and digital forms of information from various security threats [16]. Several variables are associated with different levels of IT disaster preparedness. Both operational as well as strategic reliance are significant antecedents of disaster preparedness [17]. Adequate information security measures must be in place to ensure effective information security preparedness. Preparedness activities are necessary to the extent that mitigation measures have not, or cannot, prevent disasters. In the preparedness phase, governments, organizations, and individuals and in this case the law enforcement agencies, develop measures to protect their information systems or assets and minimize damage (for example, implementing firewalls, Intrusion Detection Systems (IDS), training and awareness exercises, or installing antivirus programs, etc.) [9].Preparedness measures also seek to enhance disaster response operations (for example, having Disaster Recovery Plans (DRP) and Business Continuity Plans (BCP) in place, through training or drill or mock-up exercises, and by mobilizing emergency personnel on a standby basis, for example, Computer Emergency Response Team - CERT)."

2.5 National security preparedness

National Security or Emergency Preparedness and the Next-Generation Network requires effective communications supporting leadership and key staff in their access to information and their coordination of decisions [18]. Because of new challenges for emergency preparedness in the information society, it is progressively harder to understand and predict the effects of even simple component failures for the total system functionality since ICT systems are growing increasingly complex and the more complex they become the harder it is to understand them. It is also hard to determine which emergency preparedness measures are the most efficient for complex systems such as the law enforcement agencies Information systems, and hence vulnerabilities in critical infrastructures and societal services will emerge because of this [19]. Cyber-attacks results in millions of dollars in economic impact and hence the need to have adequate and effective information security measures to safeguard against such attacks [20].A number of currently available technologies can be

combined to provide a secure network [21]. In recent years, critical infrastructure protection such as law enforcement agencies information systems has emerged as an increasingly important framework for understanding and mitigating threats to security [22]. This is of importance because such critical infrastructures deal with classified and sensitive information such as on-line access to records concerning wanted persons, stolen vehicles, criminal histories, and other data of importance to law enforcement and criminal justice agencies [14].

III. INFORMATION SECURITY PREPAREDNESS MECHANISMS

3.1 Introduction

Information and or network security control is an issue that increases in difficulty with growths in data and or network size and in number of vulnerabilities; hence, automated approaches can be used to quickly and reliably evaluate the current security state of information and or network. Different information security evaluation frameworks, approaches, models and methods exist which vary depending on the area of application or the organization they are developed for. This paper reviews ten of these mechanisms;

3.1.1 Generic framework [10]

This framework deals with security issues based on a multi agent architecture where each specialist task for security requirement is modeled as a specialist agent task and to address the global security tasks an environment is invoked in which the multiple agents execute their specialist skills and communicate to produce the desired behavior where many agents with different skills are clustered into groups to perform the tasks such as System Administrator Assistant, Integrated Intrusion Detection, Bio-authentication, and Computer Forensics. These tasks together form this proposed IT Security Framework [10].

3.1.2 Applications [23]

These applications are used for assessing network or information security. Green (2003) developed two independent applications for assessing network or information security. The first one was a full featured port scanner named "Super Scanner" that was used to identify vulnerable ports and servers and the second one was a smaller program called "Breaker" that was able to initiate a variety of tests on a server and offered an interface to add modules to accommodate the testing of future vulnerabilities [23].

3.1.3 Attack graphs [24]

Attack graphs are a common approach to security evaluation since they show how an attacker can combine multiple vulnerabilities in a system to launch multi-stage attacks to gain privileges in the system where a tool automatically computes all possible ways a system can be broken into by analyzing the configuration of each host, the network, and the discovered vulnerabilities. Attack graphs are often used in conjunction with risk assessment tools to provide recommendations to system administrators on how to mitigate the discovered problems [24].

3.1.4 Method and systems [25]

Use of methods and systems to evaluate network security is also possible for example [25] demonstrates an invention that tracks failures in the implementation of network security where a method and system for evaluating network security allows for the detection of lack of protection and thus aids in auditing such networks against intrusion from one of the stations in the network. This is done by automatically identifying from an ordinary station connected to TCP/IP network, the network components managed by a network management station for which it is possible to read or write over the confidential network data they store. Starting from the list of the default passwords protecting the network and the IP address of the network components communicating with the ordinary station, the method allows by repeating the IP address discovery process to discover step by step the passwords used in all the network components managed by the network management station and try to use them in reading or writing network information [25].

3.1.5 Mathematical model [4]

Models can also be used evaluate information security for example [4] introduces a mathematical model based on a catalogue of criteria as a framework for evaluating the Information Security where this measure only considers the security concept and not the actual implementation quality [4]. The table below summarizes the catalogue of criteria of this mathematical model;

Table 1: Summary of the catalogue of criteria of the mathematical model

COMPONENTS OF THE CATALOGUE OF CRITERIA OF THE MATHEMATICAL MODEL [4]			
1. Confidentiality (c1)	2. Integrity	3. Availability (a1)	4. Identification and authentication
a) Secure handling of temporary files/directories b) Encryption (symmetric/asymmetric) c) Security policy models (e.g., Bell-LaPadula)	a) Identification and authentication methods; b) Message Authentication Code c) Digitally signed content d) Digitally signed teacher message e) Digitally signed learner message f) Distributed architecture	a) Distributed architecture b) Automatic fallback system c) Take backups regularly	a) Password-based authentication b) Every user has his/her own account (no group accounts) c) Identification of physical users over user-ID is possible d) Control new passwords against some dictionaries and/or perform simplicity analysis e) Encrypted password transmission and storage f) Access control for password file g) Expiration of password validity – frequent password changing h) Token based authentication (e.g., smartcard, USB-stick) i) Biometrical system (e.g., fingerprint scanner) j) Life detection (e.g., pulse control, blood flow) k) Skin resistance

	with write protection g) Security policy models (e.g., Biba or Clark-Wilson)		l) Sweat pores taken into consideration (high resolution) m) Multiple logins with same account prohibited n) Replay-attacks prohibited o) Message about last log-in (time; possibly: duration and/or client name, IP-address) p) Secure temporary file handling, secure cookie handling

Table 1 above is summary of the components of the catalogue of criteria of the mathematical model which are four namely; confidentiality, integrity, availability and identification and authentication.

3.1.6 Logic based framework based on dependency graphs and times games [26]

Bursztein and Jean (2007) presents a Logic-based framework for evaluating the resilience of computer networks based on dependency graphs and anticipate or timed games Logic-based where the Upper Layer consists of the Anticipation Games which models the evolution over time of dependency graphs, through a set of timed rules. Timed automaton games are also interesting because they include a so-called element of surprise: the administrator. The Lower Layer consists of the Dependency Graphs which models the dependencies, vulnerabilities and availability [26].

3.1.7 Conceptual framework [3]

Another approach or method is by use of a conceptual framework which theorizes a strong relationship between the effectiveness of an organizations security management in terms of the basic security criteria (availability, integrity, confidentiality and accountability) and the conceptual framework components which are security culture, managerial and information security infrastructure [3].

3.1.8 Octave approach [27]

The Octave approach which is a risk-driven and practice-based information security evaluation approach has the three key aspects of; Operationally Critical Threat, Asset and Vulnerability Evaluation. The OCTAVE Method was developed with large organizations in mind (300 employees or more). Large organizations generally have a multi-layered hierarchy and are likely to maintain their own computing infrastructure, along with the internal ability to run vulnerability evaluation tools and interpret results in relation to critical assets. The OCTAVE Method uses a three-phased approach to examine organizational and technology issues, assembling a comprehensive picture of the organization's information security needs [27].

3.1.9 Critical success factors (CSF) [28]

The Critical Success Factors approach is derived from several definitions of information security and a combination of these different definitions concludes that information security is about technology, processes and people. "Information security is a well-informed sense of assurance that information risks and technical, formal and informal controls are in dynamic balance" [28]. This approach is based on technical, formal and informal security controls (which are synonyms of technology, processes and people) since the absence of any of the three can compromise information security.

3.1.10 Sociotechnical approach [29]

The social-technical approach which is built on the assumption that information system development involves the design of a work organization where its information system has to be compatible with the surrounding social system, that is, the user and the organizational environments [30]. This means that a socio-technical model should combine the features of the information system, the user and the organizational environments [3].

3.2 A summary of the evaluation frameworks, approaches, methods and models

Table 2: Summary of the evaluation frameworks, approaches, methods and models

Type	Source	Year	Components
1. Generic framework	[10]	2005	Multi-agent architecture; • System Administrator Assistant • Integrated Intrusion Detection • Bio-authentication • Computer Forensics **Weakness: Fails to include user and organizational security mechanisms**
2. Application	[23]	2003	• Port scanner (Super scanner – (Vulnerable ports and servers) • Breaker (Performs a variety of tests on server and future vulnerabilities) **Weakness: Concentrates on scanning only and fails to include user and organizational security mechanisms**
3. Attack graphs	[24]	2011	• Host configuration • Network • Discovered vulnerabilities. **Weakness: Concentrates on network security only and fails to include user and organizational aspects of security.**
4. Method and system	[25]	2005	• Network • Confidentiality • Passwords • Read/Write • Auditing **Weakness: Fails to include the nontechnological security mechanisms**
5. Mathematical model	[4]	2006	• Confidentiality • Integrity

			• Availability • Identification and Authentication **Weakness: Fails to include the user and organizational security aspects hence not comprehensive**
6. Logic-based framework based on dependency graphs and timed games	[26]	2007	• Upper Layer – Anticipation Games (Models the evolution over time and the system administrator) • Lower Layer – Dependency Graphs (Models the dependencies, vulnerabilities and availability) **Weakness: Fails to include the user and organizational security aspects**
7. Conceptual Framework	[3]	2008	• Security culture • Management • Information security infrastructure **Weakness: Not comprehensive enough**
8. Octave approach	[27]	2008	• Operationally Critical Threat • Asset • Vulnerability Evaluation (Organizational) **Weakness: is more of organizational security approach**
9. Critical success factors approach (CSF)	[28]	2006	• Technical security controls • Formal security controls • Informal security controls (which are synonyms of technology, processes and people) **Weakness: Concentrates on technical and user security aspects**
10. Social-technical approach	[29]	1996	• Technical systems • Organizational systems (information system, the user and the organizational environments) **Weakness: Concentrates on technical and user security aspects**

Table 2 above shows summary of the type, source, year and the key components of the information security evaluation frameworks, approaches, methods and models discussed above.

IV. CONCLUSION

Technical and organizational systems are equally important and the lack of fit between social and technical systems is the primary cause of information systems problems. Technical solutions are necessary to address vulnerabilities such as viruses, denial of service attacks, etc. but the involvement of humans in information security is of equal importance and many examples of security issues such as phishing and social engineering, where humans are involved, exist and hence the need to consider the human factor when developing a framework for evaluating information security. It is also important to consider social problems when evaluating security technology since it's much harder to build a secure system with people in it than it is to build a secure system with just math in it. There is also need for provision of economic evaluations of security technology investments as a requirement that more and more customers ask vendors to satisfy by considering the typical calculation of a Return-On-Investment (ROI) index based on the evaluation of the Annual Loss Expectancy (ALE), as the one provided usually by vendors of IT security. The security mechanisms reviewed in this paper evaluate the adequateness of the implemented information security measures from various aspects of information security but they are not comprehensive enough; no single approach have factored or catered for all the areas or aspects necessary to ensure adequate information security preparedness. ICT security involves the implementation of safeguards that protect against intrusion, mishaps and mistakes. Organizations dependence on ICT is steadily growing and is present in many different areas such as; public utilities, communications (mobile telephony), financial institutions (ATM's), medical (diagnostic equipment), etc. These security measures have various components and they include and are not limited to; physical security, operational security, information security, disaster recovery, access control, cryptography, auditing and laws and ethics. It is the responsibility of organizational management, technical experts and users through information security policies and other documents and support to emphasize the importance of information security in their organizations. There is need to determine what data is valuable and needs to be protected, who is responsible for protecting it and to what extent, to what extent user may access and use the data, and what the consequences are for noncompliance. ICT security will therefore involve the implementation of security measures that covers and protects the ICT resources of an organization and hence the need for a framework to evaluate the comprehensiveness of the implemented security measures. Law Enforcement Agencies rely on network connections to provide the widest possible functionality, hence, all the information security risks related to networks and to the access to networks, are also applicable to such information systems and the fact that Law Enforcement Agencies are high-profile targets of information systems attacks due to the high criticality of the data and information they hold and transmit in their day-to-day operations. This shows the importance of adequate information security preparedness in Law Enforcement Agencies since their information systems are open and prone to information security risks, for example, unauthorized access and changes.

V. REFERENCES

[1] Colin Armstrong 2003, Developing a framework for evaluating computer forensic tools, Presented at Evaluation in Crime Trends and justice: Trends and Methods Conference in Conjunction with the Australian Bureau of Statistics, Canberra Australia 24-25
[2] The National Police Service Bill 2011, Kenya
[3] Salahuddin Alfawaz, Lauren May and Kavoos Mohanak 2008, E-government Security in Developing Countries: A Managerial Conceptual Framework. In: International Research Society for Public Management Conference, 26-28, Queensland University of Technology, Brisbane
[4] Christian J. Eibl, Basie S.H. von Solms and Sigrid Schubert 2006, A Framework for Evaluating the Information Security of E-Learning Systems, IDEA Publications
[5] Voydock and Kent 1983, Security Mechanisms in High-Level Network Protocols, ACM Computing Surveys, Vol. 15, No. 2, pp. 135-171
[6] ISO, 7498-2: 1989, Information processing systems – Open systems interconnection– Basic reference model – Part 2: Security Architecture, International Organization for Standardization (ISO), Geneva

[7] Whitman, M. E and Mattord, H.J 2004, Management of Information Security, Course Technology, Boston, MA, ISBN 0-619-21515-1
[8] Joint Chiefs of Staff 2006, United States Armed Forces Information Operations, Joint Publication 3-13 (13 February)
[9] Laura L. Wilson 2010, Before the Emergency: A Framework for Evaluating Emergency Preparedness Alternatives at Higher Education Institutions, Lexicon, Department of Homeland Security (DHS), p.19–20, National Government Association (NGA) 1979, CEM Governors' Guide, p. 13
[10] Dharmendra Sharma, Wanli Ma, and Dat Tran 2005, On an IT Security Framework, Springer-Verlag Berlin Heidelberg, R. Khosla et al. (Eds.): , LNAI 3681, pp. 226.232
[11] Kienzle, D.M. and M.C. Elder 2003. Recent Worms: A Survey and Trends in ACM Workshop on Rapid Malcode, WORM'03. 2003. Washington, DC, USA: ACM
[12] Pfleeger, C.P. and S.L. Pfleeger 2003, Security in Computing. Third ed: Prentice Hall
[13] T. H. Shake, B. Hazzard, and D. Marquis 1999, Assessing Network Infrastructure Vulnerabilities to Physical Layer Attacks, Massachusetts Institute of Technology Lexington, Massachusetts, 22nd National Information Systems Security Conference, Crystal City, Virginia, U.S.A, 18–21
[14] David A. Brown 2002, GSEC Practical Assignment Version 1.3, Steps to Secure a Law Enforcement Network, SANS Institute
[15] Lee Reese, Joseph Fitzgerald and Benjamin Thomas 2008, SERRI Project: Law Enforcement Regional Technology Assessment and Gap Analysis, U.S. Department of Homeland Security, U.S. Department of Energy Interagency Agreement 43WT10301
[16] Chief Information Security Officer 2011, Disaster Preparedness for Personal Information Assets, State of Texas Cyber Security Tips Monthly Newsletter, Volume 5, Issue 10
[17] Nelson, K 2006, Examining Factors Associated with IT Disaster Preparedness, System Sciences, 2006. HICSS '06, Proceedings of the 39th Annual Hawaii International Conference on 04-07, Volume 8, Pg 205b – 205b, ISSN: 1530-1605, ISBN: 0-7695-2507-5
[18] Patrick McGregor, Richard Kaczmarek, Vernon Mosley, Dennis Dease and Peter Adams 2006, National Security or Emergency Preparedness and the Next-Generation Network, IEEE Communications Magazine, Pg 133 - 143
[19] Janne Hagen, Havard Fridheim and Kjell Olav Nystuen 2005, New challenges for emergency preparedness in the information society, ISSN 0085-7130, ASA 2005, Telektronikk 1
[20] Keith Bea 2005, The National Preparedness System: Issues in the 109th Congress, CRS Report for Congress, Order Code RL32803, Congressional Research Service, The Library of Congress
[21] S Forrester, M Palmer, D McGlaughlin and M Robinson 1998, Security in Data Networks, BT Technol J Vol 16 No 1, Pg 52 - 75
[22] Stephen J. Collier and Andrew Lakoff 2008, The Vulnerability of Vital Systems: How "Critical Infrastructure" Became a Security Problem, Myriam Dunn and Kristian Soby Kristensen (eds.), The Politics of Securing the Homeland: Critical Infrastructure, Risk and Securitisation Routledge
[23] Joshua B. Green 2003, Assessing network security, State University of New York College at Oneonta, Consortium for Computing in Small Colleges, JCSC 18, 5, Pg 269 -270
[24] Su Zhang, Xinming Ou, and John Homer 2011, Effective Network Vulnerability Assessment through Model Abstraction, Proceedings of the 8th International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, Springer-VerlagBerlin, Heidelberg
[25] Caillau et al. 2005, Method and System for Evaluating Network Security, United States Patent, US 6,895,436 B1
[26] Elie Bursztein and Jean Goubault-Larrecq 2007, A Logical Framework for Evaluating Network Resilience against Faults and Attacks, Springer-Verlag Berlin Heidelberg, Cervesato (Ed.): ASIAN, LNCS 4846, pp. 212–227
[27] Carnegie Mellon 2008, Information Security Risks Evaluation, The OCTAVE Approach. OCTAVE 2003, Alberts C., Dorofee A. Managing Information Security Risks, "The OCTAVE Approach" Addison-Wesley Publishing — ISBN: 0321118863
[28] Jose M Torres, Jose M Sarriegi, Javier Santos, and Nicolás Serrano 2006, Managing Information Systems Security: Critical Success Factors and Indicators to Measure effectiveness, Springer-Verlag Berlin Heidelberg, Managing Information Systems Security
[29] Livari, J. and Hirschheim, R 1996, Analyzing Information Systems Development: A Comparison and Analysis of Eight IS Development. Information Systems Journal, 21 (7), 551-575
[30] Lyytinen, K 1987, Different Perspectives on Information Systems: Problems and Solutions. ACM Computing Surveys, 19 (1)