International Journal of Advanced Computer Technology (IJACT)
ISSN:2319-7900

Information Security and Survivability of Critical Computer Systems as a Component Of National Security

Mazin Al Hadidi

***Abstract*—The results of researches, allowing to raise the level of cyber protection and survivability of critical computer systems (CCS) is presented in the article. The system approach to solving problems of cyber security, proposed in this work provides for the integration of mathematical models for the survivability and protection of information. An urgency of solving a problem of survivability of the complex computer systems was proved. In the article the basic steps of creating a model of survival critical computer systems have been considered.**

***Index Terms*—information security, national security, cyber threats, critical computer systems, probability of failure element.**

I. INTRODUCTION

Active expansion of information-communication environment of critical computer systems (energy, industry, communication, transport, ets.) (CCS), especially in the segment of mobile, distributed and wireless technologies, accompanied by the emergence of new threats to cyber security (CS), as evidenced by the growing number of incidents related to information security and protection of information and discovered vulnerabilities in CCS and automated control systems (ACS). The threats are real, since criminals can get the opportunity to intercept passwords individual files, geolocation information, broadcast audio and video data, control the Wi-Fi-networks, webcams, information boards on roads and railway tracks, railway stations, airports and others.

Considering the abovementioned, is to stay on the premises of CCS protection as an integral part of national security.

First, the importance of the CCS in the national security and economy of individual countries.

Secondly, a significant vulnerability and CS of CCS, due to the emergence of new methods of attacks on information, including Cyber-attacks (CA), widespread wireless communications, navigation systems using GPS, GALILEO, video surveillance systems, communication technologies GSM, VSAT, supervisory control systems (SCADA, HMI), PLC in various modes and others.

The research purpose is the analysis of a state of cyber security and survivability of CCS, in the conditions of destabilizing effects on the safety, availability and integrity of information-communication environment of critical computer systems.

II. LIST OF THE USED SYMBOLS

$AS_n(T)$ the accuracy of the sequential occurrence of n-inputs events of the operator (from left to right)

B_{p_a} numbers of information threats

D_{isys} set of numbers of protection measures

$F_i(t)$ the distribution function

$f_i(t)$ the probability density function

$\{f_{ij}(\tau\tau)\}$ the matrix of probabilities density of process in every i state

$G_i^{p_a}$ the set of numbers of nodes of i level of state graph, which describes intruder activity to achieve p_a

$g_j^{p_a}$ the probability of overcoming of j protection boundary at intruder attempt to achieve p_a

I^{p_a} the number of levels in range state graph, which describes intruder activity to achieve p_a aim

K_{q_J} matching factor of system transition in *j* state

$K_{\omega_{p_a}}$ the level of intruder skills to achieve p_a aim

$k(s_a, j)$ the transition ordinal number at transition on PMN from transition with number s_a to transition with number *j*

MI the number of intruder's possible targets in the protected CCS

N_A set of numbers of information threats

$N_j^{p_a}$ set of numbers of protection measures

p_a aim of CA

$r_{jm}^{p_a}$ the probability of successful functioning of m protection measure to counteract intruder activity of j at attempt to achieve p_a

S_j the state of CCS

t time

$o_{spm(s_a)}$ the position number on Petri-Markov net (PMN)

$\{o_{ij}\}$ the matrix of transitions probabilities between CCS states

$\rho_{lk}^{p_a}$ the probability of transition from l state to k state of graph at intruder realization attempt of p_a aim

$\Phi_{i+n_{h(tr_{ij})}}(h(tr_{ij}),\tau)$ the transitive probabilities which are determined on the basis of solution of equations system

III. PEVIEW OF THE LITERATURE

The object of the attack to information maybe any of the elements CCS. However, in general all the elements CCS can be assigned to one of the following categories: data processing centers (DPC), ACS, information systems (IS), SCADA, human machine interface (HMI); peripherals and PLC; systems and channels for communication [1–4].

The research of cyber security and survivability of critical computer systems are dedicated such works [5–8]. In intruders have several entry points to compromise IS or ACS. CCS may be contaminated in various ways, such as virus (exploit) can be implemented via USB-connection or through a network interface. Typically, the amount of detected vulnerabilities correlated with the number of published exploits, such as in March 2011 to September 2016 was published 170 exploits [9–11], i.e., it is eight times more than in the period from 2006 to 2012. Vulnerability of CCS, ASC, SCADA, HMI, PLC is due to lack of security mechanisms in industrial protocols and systems of a project, vulnerability of software (SW) and its incorrect configuration. The need for integration with external networks (corporate, WAN, Internet), Wi-Fi and public information technology - operating systems, network protocols and services Remote access - do not contribute to the safety of ASC [1, 7, 12, 13].

IV. INFORMATION SECURITY OF CRITICAL COMPUTER SYSTEMS AS A COMPONENT OF NATIONAL SECURITY

The structure of the technological complex CCS may include various technical systems and tools: systems and tools coordinating time, meteorological, and so on., types of support; systems, equipment, lines and networks and data; systems and remote monitoring equipment; systems and means of collection, storage and processing; computerized systems and controls; system and display facilities and informations boards; other technical software and hardware.

Most of the systems and tools are used to form a feedback channel with an operator, and the controlled technical components of CCS [2, 4, 7, 14, 15, 16].

After identifying the industrial and transport SCADA and CCS such complex viruses as Stuxnet and Duqu (2010-2011), Flame (2012), Careto (2014), Duqu 2, CozeDuqu, Poseidon (2015) there was a sharp jump of interest in information security critical ACS and IS.

Information security of CCS has never been released as a separate type of national security. Moreover, the information security of CCS cannot exist outside of national security. As part of a whole, it carries heredity conceptual approaches to ensure security at the micro and macro levels, continuity of relationships, common principles and methods. Moreover, CS of CCS usually has its own characteristics and specific, reflecting the industry direction and defining its place, role and importance in the structure of national security [2, 4, 5, 7, 8, 14, 15, 16].

It is equally important the classification of CS, which allows selection of specific policies and strategies for its support. As a result, the structure we will have CS of CCS, which is presented in Fig. 1.

The practice shows that these subsystems of CCS are closely linked and are in dialectical interaction. In addition, we should clearly distinguish "a system of information security" from "survivability of CCS" as a real system structures, powers or funds that are directly involved in activities to ensure cyber safety [2, 6, 8 etc.].

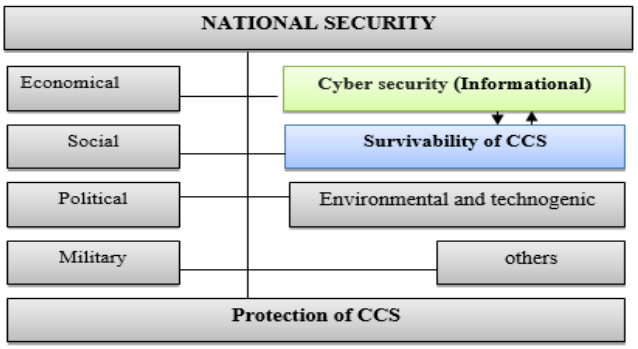

Figure 1. Place of cyber security and survivability in the general system of national security

Incomplete information about threats to information security of IS and ASC is twofold. Firstly, it is partial lack of prior information, even at the level of the structure of the object to attack information, which has, as a rule, stochastic nature. Secondly, the limited ability of observation of the object of recognition and attack threats, which belong to a particular class. In the extreme case it is previously known only to the total set of IS threats and ways to implement them, see. Fig. 2.

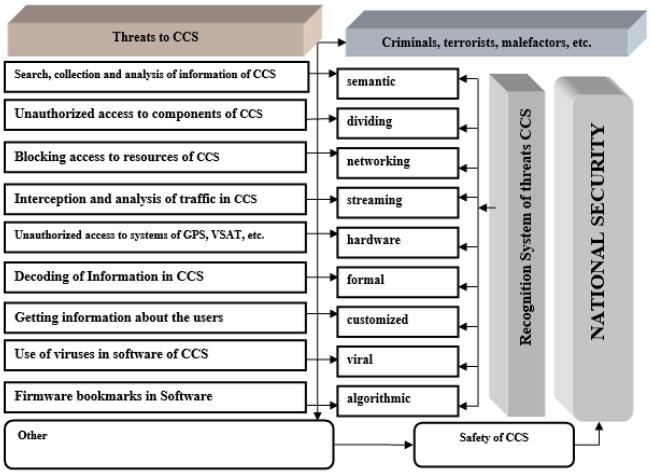

Figure 2. Threats to CCS (Source: [2, 4, 5, 7, 8, 14, 15, 16])

ISSN:2319-7900

However, in practice, one of the main characteristics of today's threats is that they are not activated for a long time, sometimes for two or three years [10, 11]. The targeted attacks, are particularly aimed at CS of enterprises, infrastructure, energy, transport, etc., is usually tailored to the environment in which they will be targeted.

Modern threats are created in a way, as to circumvent the protection, and usually are not detected by signature. Development of scenarios of cyber-attacks performed in compliance with all standards and technologies, the terms of reference, work design, testing, support and upgrade.

Interference in national, regional and municipal automated information and information management systems is frequently mentioned is threats of cyber-attacks for hackers [9–12]. The statistics of incidents of information security is updated every year, see Fig. 3.

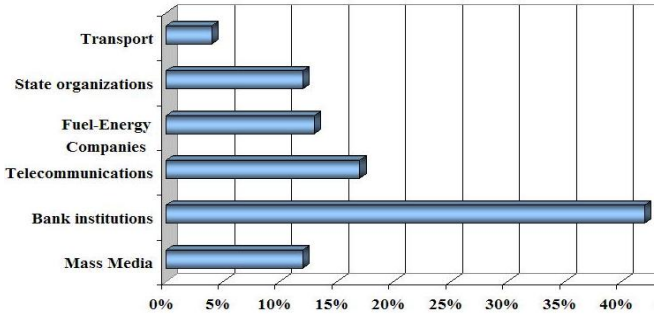

Figure 3. The overall distribution of cyber-attacks in the world for 2012-2016 (Source: [2, 4, 5, 7, 9, 10, 11, 12])

However, the task of determining the risks of attacks on information resources of CCS, in particular, to be adequately addressed and, at the best, raised on the stage [5, 7, 8, 10] of designing of information security systems, qualitative analysis of system reliability and the possible consequences of penetration to it [12].

The interest for intruders can represent such components of the automated control systems (ASC), as SCADA systems and HMI, which in the period from 2004 to 2013 it was revealed more than 120 vulnerabilities, Fig.4 [10–12].

In addition, the study showed [8, 9, 11], requirements to the level of difficulty for a successful attack against industrial and transportation systems, and communication systems (after the attacker gained access to the target of a cyber-attack), the share of low complexity vulnerabilities decreased from a peak of more than 90 % in 2004 to 48 % in 2012, Fig.5.

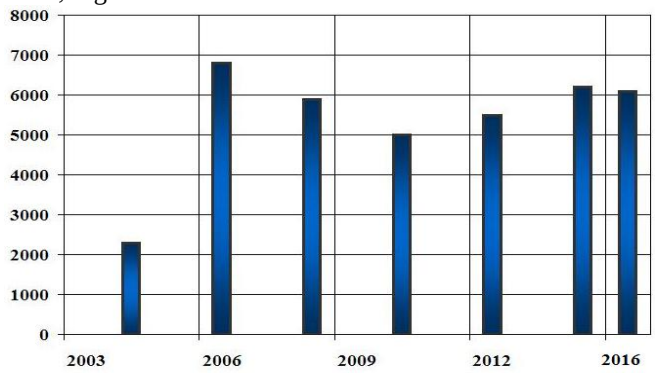

Figure 4. Dynamics of growth of vulnerabilities in ASC communications and transport (Source: (Source: [2, 4, 5, 7, 9, 10, 11, 12])

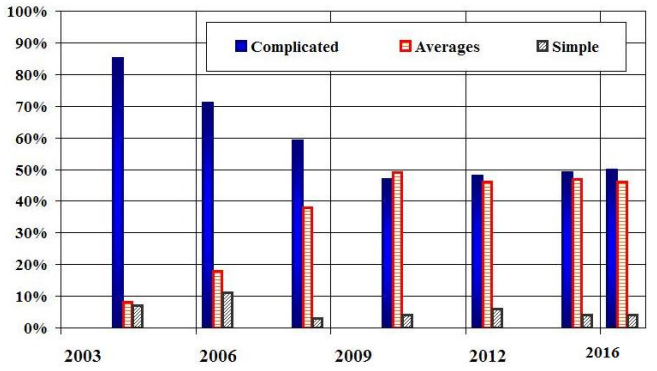

Figure 5. The necessary complexity of attacks (Source: [2, 4, 5, 7, 9, 10, 11, 12])

Meanwhile, during the same period, the average complexity vulnerabilities increased their share from 5% to 47 %. Disclosure with vulnerable complex remained stable in recent decades, their share in an average of only 4 % [10–12].

And of course, not to be taken seriously and DDoS/DoS attack on ASC, which decreases the level of cyber security. A real example of malicious use of cyber-attacks – DDoS/DoS in the transport of SCADA systems recorded in 2012, when the attackers blocked within the hour operation of the metro in Changan (PRC) [10, 12].

The failure of CCS can lead to serious disruptions and significant damage, but the developers of such systems are still not paying enough attention to the security of their products, which is demonstrated in the annual competition Choo Choo Pwn (South Korea). For example, in 2013 and 2014, the participants had to find and take advantage of the vulnerable in the ASC and gain access to the control system model railway, as well as the workability of the automatic railway crossing. ASC model railway was built on the company's products and Siemens controllers S7–1200. During the competition, they managed to send the system false signals and spoofing ASC fails (DoS) [9, 10, 12].

The vulnerability of automated control systems, SCADA, HMI, PLC due to the lack of security mechanisms in communication protocols and systems according to the project, SW vulnerability and its incorrect configuration. The need to integrate with external networks (corporate, WAN, Internet), using wireless networks and open information technologies – operating systems, network protocols and services remote access – also do not contribute to the security of the ASC.

To build an effective information security system (ISS), the selection and implementation of adequate technical equipment must precede the description, analysis and modelling of threats and vulnerabilities of an information system and conducted on the basis of their calculation and risk analysis information security. Therefore, it is evident that initially each threat should be recognized and identified.

Note that used in modern systems to detect and counter cyber-attacks, the techniques are quite effective if you know

ISSN:2319-7900

the exact characteristics of an attack on information or threats.

V. MATH PROBABILITY OF THREATS REALIZATION FOR CCS

Let's designate the total number of threats by *MI* and the number of intruder's possible targets in the protected CCS by *PA*.

Accepted $p_a = 1,2,...,PA;\ j = 1,2,...,MI$. And, $B_{p_a} \subset N_A$, $\bigcup_{p_a=1}^{PA} B_{p_a} = N_A$, $n_{p_a} = |B_{p_a}|$ and $\bigcup_{p_a=1}^{PA} \bigcup_{j \in B_{p_a},}^{n_{p_a}} N_j^{p_a} \subset D_{isys}$.

In this case the process of realization of intruder aims is shown in directed graph in fig 6.

The node of graph represents CCS states which corresponds to attempts of intruder realization of some information threats. S_0 is the initial system state at which any information threat is not realized.

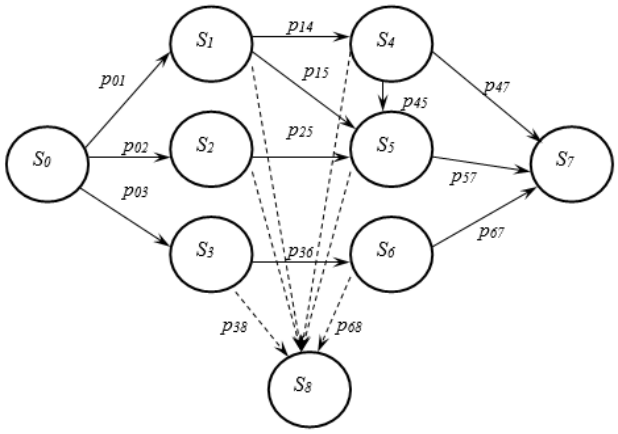

Figure 6. An example of CCS state graph

The state of S_j ($j \in B_{p_a}$) corresponds to realization attempt of *j* threat. In case of it's successful realization, there is a transition to the next system state, otherwise (at regular reaction of IPS) there is a transition to the state of $S_{n_{pa}+1}$ (fig. 6 $S_{n_{pa}+1} \equiv S_8$). The state of $S_{n_{pa}}$ is final and corresponds to intruder achievement p_a aim ($p_a = 1,2,...,PA$). The directed links of graph shows directions of transitions between states. Each link is characterized by value of probable transition between system states. Links corresponding to transition from $S_{n_{pa}}$ to $S_{n_{pa}+1}$ state are designated dotted line.

The probability of system in *k* state, at intruder attempt to achieve p_a aim, is defined by following expression

$$P_k^{p_a} = \sum_{l \in G_{i-1}^{p_a}} P_l^{p_a} p_{lk}^{p_a},\quad k \in G_i^{p_a},\ i = 0,1,2,...,I^{p_a}, \qquad (1)$$

$p_a = 1,2,...,PA$

and

$$\bigcup_{i=0}^{I^{p_a}} G_i^{p_a} \subset B_{p_a};\ p_{lk}^{p_a} = \rho_{lk}^{p_a} g_l^{p_a}; \qquad (2)$$

The probability of overcoming of j protection boundary at intruder attempt to achieve p_a aim

$$g_j^{p_a} = \left(1 - e^{-Kq_j K\omega_{p_a}}\right) \prod_{m \in N_j^{p_a}} \left(1 - r_{jm}^{p_a} x_{jm}\right) \qquad (3)$$

Accepted $K_{\omega_{p_a}} \in [0,1]$, $(p_a = 1,2,...,PA)$, $x_{jm} = \{0,1\}$, $x_{jm}=1$, if m measure is used on *j* protection boundary, $x_{jm}=0$, otherwise, ($j \in B_{p_a}, j \neq 0, j \neq MI+1$; $m \in N_j^{p_a}$).

The probability of transition of process from initial state $S_{i(a)}$ to final $S_{j(z)}$ on trajectory $h(tr_{ij})$ is defined on the basis of solution of integro-differential equations:

$$\Phi_{ij}(h(tr_{ij}), \tau) = \\ = o_{ij} \cdot \int_0^{\tau} f_{ik}(h(tr_{ij}), \tau) \cdot \Phi_{kj}(h(tr_{ij}) - \tau) \cdot d\tau \qquad (4)$$

As the trajectory is chosen (graph links are known) alternative variants of transitions on links, which are incidental to $S_{i(a)}$ position, are not considered.

However, if on $h(tr_{ij})$ trajectory there is a transition with a logic condition and there are some trajectories it is necessary to calculate probability of this logic transition.

The general number of this transition (on Petri-Markov net (PMN) [17–21]) numbering or Markov chain) is ϑ, and current number of this transition according to $h(tr_{ij})$ trajectory numbering corresponds to $n_{h(rt_{ij})}$ and this specified probability is:

$$\Phi_{\vartheta}(\tau) = \begin{cases} \prod_{h(tr) \in H} \Phi_{i+n_{h(tr_{ij})}}(h(tr_{ij}), \tau); \text{ for } \wedge; \\ 1 - \prod_{h(tr) \in H} \left[1 - \Phi_{i+n_{h(tr_{ij})}}(h(tr_{ij}), \tau)\right]; \text{ for } \vee \end{cases} \qquad (5)$$

If there is no any logic transitions on $h(tr_{ij})$ trajectory, there is probability that process will reach final transition by calculated time, and will get to last graph node. This probability defined as follows:

ISSN:2319-7900

$$\Phi_{i,j(t)} = \prod_{k=1}^{j} o_{spm(S_a)}, k(s_a, j) \cdot \int_0^t \Phi_{s_a}(\tau) \cdot \cdot f_{spm(S_a),j} \cdot (t-\tau) d\tau \quad (6)$$

Probability of $\Phi_{i,j(t)}$ is probability of threat realization. If there are transitions with logic conditions on this trajectory the procedure repeats for them.

Then we create a dynamic fault trees through the introduction of dynamic vertex (which we use as operators), we define a set of dynamic and static nodes that allow you to build an adequate model of survivable information network of critical computer systems (SIN CCS). The procedure of use of n–inputs dynamic statement, the occurrence of input events in the interval $(0,T)$ the recurrence of the integral equation, which takes into account the sequence:

$$AS_n(t) = \int_0^T f_n(\tau) \cdot AS_{n-1}(\tau) d\tau,$$
$$AS_2(t) = \int_0^T f_1(\tau)(1-F_2(\tau)) \cdot AS_2(T-\tau) d\tau \quad (7)$$

The use of this integrated model (7), instead of the Markov model, allowed us to remove the restriction on the proportionate distribution function.

VI. THE SIMULATION RESULTS

For the three server survivable CCS with frequency and consistent criteria for the recognition of components that fails or refuses, we construct a hierarchy of nested dynamic fault trees, Markov model is implemented survivability triple block servers with the incompleteness of the control and distribution of the failure modes of the dangerous and safe, the correction accuracy implementation of the basic events in the fault tree models that performs a "screening" flow disruptions special software to implement procedures for handling failures [17–19, 21].

The developed model enabled to make a calculation of indicators of survivability CCS and to give recommendations on the choice of parameters of computational procedures for the reduction process, broken by the problems with different ratios of the intensities of failures and permanent failures of network elements. The proposed model realized in MathCAD. A plot of the probability of failure of element SIN CCS on the number of retries in the interval (0,1 hours) to $r = 20\,(1/h)$ and $r = 60\,(1/h)$ at a fixed failure rate equal to $2{,}3 \cdot 10^{-6}$, is shown in fig. 7.

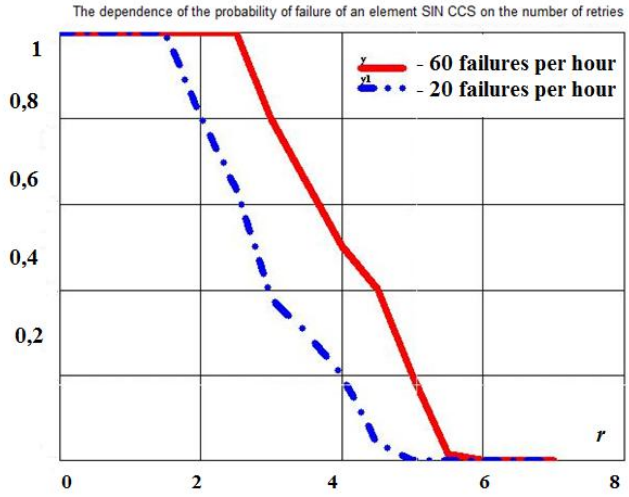

Figure 7. A plot of the probability of failure element SIN CCS on the number of retries

The graph shows that a small number of retries (< 4) failures define low reliability, survival and cyber security of critical computer systems. As the number of retries (> 5) failures do not affect the reliability, survival and cyber security of critical computer systems, which in this case is completely determined by the flow of permanent failures.

VII. CONCLUSION

The main research results are:

1) the general issues of cyber protection and survivability of critical computer systems (CCS) are regarded;

2) the urgency of the problem and its current state is shown;

3) the basic steps of creating a model of survival critical computer systems have been considered.

REFERENCES

[1] A. A. El Hassani, A. A. El Kalam, A. Bouhoula, R. Abassi, A. "Ait Ouahman, Integrity-OrBAC: a new model to preserve Critical Infrastructures integrity," International Journal of Information Security, vol. 14, iss. 4, pp. 367–385, 2014. doi:10.1007/s10207-014-0254-9

[2] N. R. Storey. Safety Critical Computer Systems. Addison-Wesley Longman Publishing Co., Inc. Boston, MA., pp. 22–34, 1996.

[3]. W. Dunn. Practical Design of Safety-critical Systems, Reliability Press, pp. 22–61, 2002.

[4] G. Qu, R. Jayaprakash, S. Hariri, C. Raghavendra, "A framework for network vulnerability analysis," In *CT* '02: Proceedings of the 1st IASTED international conference on communications, Internet, information technology, St. Thomas, Virgin Islands, USA, pp. 289–298, 2002.

[5] P. Attasara-Mason, "Safety critical computer systems: An information management perspective on their development," Management of Innovation and Technology. ICMIT 2008. 4th IEEE International Conference on 21–24 Sept. pp. 1271–1276, 2008. doi: 10.1109/ICMIT.2008.4654553.

[6] S. Selim, M. Hashem, T. M. Nazmy, "Detection using multi-stage neural network", International Journal of Computer Science and Information Security (IJCSIS), vol. 8, no. 4. pp. 14–20, 2010.

[7] M. Theoharidou, M. Kandias, D. Gritzalis, "Securing Transportation-Critical Infrastructures: Trends and Perspectives," Chapter Global

ISSN:2319-7900

Security, Safety and Sustainability & e-Democracy Volume 99 of the series Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, pp. 171–178, 2012. doi: 10.1007/978-3-642-33448-1_24

[8] V.A. Lakhno, O.S. Petrov, A.V. Hrabariev, Y.V. Ivanchenko, Beketova G.S. "Improving of information transport security under the conditions of destructive influence on the information-communication system," Journal of theoretical and applied information technology, vol. 89, no 2, pp. 352–361, 2016.

[9] 2015 Cyber Attacks Statistics. [Online]. Available: http://www.hackmageddon.com /2016/01/11/2015-cyber-attacks-statistics/

[10] MITRE Research Program. [Online]. Available: http://www.mitre.org

[11]. Creating trust in the digital world EY's Global Information Security Survey 2015. [Online]. Available: http://www.ey.com/Publication/vwLUAssets/ey-global-information-security-survey-2015/$FILE/ey-global-information-security-survey-2015.pdf

[12] T. Walk. "Cyber-attack protection for pipeline SCADA systems," Pipelines International digest, p. 4–8, 2012.

[13] M.-H. Maras, "Cybercrime Laws: Which Statute for Which Crimes," Computer Forensics: Cybercriminals, Laws, and Evidence. Sudbury, MA: Jones & Bartlett Learning, pp. 104–106, 2012.

[14] O. Korchenko, E. Vasiliu, S. Gnatyuk, "Modern quantum technologies of information security against cyber- terrorist attacks," Aviation, vol. 3, pp. 58–69, 2010. doi:10.3846/aviation.2010.10.

[15] H. A. Boyes, "Maritime Cyber Security – Securing the Digital Seaways," Engineering & Technology Reference, pp. 8, 2014.

[16] R. Baskervillea, P. Spagnolettib, J. Kim, "Incident-centered information security: Managing a strategic balance between prevention and response," Information & Management, vol. 51, iss. 1, pp. 138–151, 2014. doi:10.1016/j.im.2013.11.004

[17] S. Dilek, H. Cakır, M. Aydın, M. "Applications of artificial intelligence techniques to combating cybercrimes: A review," International Journal of Artificial Intelligence & Applications, vol. 6, 21–39, 2015. doi: 10.5121/ijaia.2015.6102

[18] J. Sterbenz, E. K. Cetinkaya, M. A. Hameed, A. Jabbar, S. Qian, J.P. Rohrer, "Evaluation of network resilience, survivability, and disruption tolerance: analysis, topology generation, simulation, and experimentation," Telecommunication Systems, vol. 52, iss. 2, pp. 705–736, 2013. doi: 10.1007/s11235-011-9573-6

[19] A. Pătraşcu, V.V. Patriciu, "Digital Forensics in Cloud Computing," Advances in Electrical and Computer Engineering, vol. 14, no. 2, pp. 2014. doi: 10.4316/aece.2014.02017

[20] K. Trivedi, D. Kim, A. Roy, D. Medhi, "Dependability and security models," In Proceedings of the international workshop of design of reliable communication networks (DRCN), New York: IEEE Press, pp. 11–20, 2009.

[21] P. Smith, A. Schaeffer-Filho, A. Ali, M. Schöller, N. Kheir, A. Mauthe, D. Hutchison, "Strategies for network resilience: capitalising on policies," Lecture notes in computer science: vol. 6155. Mechanisms for autonomous management of networks and services, Berlin/Heidelberg: Springer, p. 118–122, 2010.