I. J. Computer Network and Information Security, **2017, 6, 30-43**
Published Online June 2017 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2017.06.04

Method for Cyberincidents Network-Centric Monitoring in Critical Information Infrastructure

Zhengbing Hu
Central China Normal University, Wuhan, China
E-mail: hzb@mail.ccnu.edu.cn

Viktor Gnatyuk, Viktoriia Sydorenko, Roman Odarchenko and Sergiy Gnatyuk
National Aviation University, Kyiv, Ukraine
E-mail: viktorgnatyuk@ukr.net, v.sydorenko@ukr.net, odarchenko.r.s@mail.ru, s.gnatyuk@nau.edu.ua

***Abstract*—**In this paper the method of network-centric monitoring of cyberincidents was developed, which is based on network-centric concept and implements in 8 stages. This method allows to determine the most important objects for protection, and predict the category of cyberincidents, which will arise as a result of cyberattack, and their level of criticality.

***Index Terms*—**Cyberincident, ICT, ITS, network-centric concept, monitoring, criticality, KDD 99 base, CERT/CSIRT.

I. Introduction

Given the dynamics of development and globalization of information and communication technologies (ICT) implementation and use of ICT in most areas of public life has become outstanding relevance. This process includes: development of the interactive communication and information exchange (social networks, e-mail sharing, instant messaging, video and Internet telephony); computerization and automation of manufacturing processes and most areas of public life (creation of local (corporate) computer networks, systematization of information in databases, platforms for collaboration users, sharing resources, VoIP and video communication, electronic documents, customer relationship management system (CRM); enterprise resource planning system (ERP), information security management system, monitoring and access control); Internet-banking, e-commerce, instant money transfer and more. All of these procedures, the operation of which is providing by ICT, is quite critical, even for the average citizen, especially in terms of the information that circulates in them. The emergence of cyberincidents (events that can disrupt cyber security (confidentiality, integrity and availability of information in cyberspace) [1]) and, consequently, violations of the regular mode of operation of the entire system can cause considerable damage.

The work includes original research and proposes new method of network-centric monitoring of ITS incidents implemented in 8 phases: classification of cyberattacks, detecting the type of cyberattack, categorization of cyberincidents, forming the set of rules cyberincidents extrapolation, determination the objects of protection, determination the impact of cyberincidents on ITS components, identification of the most critical components of the ITS, ranking the degree of cyberincidents danger. On the input is filed, the set of measurement standards of cyberattacks parameters, set of current parameters that recorded by sensors, statistic of ITS incidents, categories of ITS incidents, ITS components; and on the output we get: the type of cyberattack, forecasted incident as a result of realized cyberattack, the level of incident criticality, impact assessment of incidents categories on ITS components, the most critical ITS components.

II. Analysis of The Research and Problem Statement

Today there are many works devoted to the research of detection of unauthorized activities in ICT, for example, in [3] carried out a comparative analysis of intrusion detection system (IDS) using virtual honeypots (Honeypot) last generation Honeynet GenIII (Autograph, PADS, PAYL, COVERS, DIRA, DOME, Minos, Paid, Vigilante, HoneyStat etc.), which have different mechanisms of intrusion detection and working with different input data. Work [4] contains a detailed analysis of the systems and tools of crisis management in various fields, including a prediction, identification, assessment and crisis response. Although most of the examined systems are based on the use of sensors (sensors) and collected statistics, however such systems can't be used in cyberspace to manage information (cybernetic) security, since they do not operate with real parameters of cyberspace. Considering this, it is not possible the prediction of defeat by cyberincidents also for specific components of Information and Telecommunication Systems (ITS) as components of cyberspace and, consequently, it is not possible to control resistance (countermeasures) and elimination of consequences of various categories of cyberincidents.

III. The Concept of Network-Centric Monitoring of Cyberincidents

Anti-emergence and elimination of cyberincidents consequences through the facilities that are combined by information networks into a single system includes: 1) Constant computer monitoring of potentially dangerous places and objects to determine the necessary measures for eliminating the consequences of each type of possible cyberincidents; 2) Implementation of necessary measures of preparation for the elimination of consequences of possible groups of cyberincidents; 3) Establishment of goals for parallel elimination of possible types of cyberincidents, their synchronization, coordination and ranking; 4) Implementation of parallel strategies purposes, their interaction and synchronization of resources used; 5) The formation of a possible set of parallel operational impacts, their scheduling, synchronization and maneuvering resources management dynamics.

Network-centric monitoring system combines monitoring tools at all levels and areas of governance into a coherent whole. It should provide proof of all necessary information to recipients in real time or close to it, in process of receipt, very importantly, by using the information gained at all levels and areas of control. This approach allows dramatically improve the understanding of the situation by the leaders at all levels, increase the level of interaction and implement the synchronization of efforts by the horizontal and vertical control. It should be noted that the violation of even one of these principles can lead to serious complications. Network-centric concept is focused not only on effective management of available technical, financial and on other means, but also to achieve information superiority in economics, politics, social sphere, etc., providing the system's ability to quickly adapt to transient conditions and to transfer the functions of strategic and operational control vertically and horizontally according to the needs of the existing situation. For this network-centric monitoring should provide real-time complex multilevel analysis of streams separate, uninformative and often contradictory initial information about new facilities or processes and dynamic of parameters changing. The system should be able to change the logic of the analysis of the existing situation as far as changing information sources and new information, which was receive about the situation. Failure of one or more local monitoring subsystems should not lead to the collapse of all network-centric monitoring.

When working response teams with cyberincidents of type CERT / CSIRT [10] according to specified concept we set sequence (Fig. 1): in ITS happens a certain event of information security E_1 ... E_n (according to [2] in meaning of event of information security, we understand identified system behavior , service or network, that points to a possible breach of information security, policy, control facilities failure or previously unknown situation that may be relevant to information security) caused by cyberattacks CA_1 ... CA_n [11] as well as unintentional actions that coming on the sensors S_1 ... S_n (sensors of network-centric monitoring system of cyberincidents can be sources of information such as intrusion detection/prevention systems IDS / IPS [23, 24], integrity monitoring systems, firewalls, honeypot systems, analyze vulnerabilities systems, exploits, operating systems, different applications (including specialized detection systems of cyberincidents with type SIEM), anti-virus and anti-spam systems, user requests in systems such as Service Desk or Help Desk etc.) which identifies and fixes cyberincidents I_1 ... I_n in particular set of parameters, comparing with relevant patterns.

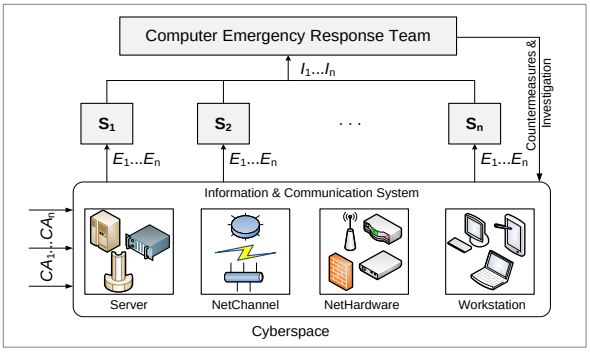

Fig.1. Implementation Scheme of Cyberincidents Network-Centric Monitoring Concept

Network-centric monitoring is determined by that for each management system of cyberincidents forms a network of agents (sensors). The overall management system of cyberincidents region or state can be displayed as a complex network of interconnected centers (teams) campus type, each of which is able to: have a clearly defined goal of the functioning; act in accordance with its rules and algorithms; manage a database containing the requested information; use the results of monitoring, responding to them by their actions; take their own initiative; send and receive messages from other systems and join with them in interaction.

IV. Method for Cyberincidents Network-Centric Monitoring

On the basis of this conception the method for cyberincidents network-centric monitoring in general is based on the following sequence of events (Fig. 2): identified and classified at several levels cyberattacks (based on a comparison of current parameters with the parameters listed in the database templates attacks, such as KDD 99 (2 level classification), CAPEC (4 level classification) etc. [12-14]) may cause for cyberincidents who belong to one of the categories (in various fields these categories may be different, for example CERT-UA [15] defines 7 categories of incidents which indicated in Fig. 2). Cyberincident which may arise because of attack could potentially harm the components of ITS (a set of information and telecommunication systems which are acts in data processing as a coherent whole [16]), for example, according to [15] can be identified 4. Definition of ITS components that require protection (objects of

protection) will minimize the impact of cyberincidents on them. In addition, in the case of simultaneous occurrence of incidents is important to predict the level of danger for more effective treatment and adequate response (investigation) by teams CERT / CSIRT.

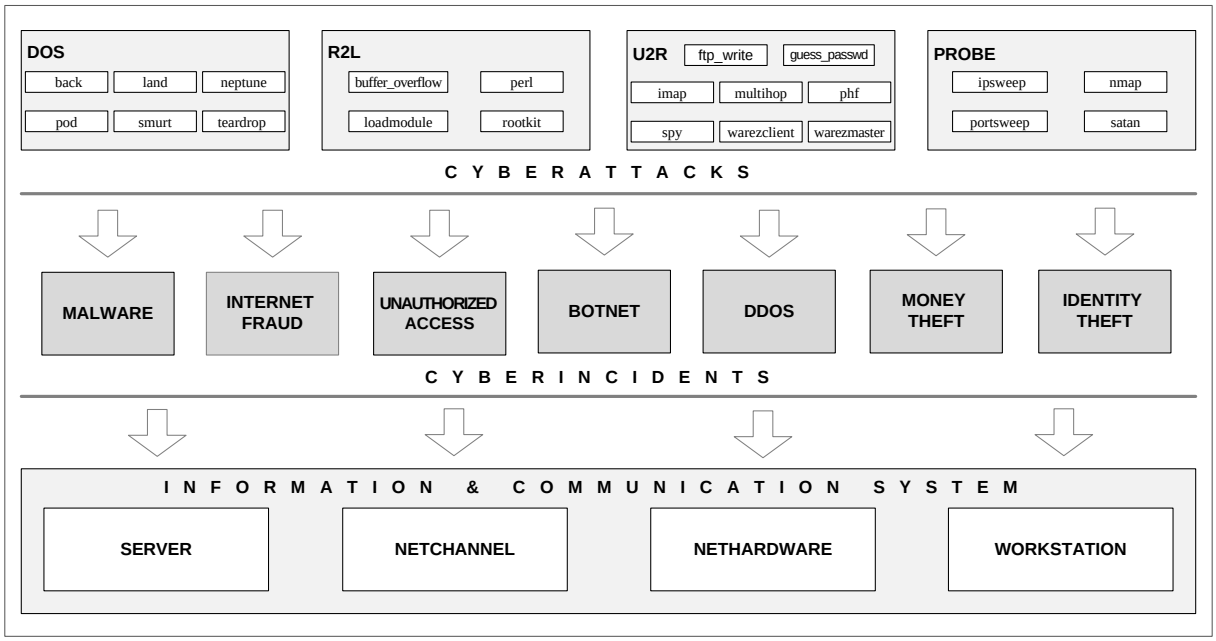

Fig.2. General Scheme of Method for Cyberincidents Network-Centric Monitoring

The proposed method for cyberincidents network-centric monitoring implements in 8 phases: classification of cyberattacks, detecting the type of cyberattack, categorization of cyberincidents, forming the set of rules cyberincidents extrapolation, determination the objects of protection, determination the impact of cyberincidents on ITS components, identification of the most critical components of the ITS, ranking the degree of cyberincidents danger.

Phase 1 – Classification of cyberattacks. For this stage we ask the set of cyberattacks parameters standards CA that may occur in the ITS:

$$\{\bigcup_{i=1}^{n}\mathbf{CA_i}\}=\{\mathbf{CA}_1,\mathbf{CA}_2,...,\mathbf{CA}_n\}, \quad (1)$$

where $\mathbf{CA_i} \subseteq \mathbf{CA}$, $(i=\overline{1,n})$, n – cyberattacks quantity, and

$$\mathbf{CA_i}=\{\bigcup_{j=1}^{m_i}\mathbf{CA_{ij}}\}=\{\mathbf{CA_{i1}},\ \mathbf{CA_{i2}},\ \ldots,\ \mathbf{CA}_{im_i}\}, \quad (2)$$

where $\mathbf{CA_{ij}}$ $(j=\overline{1,m_i})$ – subsets of the subclasses of cyberattacks.

Considering (2) write the expression (1) as follows:

$$\{\bigcup_{i=1}^{n}\mathbf{CA_i}\}=\{\bigcup_{i=1}^{n}\{\bigcup_{j=1}^{m_i}\mathbf{CA_{ij}}\}\}=\{\{\mathbf{CA}_{11},\mathbf{CA}_{12},...,\mathbf{CA}_{1m_1}\},$$
$$\{\mathbf{CA}_{21},\mathbf{CA}_{22},...,\mathbf{CA}_{2m_2}\},...,\{\mathbf{CA}_{n1},\mathbf{CA}_{n2},...,\mathbf{CA}_{nm_n}\}\},(j=\overline{1,m_i}) \quad (3)$$

Subsets of the subclasses of cyberattacks $\mathbf{CA_{ij}} \subseteq \mathbf{CA_i}$ define as:

$$\mathbf{CA_{ij}}=\{\bigcup_{s=1}^{r_{ij}}\mathbf{CA_{ijs}}\}=\{\mathrm{CA}_{\mathrm{ij1}},\ \mathrm{CA}_{\mathrm{ij2}},\ \ldots,\ \mathrm{CA}_{\mathrm{ijr_j}}\}, \quad (4)$$

where $\mathrm{CA}_{\mathrm{ijs}}$ $(s=\overline{1,r_{ij}})$ – parameters that describes cyberattacks $\mathbf{CA_{ij}}$; r_{ij} – parameters quantity.

Then the expression (3) with considering (4) will receive as follows:

$$\{\bigcup_{i=1}^{n} \mathbf{CA_i}\} = \{\bigcup_{i=1}^{n}\{\bigcup_{j=1}^{m_i} \mathbf{CA_{ij}}\}\} = \{\bigcup_{i=1}^{n}\{\bigcup_{j=1}^{m_i}\{\bigcup_{s=1}^{r_{ij}} CA_{ijs}\}\}\} =$$
$$= \{\{\{CA_{111}, CA_{112}, ..., CA_{11r_1}\}, \{CA_{121}, CA_{122}, ..., CA_{12r_2}\}, ..., \{CA_{1m_11}, CA_{1m_12}, ..., CA_{1m_1r_{m1}}\}\},$$
$$\{\{CA_{211}, CA_{212}, ..., CA_{21r_1}\}, \{CA_{221}, CA_{222}, ..., CA_{22r_2}\}, ..., \{CA_{2m_21}, CA_{2m_22}, ..., CA_{2m_2r_{m2}}\}\}, \quad (5)$$
$$...,$$
$$\{\{CA_{n11}, CA_{n12}, ..., CA_{n1r_1}\}, \{CA_{n21}, CA_{n22}, ..., CA_{n2r_2}\}, ..., \{CA_{nm_n1}, CA_{nm_n2}, ..., CA_{nm_nr_{mn}}\}\}\}.$$

For example, using that contains 5 million of cyberattacks parameter sets and normal behavior (from KDD 99 base), if $n = 4$, according to the expression (1) we will get the following:

$$\{\bigcup_{i=1}^{4} \mathbf{CA_i}\} = \{\mathbf{CA_1}, \mathbf{CA_2}, \mathbf{CA_3}, \mathbf{CA_4}\} =$$
$$= \{\mathbf{CA_{DOS}}, \mathbf{CA_{R2L}}, \mathbf{CA_{U2R}}, \mathbf{CA_{PROBE}}\} = \quad (6)$$
$$= \mathbf{\{DOS, R2L, U2R, PROBE\}.}$$

where $\mathbf{CA_1} = \mathbf{CA_{DOS}} = \mathbf{DOS}$, $\mathbf{CA_2} = \mathbf{CA_{R2L}} = \mathbf{R2L}$, $\mathbf{CA_3} = \mathbf{CA_{U2R}} = \mathbf{U2R}$, $\mathbf{CA_4} = \mathbf{CA_{PROBE}} = \mathbf{PROBE}$ – cyberattacks classes from KDD 99 base. Consider the cyberattacks classes in details (Table. 1):

Table 1. Cyberattacks from KDD 99

Class	Subclass
1. DOS	1.1. BACK, 1.2. LAND, 1.3. NEPTUNE, 1.4. POD, 1.5. SMURT, 1.6. TEARDROP
2. R2L	2.1. BUFFER_OVERFLOW, 2.2. PERL, 2.3. LOADMODULE, 2.4. ROOTKIT
3. U2R	3.1. FTP_WRITE, 3.2. GUESS_PASSWD, 3.3. IMAP, 3.4. MULTIHOP, 3.5. PHF, 3.6. SPY, 3.7. WAREZCLIENT, 3.8. WAREZMASTER
4. PROBE	4.1. IPSWEEP, 4.2. NMAP, 4.3. PORTSWEEP, 4.4. SATAN

Under the specified classes in the Table 1 according to [15] will understand the following:

1. *Denial of Service* (**DOS**) – cyberattacks the denial of service, which are characterized by generating a large volume of traffic, that leading to congestion and blocking server (including 6 subclasses of cyberattacks);
2. *Remote to User* (**R2L**) – cyberattacks, which are characterized by obtaining illegitimate (unregistered) user unauthorized remote access to the management information (including 4 subclasses of cyberattacks);
3. *User to Root* (**U2R**) – cyberattacks that provides unauthorized empowerment of illegitimate (unregistered) users to the level of local superuser (administrator) (including 8 subclasses of cyberattacks);
4. *Probing* (**PROBE**) – scanning ports cyberattacks to obtain confidential information (including 4 subclasses of cyberattacks).

Using the expression (2), and data from the Table 1, for example if $m_1 = 6,\ m_2 = 4,\ m_3 = 8,\ m_4 = 4$, we get:

$$\mathbf{CA_1} = \{\bigcup_{j=1}^{6} \mathbf{CA_{ij}}\} = \{\mathbf{CA_{1,1}}, \mathbf{CA_{1,2}}, \ldots, \mathbf{CA_{1,6}}\} =,$$
$$= \{\mathbf{CA_{DOS,1}}, \mathbf{CA_{DOS,2}}, ..., \mathbf{CA_{DOS,6}}\} =$$
$$= \{\mathbf{DOS}_{BACK}, \mathbf{DOS}_{LAND}, \mathbf{DOS_{NEPTUNE}},$$
$$\mathbf{DOS_{POD}}, \mathbf{DOS_{SMURT}}, \mathbf{DOS}_{TEARDROP}\} = \quad (7)$$
$$\mathbf{= \{BACK, LAND, NEPTUNE,}$$
$$\mathbf{POD, SMURT, TEARDROP\},}$$

where $\mathbf{CA_{1,1}} = \mathbf{CA_{DOS,1}} = \mathbf{DOS}_{BACK} = \mathbf{BACK}$, $\mathbf{CA_{1,2}} = \mathbf{CA_{DOS,2}} = \mathbf{DOS}_{LAND} = \mathbf{LAND}$, $\mathbf{CA_{1,3}} = \mathbf{CA_{DOS,3}} = \mathbf{DOS_{NEPTUNE}} = \mathbf{NEPTUNE}$, $\mathbf{CA_{1,4}} = \mathbf{CA_{DOS,4}} = \mathbf{DOS_{POD}} = \mathbf{POD}$, $\mathbf{CA_{1,5}} = \mathbf{CA_{DOS,5}} = \mathbf{DOS_{SMURT}} = \mathbf{SMURT}$, $\mathbf{CA_{1,6}} = \mathbf{CA_{DOS,6}} = \mathbf{DOS_{TEARDROP}} = \mathbf{TEARDROP}$ – cyberattacks subclasses of class **DOS** according to KDD 99 base (Table 1).

$$\mathbf{CA_2} = \{\bigcup_{j=1}^{4} \mathbf{CA_{ij}}\} = \{\mathbf{CA_{1,1}}, \mathbf{CA_{1,2}}, \mathbf{CA_{1,3}}, \mathbf{CA_{1,4}}\} =$$
$$= \{\mathbf{CA_{R2L,1}}, \mathbf{CA_{R2L,2}}, \mathbf{CA_{R2L,3}}, \mathbf{CA_{R2L,4}}\} =$$
$$= \{\mathbf{R2L}_{\text{BUFFER\_OVERFLOW}}, \mathbf{R2L}_{\text{PERL}},$$
$$\mathbf{R2L}_{\text{LOADMODULE}}, \mathbf{R2L}_{\text{ROOTKIT}}\} =$$
$$\mathbf{= \{BUFFER\_OVERFLOW, PERL,}$$
$$\mathbf{LOADMODULE, ROOTKIT\},} \quad (8)$$

where $\mathbf{CA_{1,1}} = \mathbf{CA_{R2L,1}} = \mathbf{R2L}_{\text{BUFFER\_OVERFLOW}} = \mathbf{BUFFER\_OVERFLOW}$, $\mathbf{CA_{1,2}} = \mathbf{CA_{R2L,2}} = \mathbf{R2L}_{\text{PERL}} = \mathbf{PERL}$, $\mathbf{CA_{1,3}} = \mathbf{CA_{R2L,3}} = \mathbf{LOADMODULE}$, $\mathbf{CA_{1,4}} = \mathbf{CA_{R2L,4}} = \mathbf{R2L}_{\text{ROOTKIT}} = \mathbf{ROOTKIT}$ – cyberattacks subclasses of class R2L according to KDD 99 base (Table 1).

$$\mathbf{CA_3} = \{\bigcup_{j=1}^{8} \mathbf{CA_{ij}}\} = \{\mathbf{CA_{1,1}}, \mathbf{CA_{1,2}}, \ldots, \mathbf{CA_{1,8}}\} =$$
$$= \{\mathbf{CA_{U2R,1}}, \mathbf{CA_{U2R,2}}, ..., \mathbf{CA_{U2R,8}}\} =$$

$$= \{\mathbf{U2R}_{\text{FTP\_WRITE}}, \mathbf{U2R}_{\text{GUESS\_PASSWD}}, \mathbf{U2R}_{\text{IMAP}}, \mathbf{U2R}_{\text{MULTIHOP}}, \mathbf{U2R}_{\text{PHF}}, \mathbf{U2R}_{\text{SPY}}, \mathbf{U2R}_{\text{WAREZCLIENT}}, \mathbf{U2R}_{\text{WAREZMASTER}}\} = \mathbf{= \{FTP\_WRITE, GUESS\_PASSWD, IMAP, MULTIHOP, PHF, SPY, WAREZCLIENT, WAREZMASTER\},} \quad (9)$$

where $\mathbf{CA}_{1,1} = \mathbf{CA}_{\mathbf{U2R},1} = \mathbf{U2R}_{\text{FTP\_WRITE}} = \mathbf{FTP\_WRITE}$, $\mathbf{CA}_{1,2} = \mathbf{CA}_{\mathbf{U2R},2} = \mathbf{U2R}_{\text{GUESS\_PASSWD}} = \mathbf{GUESS\_PASSWD}$, $\mathbf{CA}_{1,3} = \mathbf{CA}_{\mathbf{U2R},3} = \mathbf{U2R}_{\text{IMAP}} = \mathbf{IMAP}$, $\mathbf{CA}_{1,4} = \mathbf{CA}_{\mathbf{U2R},4} = \mathbf{U2R}_{\text{MULTIHOP}} = \mathbf{MULTIHOP}$, $\mathbf{CA}_{1,5} = \mathbf{CA}_{\mathbf{U2R},5} = \mathbf{U2R}_{\text{PHF}} = \mathbf{PHF}$, $\mathbf{CA}_{1,6} = \mathbf{CA}_{\mathbf{U2R},6} = \mathbf{U2R}_{\text{SPY}} = \mathbf{SPY}$, $\mathbf{CA}_{1,7} = \mathbf{CA}_{\mathbf{U2R},7} = \mathbf{U2R}_{\text{WAREZCLIENT}} = \mathbf{WAREZCLIENT}$, $\mathbf{CA}_{1,8} = \mathbf{CA}_{\mathbf{U2R},8} = \mathbf{U2R}_{\text{WAREZMASTER}} = \mathbf{WAREZMASTER}$ – cyberattacks subclasses of class U2R according to KDD 99 base (Table 1).

$$\mathbf{CA}_4 = \{\bigcup_{j=1}^{4} \mathbf{CA_{ij}}\} = \{\mathbf{CA_{1,1}}, \mathbf{CA_{1,2}}, \mathbf{CA_{1,3}}, \mathbf{CA}_{1,4}\} = \{\mathbf{CA}_{\mathbf{PROBE},1}, \mathbf{CA}_{\mathbf{PROBE},2}, \mathbf{CA}_{\mathbf{PROBE},3}, \mathbf{CA}_{\mathbf{PROBE},4}\} = \mathbf{= \{PROBE}_{\mathbf{IPSWEEP}}, \mathbf{PROBE}_{\mathbf{NMAP}}, \mathbf{PROBE}_{\mathbf{PORTSWEEP}}, \mathbf{PROBE}_{\mathbf{SATAN}}\} = \mathbf{= \{IPSWEEP, NMAP, PORTSWEEP, SATAN\},} \quad (10)$$

where $\mathbf{CA}_{1,1} = \mathbf{CA}_{\mathbf{PROBE},1} = \mathbf{PROBE}_{\mathbf{IPSWEEP?}} = \mathbf{IPSWEEP}$, $\mathbf{CA_{1,2}} = \mathbf{CA}_{\mathbf{PROBE},2} = \mathbf{PROBE}_{\mathbf{NMAP}} = \mathbf{NMAP}$, $\mathbf{CA_{1,3}} = \mathbf{CA}_{\mathbf{PROBE},3} = \mathbf{PROBE}_{\mathbf{PORTSWEEP}} = \mathbf{PORTSWEEP}$, $\mathbf{CA}_{1,4} = \mathbf{CA}_{\mathbf{PROBE},4} = \mathbf{PROBE}_{\mathbf{SATAN}} = \mathbf{SATAN}$ – cyberattacks subclasses of class **PROBE** according to KDD 99 base (Table 1).

Each of the attacks, which belong to one of these classes, is represented as a tuple of parameters [13]:

$$< D, PT, S, F, SB, DB, L, WF, U, H, NFL, LI, NC, RS, SA, NR, NFC, NS, NAF, NOC, IHL, IGL, C, SC, SR, SSR, RR, SRR, SSER, DSR, SDHR, DHC, DHSC, DHSSR, DHDSR, DHSSPR, DHSDHR, DHSR, DHSSR, DHRR, DHSRR > \quad (11)$$

All the above parameters of a tuple are divided into 4 categories [12, 13]:

1. Characteristics of the individual TCP-connections (Table 2); 2. Characteristics of content (Table 3); 3. Characteristics of traffic using the two-second time window (Table 4); 4. Characteristics of the destination host (Table 5).

Table 2. Characteristics of the Individual TCP-Connections

Code	Name	Description	Data type
D	duration	connection time (in seconds)	continuous
PT	protocol_type	protocol type, ie tcp, udp, etc.	discrete
S	service	target service that used, ie http, telnet, etc.	discrete
SB	src_bytes	the number of bytes transferred from the source to destination at one connection	continuous
DB	dst_bytes	the number of bytes transferred from destination to the source at one connection	continuous
F	flag	status of connection: normal, error	discrete
L	land	If the source and the receiver has the same numbers of ports, the parameter takes the value of “1”, if not – “0”	discrete
WF	wrong_fragment	the total number of damaged fragments in a particular connection	continuous
U	urgent	the number of urgent packets in a particular connection. Urgent packet - it is a packet in which URG bit of urgency was enabled	continuous

Table 3. Characteristics of Content

Code	Name	Description	Data type
H	hot	the number of "hot" indicators that are includes at content, such as entry into system directories, creation and execution of programs	continuous
NFL	num_failed_logins	the number of authorization failures	continuous
LI	logged_in	Authorization status: "1" - authorization is successful, "0" - failed	discrete
NC	num_compromised	the number of compromised conditions	continuous
RS	root_shell	"1" if an administrator rights were received, "0" - if not	discrete
SA	su_attempted	"1" if there was an attempt to get administrator rights or if an administrator rights were received, "0" - if not	discrete
NR	num_root	the number of administrative access, or the number of operations performed by an administrator in a particular connection	continuous

End of Table 3

NFC	num_file_creations	the number of operations of the files creation in a particular connection	continuous
NS	num_shells	the number of requests for access to the administration shell	continuous
NAF	num_access_files	the number of operations with access control file	continuous
NOC	num_outbound_cmds	the number of outgoing commands in ftp session	continuous
IHL	is_hot_login	"1" if the authorization belongs to the "hot" list ie administrators,"0" - if not	discrete
IGL	is_guest_login	"1" if the authorization belongs to the guest account, "0" - if not	discrete

Table 4. Characteristics of Traffic using the Two-Second Time Window

Code	Name	Description	Data type
C	count	the number of connections to the target host during the time interval of 2 seconds	continuous
SR	serror_rate	% of connections with error type SYN for the host source	continuous
RR	rerror_rate	% of connections with error type REJ for the host source	continuous
SSR	same_srv_rate	% of connections to the service	continuous
DSR	diff_srv_rate	% of connections with different services	continuous
SC	srv_count	the number of connections to the current service (port number) for the last 2 seconds.	continuous
SSER	srv_serror_rate	% of connections with error type SYN for the source service	continuous
SRR	srv_rerror_rate	% of connections with error type REJ for the source service	continuous
SDHR	srv_diff_host_rate	% of connections with different hosts	continuous

Table 5. Characteristics of the Destination Host

Code	Name	Description	Data type
DHC	dst_host_count	the number of connections to the host	continuous
DHSC	dst_host_srv_count	the number of connections to the service	continuous
DHSSR	dst_host_same_srv_rate	% of connections to the service on this host	continuous
DHDSR	dst_host_diff_srv_rate	% of connections with different services on this host	continuous
DHSSPR	dst_host_same_src_port_rate	% of connections to this host with current source port number	continuous
DHSDHR	dst_host_srv_diff_host_rate	% of connections to the service from different hosts	continuous
DHSR	dst_host_serror_rate	% of connections with error type SYN for this destination host	continuous
DHSSR	dst_host_srv_serror_rate	% of connections with error type SYN for this destination service	continuous
DHRR	dst_host_rerror_rate	% of connections with error type REJ for this destination host	continuous
DHSRR	dst_host_srv_rerror_rate	% of connections with error type REJ for this destination service	continuous

By using the expressions (3-5) will forms the value $r_{ij}(i=\overline{1,n},\ j=\overline{1,m_i})$. For example, KDD 99 base as shown in Table 1-5

$$r_{ij} = 41(i=\overline{1,4},\ m_1=6,\ m_2=4,\ m_3=8,\ m_4=4).$$

As if **CA** we choose the set of cyberattacks parameters standards from KDD 99, than $\mathbf{CA} = \mathbf{CA}_{KDD}$ and then we get:

$$\mathbf{CA}_{KDD} = \{\bigcup_{i=1}^{4}\mathbf{CA}_i\} = \{\bigcup_{i=1}^{4}\{\bigcup_{j=1}^{m_i}\mathbf{CA}_{ij}\}\} = \{\bigcup_{i=1}^{4}\{\bigcup_{j=1}^{m_i}\{\bigcup_{s=1}^{41}\mathbf{CA}_{ijs}\}\}\} =$$

$$= \{\{\{\mathbf{CA}_{1,1,1},\mathbf{CA}_{1,1,2},...,\mathbf{CA}_{1,1,r_1}\},\{\mathbf{CA}_{1,2,1},\mathbf{CA}_{1,2,2},...,\mathbf{CA}_{1,2,r_2}\},...,\{\mathbf{CA}_{1,m_1,1},\mathbf{CA}_{1,m_1,2},...,\mathbf{CA}_{1,m_1,r_{m1}}\}\},$$
$$\{\{\mathbf{CA}_{2,1,1},\mathbf{CA}_{2,1,2},...,\mathbf{CA}_{2,1,r_1}\},\{\mathbf{CA}_{2,2,1},\mathbf{CA}_{2,2,2},...,\mathbf{CA}_{2,2,r_2}\},...,\{\mathbf{CA}_{2,m_2,1},\mathbf{CA}_{2,m_2,2},...,\mathbf{CA}_{2,m_2,r_{m2}}\}\},$$
$$...,$$
$$\{\{\mathbf{CA}_{n,1,1},\mathbf{CA}_{n,1,2},...,\mathbf{CA}_{n,1,r_1}\},\{\mathbf{CA}_{n,2,1},\mathbf{CA}_{n,2,2},...,\mathbf{CA}_{n,2,r_2}\},...,\{\mathbf{CA}_{n,m_n,1},\mathbf{CA}_{n,m_n,2},...,\mathbf{CA}_{n,m_n,r_{mn}}\}\}\} =$$

$$= \{\{\{\mathbf{CA}_{1,1,1},\mathbf{CA}_{1,1,2},...,\mathbf{CA}_{1,1,41}\},\{\mathbf{CA}_{1,2,1},\mathbf{CA}_{1,2,2},...,\mathbf{CA}_{1,2,41}\},...,\{\mathbf{CA}_{1,6,1},\mathbf{CA}_{1,6,2},...,\mathbf{CA}_{1,6,41}\}\},$$
$$\{\{\mathbf{CA}_{2,1,1},\mathbf{CA}_{2,1,2},...,\mathbf{CA}_{2,1,41}\},\{\mathbf{CA}_{2,2,1},\mathbf{CA}_{2,2,2},...,\mathbf{CA}_{2,2,41}\},...,\{\mathbf{CA}_{2,4,1},\mathbf{CA}_{2,4,2},...,\mathbf{CA}_{2,4,41}\}\},$$
$$\{\{\mathbf{CA}_{3,1,1},\mathbf{CA}_{3,1,2},...,\mathbf{CA}_{3,1,41}\},\{\mathbf{CA}_{3,2,1},\mathbf{CA}_{3,2,2},...,\mathbf{CA}_{3,2,41}\},...,\{\mathbf{CA}_{3,8,1},\mathbf{CA}_{3,8,2},...,\mathbf{CA}_{3,8,41}\}\},$$
$$\{\{\mathbf{CA}_{4,1,1},\mathbf{CA}_{4,1,2},...,\mathbf{CA}_{4,1,41}\},\{\mathbf{CA}_{4,2,1},\mathbf{CA}_{4,2,2},...,\mathbf{CA}_{4,2,41}\},...,\{\mathbf{CA}_{4,4,1},\mathbf{CA}_{4,4,2},...,\mathbf{CA}_{4,4,41}\}\}\} =$$

$$= \{\{\{\mathbf{CA}_{DOS,1,1},\mathbf{CA}_{DOS,1,2},...,\mathbf{CA}_{DOS,1,41}\},\{\mathbf{CA}_{DOS,2,1},\mathbf{CA}_{DOS,2,2},...,\mathbf{CA}_{DOS,2,41}\},...,\{\mathbf{CA}_{DOS,6,1},\mathbf{CA}_{DOS,6,2},...,\mathbf{CA}_{DOS,6,41}\}\},$$
$$\{\{\mathbf{CA}_{R2L,1,1},\mathbf{CA}_{R2L,1,2},...,\mathbf{CA}_{R2L,1,41}\},\{\mathbf{CA}_{R2L,2,1},\mathbf{CA}_{R2L,2,2},...,\mathbf{CA}_{R2L,2,41}\},...,\{\mathbf{CA}_{R2L,4,1},\mathbf{CA}_{R2L,4,2},...,\mathbf{CA}_{R2L,4,41}\}\},$$
$$\{\{\mathbf{CA}_{U2R,1,1},\mathbf{CA}_{U2R,1,2},...,\mathbf{CA}_{U2R,1,41}\},\{\mathbf{CA}_{U2R,2,1},\mathbf{CA}_{U2R,2,2},...,\mathbf{CA}_{U2R,2,41}\},...,\{\mathbf{CA}_{U2R,8,1},\mathbf{CA}_{U2R,8,2},...,\mathbf{CA}_{U2R,8,41}\}\},$$
$$\{\{\mathbf{CA}_{PROBE,1,1},\mathbf{CA}_{PROBE,1,2},...,\mathbf{CA}_{PROBE,1,41}\},\{\mathbf{CA}_{PROBE,2,1},\mathbf{CA}_{PROBE,2,2},...,\mathbf{CA}_{PROBE,2,41}\},...,$$
$$\{\mathbf{CA}_{PROBE,4,1},\mathbf{CA}_{PROBE,4,2},...,\mathbf{CA}_{PROBE,4,41}\}\}\} =$$
$$= \{\{\{\mathbf{DOS}_{BACK,1},\mathbf{DOS}_{BACK,2},...,\mathbf{DOS}_{BACK,41}\},\{\mathbf{DOS}_{LAND,1},\mathbf{DOS}_{LAND,2},...,\mathbf{DOS}_{LAND,41}\},...,$$
$$\{\mathbf{DOS}_{TEARDROP,1},\mathbf{DOS}_{TEARDROP,2},...,\mathbf{DOS}_{TEARDROP,41}\}\},$$
$$\{\{\mathbf{R2L}_{BUFFER\_OVERFLOW,1},\mathbf{R2L}_{BUFFER\_OVERFLOW,2},...,\mathbf{R2L}_{BUFFER\_OVERFLOW,41}\},\{\mathbf{R2L}_{PERL,1},\mathbf{R2L}_{PERL,2},...,\mathbf{R2L}_{PERL,41}\},...,$$
$$\{\mathbf{R2L}_{ROOTKIT,1},\mathbf{R2L}_{ROOTKIT,2},...,\mathbf{R2L}_{ROOTKIT,41}\}\},$$
$$\{\{\mathbf{U2R}_{FTP\_WRITE,1},\mathbf{U2R}_{FTP\_WRITE,2},...,\mathbf{U2R}_{FTP\_WRITE,41}\},\{\mathbf{U2R}_{GUESS\_PASSWD,1},$$
$$\mathbf{U2R}_{GUESS\_PASSWD,2},...,\mathbf{U2R}_{GUESS\_PASSWD,41}\},...,\{\mathbf{U2R}_{WAREZMASTER,1},\mathbf{U2R}_{WAREZMASTER,2},...,\mathbf{U2R}_{WAREZMASTER,41}\}\},$$
$$\{\{\mathbf{PROBE}_{IPSWEEP,1},\mathbf{PROBE}_{IPSWEEP,2},...,\mathbf{PROBE}_{IPSWEEP,41}\},\{\mathbf{PROBE}_{NMAP,1},\mathbf{PROBE}_{NMAP,2},...,\mathbf{PROBE}_{NMAP,41}\},...,$$
$$\{\mathbf{PROBE}_{SATAN,1},\mathbf{PROBE}_{SATAN,2},...,\mathbf{PROBE}_{SATAN,41}\}\}\} =$$
$$= \{\{\{\mathbf{DOS}_{BACK,D},\mathbf{DOS}_{BACK,PT},...,\mathbf{DOS}_{BACK,DHSRR}\},\{\mathbf{DOS}_{LAND,D},\mathbf{DOS}_{LAND,PT},...,\mathbf{DOS}_{LAND,DHSRR}\},...,$$
$$\{\mathbf{DOS}_{TEARDROP,D},\mathbf{DOS}_{TEARDROP,PT},...,\mathbf{DOS}_{TEARDROP,DHSRR}\}\},\{\{\mathbf{R2L}_{BUFFER\_OVERFLOW,D},\mathbf{R2L}_{BUFFER\_OVERFLOW,PT},...,$$
$$\mathbf{R2L}_{BUFFER\_OVERFLOW,DHSRR}\},\{\mathbf{R2L}_{PERL,D},\mathbf{R2L}_{PERL,PT},...,\mathbf{R2L}_{PERL,DHSRR}\},...,$$
$$\{\mathbf{R2L}_{ROOTKIT,D},\mathbf{R2L}_{ROOTKIT,PT},...,\mathbf{R2L}_{ROOTKIT,DHSRR}\}\},$$
$$\{\{\mathbf{U2R}_{FTP\_WRITE,D},\mathbf{U2R}_{FTP\_WRITE,PT},...,\mathbf{U2R}_{FTP\_WRITE,DHSRR}\},\{\mathbf{U2R}_{GUESS\_PASSWD,D},$$
$$\mathbf{U2R}_{GUESS\_PASSWD,PT},...,\mathbf{U2R}_{GUESS\_PASSWD,DHSRR}\},...,$$
$$\{\mathbf{U2R}_{WAREZMASTER,D},\mathbf{U2R}_{WAREZMASTER,PT},...,\mathbf{U2R}_{WAREZMASTER,DHSRR}\}\},$$
$$\{\{\mathbf{PROBE}_{IPSWEEP,D},\mathbf{PROBE}_{IPSWEEP,PT},...,\mathbf{PROBE}_{IPSWEEP,DHSRR}\},$$
$$\{\mathbf{PROBE}_{NMAP,D},\mathbf{PROBE}_{NMAP,PT},...,\mathbf{PROBE}_{NMAP,DHSRR}\},...,$$
$$\{\mathbf{PROBE}_{SATAN,D},\mathbf{PROBE}_{SATAN,PT},...,\mathbf{PROBE}_{SATAN,DHSRR}\}\}\} =$$
$$= \{\{\{\mathbf{BACK}_D,\mathbf{BACK}_{PT},...,\mathbf{BACK}_{DHSRR}\},\{\mathbf{LAND}_D,\mathbf{LAND}_{PT},...,\mathbf{LAND}_{DHSRR}\},...,$$
$$\{\mathbf{TEARDROP}_D,\mathbf{TEARDROP}_{PT},...,\mathbf{TEARDROP}_{DHSRR}\}\},$$
$$\{\{\mathbf{BUFFER\_OVERFLOW}_D,\mathbf{BUFFER\_OVERFLOW}_{PT},...,\mathbf{BUFFER\_OVERFLOW}_{DHSRR}\},$$
$$\{\mathbf{PERL}_D,\mathbf{PERL}_{PT},...,\mathbf{PERL}_{DHSRR}\},...,\{\mathbf{ROOTKIT}_D,\mathbf{ROOTKIT}_{PT},...,\mathbf{ROOTKIT}_{DHSRR}\}\},$$
$$\{\{\mathbf{FTP\_WRITE}_D,\mathbf{FTP\_WRITE}_{PT},...,\mathbf{FTP\_WRITE}_{DHSRR}\},$$
$$\{\mathbf{GUESS\_PASSWD}_D,\mathbf{GUESS\_PASSWD}_{PT},...,\mathbf{GUESS\_PASSWD}_{DHSRR}\},...,$$
$$\{\mathbf{WAREZMASTER}_D,\mathbf{WAREZMASTER}_{PT},...,\mathbf{WAREZMASTER}_{DHSRR}\}\},$$
$$\{\{\mathbf{IPSWEEP}_D,\mathbf{IPSWEEP}_{PT},...,\mathbf{IPSWEEP}_{DHSRR}\},\{\mathbf{NMAP}_D,\mathbf{NMAP}_{PT},...,\mathbf{NMAP}_{DHSRR}\},...,$$
$$\{\mathbf{SATAN}_D,\mathbf{SATAN}_{PT},...,\mathbf{SATAN}_{DHSRR}\}\}, \quad (12)$$

where $\mathbf{CA}_{1,1,1} = \mathbf{CA}_{DOS,1,1} = \mathbf{DOS}_{BACK,1} = \mathbf{CA}_{4,4,1} = \mathbf{CA}_{PROBE,4,1} = \mathbf{PROBE}_{SATAN,1} = \mathbf{DOS}_{BACK,D} = \mathbf{BACK}_D$, $\mathbf{CA}_{1,1,2} = \mathbf{CA}_{DOS,1,2} = \mathbf{DOS}_{BACK,2} = \mathbf{PROBE}_{SATAN,D} = \mathbf{SATAN}_D$, $\mathbf{CA}_{n,m_n,2} = \mathbf{CA}_{4,4,2} = \mathbf{DOS}_{BACK,PT} = \mathbf{BACK}_{PT}$, $\mathbf{CA}_{1,1,r_1} = \mathbf{CA}_{1,1,41} = \mathbf{CA}_{DOS,1,41} = \mathbf{CA}_{PROBE,4,2} = \mathbf{PROBE}_{SATAN,2} = \mathbf{PROBE}_{SATAN,PT} = \mathbf{SATAN}_{PT}$, $\mathbf{DOS}_{BACK,41} = \mathbf{DOS}_{BACK,DHSRR} = \mathbf{BACK}_{DHSRR}$, …, $\mathbf{CA}_{n,m_n,1} = \mathbf{CA}_{n,m_n,r_{mn}} = \mathbf{CA}_{4,4,41} = \mathbf{CA}_{PROBE,4,41} = \mathbf{PROBE}_{SATAN,41} =$

$\mathbf{PROBE}_{\mathbf{SATAN},DHSRR} = \mathbf{SATAN}_{DHSRR}$ - parameters subsets of the subclasses of cyberattacks.

According to the set of cyberattacks parameters standards (8) will forms the set of current parameters **SP**, that recorded by the sensors at the time period τ:

$$\mathbf{SP}^{\tau} = \{\bigcup_{z=1}^{q} \mathbf{SP}_z^{\tau}\} = \{SP_1^{\tau}, SP_2^{\tau}, ..., SP_q^{\tau}\}, \quad (13)$$

where $(z = \overline{1,q})$, q – number of current parameters.

For example, using the expression (13) for the particular case [13], if $r_{ij} = q = 41(\forall i,j)$ considering (11), we get:

$$\mathbf{SP}^{\tau} = \{\bigcup_{z=1}^{41} \mathbf{SP}_z^{\tau}\} = \{SP_1^{\tau}, SP_2^{\tau}, ..., SP_{41}^{\tau}\} = \quad (14)$$
$$= \{D^{\tau}, PT^{\tau}, ..., DHSRR^{\tau}\}.$$

Phase 2 – Identification the type of cyberattack. For comparison, current parameters which were records by sensors with standard parameters of cyberattacks introduce logic function of equivalence:

$$E(x, y) = \begin{cases} 1, \textit{ when } x = y, \\ 0, \textit{ when } x \neq y. \end{cases} \quad (15)$$

For example, at the time period τ = 1 the set of parameters signatures, which were measured by ITS sensors, entering to the system (descriptions of the parameters are shown in Tables 2-5):

SP^1={184, tcp, telnet, SF, 1511, 2957, 0, 0, 0, 3, 0, 1, 2, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0.00, 0.00, 0.00, 0.00, 1.00, 0.00, 0.00, 1, 3, 1.00, 0.00, 1.00, 0.67, 0.00, 0.00, 0.00, 0.00}.

Categorization of cyberattacks occurred by comparing the input data **SP** with attacks templates (according to (12)), comparing each of given in (11) parameters using the functions of equivalence (15). As a result, the cyberattack with R2L class and *buffer_overflow* subclass was classified.

Phase 3 – Categorization of cyberincidents. For implementation of this phase we define the set of cyberincidents $\mathbf{I}$ that may arise as a result of cyberattacks CA:

$$\mathbf{I} = \{\bigcup_{i=1}^{n} \mathbf{I}_i\} = \{\mathbf{I}_1, \mathbf{I}_2, ..., \mathbf{I}_n\}, \ (i = \overline{1,n}), \quad (16)$$

where n – number of possible cyberincidents types.

For example, according to the most common types of contemporary computer threats, according to [11] under the categories of cyberincidents will understand (Table 6).

Table 6. Categories of Cyberincidents According to CERT-UA

Code	Category	Description	Definition
MW	Malware	Defeat ITS by viruses and others malicious software	One of the most common ways of infection is drive-by download - infection the users computer when visiting malicious website. Viruses: network worms (networm) is the subclass of viruses that infect computers and looking for ways to spread the network, creating their own copies; trojan programs are programs, that designed for hidden (under the guise of something else) entering the system, usually with malicious intent; rootkits are the set of programs designed to hide the fact of "presence" intruders in the system (computer); keyboard spyware (keylogger) are providing record all of the interruptions that come into the system input at the moment of pressing keys on the keyboard; advertising systems (adware) is malicious software designed to impose advertising means, as an example, blocking user actions by "popup window" that contains advertising material)
IF	Internet Fraud	Implementation of Internet fraud	Phishing attack is prompting the users to enter their authentication information (login, password, banking information) and other information by assurance of users the veracity and authenticity of false (specially created for this) network resources (including a link, which is needed to go) such as mail, websites designed for Internet banking, login page in social networks, etc; vishing is type of fraud to obtain from user during a call information that is necessary for attacker by using different methods of persuasion . One of the varieties of "social engineering"
UA	Unauthorized Access	Unauthorized access to information resources and ITS	Targeted hacking - actions aimed at violating the regular mode of operation of the system, violation of the availability of services (components), obtaining of unauthorized access to confidential information, violation of the integrity of information etc; website defacement attack it is changing the content of the main page of the website, in result at the moment of website visiting instead of the usual content displayed something else (the inscription "hacked by", obscene or vulgar phrases / pictures, etc.)
BN	Botnet	Bot networks	The set of computers, which were infected by malicious software, resources of which (both informational and industrial) through a special command-control servers (C & C) are illegally used by hackers (ZeuS, SpyEye, Carberp, Rustock, Kelihos, Pandora, BlackEnergy)

End of Table 6

DD	DDoS	Implementation of DDoS-attacks	A distributed network attack, which through a large number of sources is intended to disrupt the availability of the service (automated system) by exhausting its computing resources
MT	Money Theft	Money Theft	Unlawful appropriation of the persons funds which implemented by hackers using the resources of cyberspace
IT	Identity Theft	"Identity theft"	Unauthorized acquisition of personal data of individuals, which allows an attacker to operate (to sign documents, get access to resources, use the services, etc.) on its behalf (as one of the authentication mechanisms of individuals can be used the electronic digital signature)

Next, using the expression (16) and data from the Table 6, if $n = 7$ we get:

$$\begin{aligned}\mathbf{I} &= \{\bigcup_{i=1}^{7}\mathbf{I}_i\} = \{I_1, I_2, I_3, I_4, I_5, I_6, I_7\} = \\ &= \{I_{MW}, I_{IF}, I_{UA}, I_{BN}, I_{DD}, I_{MT}, I_{IT}\} = \\ &= \{MW, IF, UA, BN, DD, MT, IT\},\end{aligned} \quad (17)$$

where

$$I_1 = I_{MW} = MW,\ I_2 = I_{IF} = IF,$$
$$I_4 = I_{BN} = BN,\ I_5 = I_{DD} = DD,\ I_6 = I_{MT} = MT,$$
$$I_7 = I_{IT} = IT \text{ – categories of cyberincidents.}$$

Phase 4 – Forming the set of cyberincidents extrapolation rules. To implement this phase is necessary to form a set of basic rules $\mathbf{R}$ [6]:

$$\mathbf{R} = \{\bigcup_{i=1}^{g}\mathbf{R}_i\} = \{\mathbf{R}_1, \mathbf{R}_2, ..., \mathbf{R}_g\},\ (i = \overline{1, g}), \quad (18)$$

where g – number of basic rules.

Similarly to the approach described in [17-20], based on expert evaluation (which does not require large time cost for statistical data forming) is forming a set of rules (17) that establishes connections between subclass of cyberattack **CA** and category of cyberincident $\mathbf{I}$.

Using subclasses of cyberattacks (Phase 1), the implementation of which may cause occurrence of cyberincidents (Phase 3) and considering (17) experts calculates a probability value $PR_{CA_1 I_1}$ ... $PR_{CA_m I_n}$ (normalized from 0 to 1 or percentage) of the occurrence of cyberincident in implementing of a specific class of cyberattacks (19).

$$PR = \begin{vmatrix} PR_{CA_1 I_1} & PR_{CA_1 I_2} & \dots & PR_{CA_1 I_n} \\ PR_{CA_2 I_1} & PR_{CA_2 I_2} & \dots & PR_{CA_2 I_n} \\ \dots & \dots & \dots & \dots \\ PR_{CA_m I_1} & PR_{CA_m I_2} & \dots & PR_{CA_m I_n} \end{vmatrix} \quad (19)$$

Thus, using the statistics describing empirical data of the occurrence of cyberincidents as result of cyberattacks, experts generate probability value $PR_{CA_1 I_1}$ ... $PR_{CA_m I_n}$ and the corresponding set of rules $\mathbf{R}$ (17), which are presented in the following form:

$$\mathrm{R}_g = (PR_{CA_m}^{I_n} \geq PR_{lim}) \rightarrow I_n, \quad (20)$$

where PR_{lim} – is the probability threshold value at which experts believe in the emergence of cyberincident $\mathbf{I}$ as a result of cyberattack **CA** (based on analysis of statistics of cyberincidents).

For example, if m = 22 (Phase 1), n = 7 (Phase 3) experts on the basis of statistics of cyberincidents domestic mobile operator for the last year (Fig. 3) are filling the matrix (19) establishing a connection between the *buffer_overflow* cyberattack subclass defined in Phase 2 and categories of cyberincidents that have been identified (17) in Phase 3 (Table 7). Thus, forming probabilities

$$PR_{buffer\_overflow}^{MW}, PR_{buffer\_overflow}^{IF}, \dots, PR_{buffer\_overflow}^{IT}$$

considering the time period τ, at which *buffer_overflow* cyberattack was implemented. Further, based on the analysis of statistical data is set threshold probability value of cyberincident occurrence PR_{lim} (with this matter the expert analyzes of the attacks that took place simultaneously and determines their differential impact for the occurrence of cyberincident). Next, for the example if $PR_{lim} = 0{,}15$ the expression (20) can be represented as follows:

$$R_1 = (PR_{buffe\_overflow}^{MW} > 0{,}15) \rightarrow MW;$$
$$R_2 = (PR_{buffe\_overflow}^{UA} > 0{,}15) \rightarrow UA;$$
$$R_3 = (PR_{buffe\_overflow}^{BN} > 0{,}15) \rightarrow BN.$$

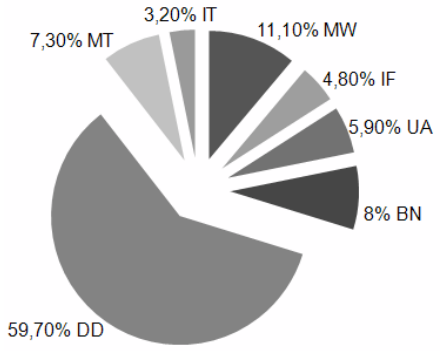

Fig.3. Statistics of Cyberincidents Presented In Categories

Table 7. The Example of Assessment of the Cyberincident Probability in Implementing Cyberattack

Cyberincident / Cyberattack	MW	IF	UA	BN	DD	MT	IT
buffer_overflow	0,18	0,01	0,52	0,21	0,06	0,015	0,005

Because of the formed rules R_1, R_2 and R_3 can be concluded that *buffer_overflow* cyberattack which is implemented at the time period may cause to occur of three types of incidents: Malware (18%), Unauthorized Access (52%) and Botnet (21%). This data is then used to determine the effect of cyberincidents to objects of protection (Phase 6).

Phase 5 – Determination of protection objects. To determine protection objects we will form their set O:

$$\mathbf{O} = \{\bigcup_{i=1}^{n} \mathbf{O}_i\} = \{O_1, O_2, ..., O_n\}, \ (i = \overline{1,n}), \quad (21)$$

where n – number of protection objects.

For example, as objects of protection may be the components of ITS. Thus, the input data at this phase are the categories of cyberincidents (defined by Phase 3 method) and ITS components (ITS components can be defined according to [11]). ITS is an environment in which can occur cyberincidents, typical structure of ITS according to [11, 21, 22] given in Table 8.

Table 8. The set of ITS Components According to CERT-UA

Code	ITS component	Description	Definition
SV	Server	Server equipment	Computers with high performance and technical characteristics; usually designed to one or more specific services, such as e-mail exchange, databases, IP-telephony, file storage, etc.
NC	NetChannel	Data transferring environment	Fiber optic lines, cable with type of "twisted pair" telephone cables, wireless data channels (Wi-Fi, Wi-MAX, Bluetooth)
NH	NetHardware	Active network equipment and communications equipment	Switches, routers, modems, wireless access points, telephony and security devices (firewalls, intrusion detection / prevention systems, etc.)
WS	WorkStation	Automated workplaces of employees	Desktops, laptops, mobile devices

Next, using the expression (21) and data from the Table 8, if $n = 4$ we get:

$$\begin{aligned} &\mathbf{O} = \{\bigcup_{i=1}^{4} \mathbf{O}_i\} = \{\mathbf{O_1}, \mathbf{O_2}, \mathbf{O_3}, \mathbf{O_4}\} = \\ &\{\mathbf{O_{SV}}, \mathbf{O_{NC}}, \mathbf{O_{NH}}, \mathbf{O_{WS}}\} = \\ &\{\mathbf{SV}, \mathbf{NC}, \mathbf{NH}, \mathbf{WS}\}, \end{aligned} \quad (22)$$

where $\mathbf{O_1 = O_{SV} = SV}$, $\mathbf{O_2 = O_{NC} = NC}$, $\mathbf{O_3 = O_{NH} = NH}$, $\mathbf{O_4 = O_{WS} = WS}$ – protection objects (ITS components).

Phase 6 – Identification of cyberincidents impact on ITS components. To determine the impact of the cyberincidents which are categorized in Phase 3, on the ITS components that are determined in Phase 5, experts are encouraged to score U impact of the cyberincident on ITS component (23). Cyberincident that having a greater impact, gets a lower score (1, 2), less influential – bigger (3, 4) [23, 24].

$$U = \begin{vmatrix} U_{O_1 I_1} & U_{O_1 I_2} & \dots & U_{O_1 I_n} \\ U_{O_2 I_1} & U_{O_2 I_2} & \dots & U_{O_2 I_n} \\ \dots & \dots & \dots & \dots \\ U_{O_m I_1} & U_{O_m I_2} & \dots & U_{O_m I_n} \end{vmatrix} \quad (23)$$

For example, if $m = 4$ (Phase 5), $n = 7$ (Phase 3) experts fill the Table 9 establishing the connection between ITS component and category of cyberincident.

Table 9. Impact Assessment of Cyberincidents on the Components of ITS

ITS components	Assessments of cyberincidents by types						
	MW	IF	UA	BN	DD	MT	IT
SV	2	3	2	1	1	4	4
NC	3	4	4	2	2	4	4
NH	3	4	3	3	3	3	3
WS	1	1	1	1	1	1	1

The input data are assessing the impact of cyberincident categories on the ITS components. Thus, in case of the occurrence of three cyberincident categories the most impact exposed are such ITS components as WorkStation and Server.

Phase 7 – Identifying of the most critical components of the ITS. Input data at this phase is ITS components (Phase 5). This phase is implemented in two steps:

Step 1. The scoring by experts. Experts define data $U_{O_1 I_1}$ ... $U_{O_m I_n}$ (23), adding in every cell one of the signs: "important" (>) "less important" (<) and "equivalent" (=). Determining the most critical component of ITS may be made, for example, by *pairwise comparisons* (the main advantage is the opportunity of expert to focus on two objects at a time – this advantage is evident with increasing quantity of evaluation objects) and the number of tables should comply the number of experts. In order to determine the most critical component of ITS may be used one of the following in [25] methods, ranging, multiple comparisons, Delphi method, normalization method, vector benefits method, cluster analysis method, method of rank transformation, utility function approximation method and so on.

In Table 9 each k -th expert replacing signs of the ratio on value (score) r_{ij}^k by the rule:

$$r_{ij}^k = \begin{cases} 1, \text{ if } a_i > a_j, \\ 2, \text{ if } a_i = a_j, \\ 3, \text{ if } a_i < a_j, \end{cases} \quad (24)$$

where a_i, a_j – ITS components to be compared.

Step 2. Coordination of the statements of experts. Then performs the coordination of matrix of each expert R^k, in result is forming reduced matrix of collective benefits [9]. Coordination can be performed by various algorithms. Table 9 used 3 point scale (<, >, =). Can be used larger point scales. In case of violation of transitivity advantages the situation when the matrix is not a ranking R^*, may arise, that is not to determine benefits. Then constructed a ranking R that is closest to the group opinion. By denoting $d(R, R^*)$ the distance between R and R^*, we get the request $d(R, R^*)\min$. Group selection R^* is determined by:

$$\sum_{k=1}^{K} d(R^*, R^k) = \min_{R \in R(n)} \sum_{k=1}^{K} d(R, R^k). \quad (25)$$

Calculated score WC of each criteria as the sum r_{ij}^k (perhaps some other algorithm, it is important to reflect the "weight" of criteria which specified in the experts paired comparisons of criteria) and defines the place of criteria in the ranking RC. Table 10 filled on the basis of agreed estimates of experts concerning the most critical components of the ITS.

Output data of this phase is the assessment of the criticality of ITS components.

For example, if $i = j = 4$ (Phase 5) experts determine the value $r_{O_1O_1}^k$ ... $r_{O_iO_j}^k$ by filling the Table 11 determining the most critical of ITS components.

Table 10. Determination of the Most Critical ITS Components

ITS components / ITS components	$\mathbf{O}_1$	$\mathbf{O}_2$	…	$\mathbf{O}_i$	Score, "weight" of criteria	Place of criteria in the ranking
$\mathbf{O}_1$	$r_{O_1O_1}^k$	$r_{O_2O_1}^k$	…	$r_{O_iO_1}^k$	WC_1	RC_1
$\mathbf{O}_2$	$r_{O_1O_2}^k$	$r_{O_2O_2}^k$	…	$r_{O_iO_2}^k$	WC_2	RC_2
…	…	…	…	…	…	…
$\mathbf{O}_j$	$r_{O_1O_j}^k$	$r_{O_2O_j}^k$	…	$r_{O_iO_j}^k$	WC_m	RC_n

Table 11. Determination of the most Critical Of ITS Components

ITS components / ITS components	SV	NC	NH	WS	Score, "weight" of criteria	Place of criteria in the ranking
SV		>	>	>	3	1
NC	<		>	>	5	2
NH	<	<		>	8	3
WS	<	<	<		9	4

Thus, we have score of the criterion according to which determining place of criteria in the ranking. Most critical in this case is ITS Server, and the least critical is WorkStation.

Phase 8 – Cyberincidents degrees of danger ranking. The input data of this phase is the assessment of the criticality of ITS components (Phase 7, Table 10) and assessments the impact of cyberincidents on ITS components (Phase 6 (23)).

Determining the comparative importance of possible damage, to which cyberincident can lead according to the values of each criterion (26) and their "weights" (Table 10). It is important for dispatching strategies and operational impacts. The assessment of comparative importance can be calculated using the formula:

$$Q_j = \sum_{i=1}^{i} a_i x_{ij}, \; j = \overline{1, j}, \quad (26)$$

where x_{ij} – value of i-th criteria j-th cyberincident type in Table 9; a_i – "weight" of i-th criteria in Table 11. When using the criteria values from the Table 11, the smaller the value Q_j, the more danger makes cyberincident.

The calculation of standardized assessments (Table 12) of cyberincidents implements by the formula:

$$\mathbf{IL}_j = \frac{Q_j}{\sum_j Q_j}, \quad (27)$$

Table 12. Evaluation the Danger of Cyberincident

The level of danger	Cyberincident	Standardized assessment
1	$\mathbf{I}_1$	$\mathbf{IL}_1$
2	$\mathbf{I}_2$	$\mathbf{IL}_2$
…	…	…
n	$\mathbf{I}_n$	$\mathbf{IL}_j$

In case of occurrence multiple parallel cyberincidents (probability of this is very high due to shown in Fig. 3 statistics and research), and by having a hazard assessment levels of cyberincidents, it is possible to hold the prioritization of cyberincidents in order to adequate responding to them.

Output data on this phase is the assessment of risk level (criticality) of cyberincidents that arise in result of implemented attack category.

For example, using the values from the Table 9 and Table 11 by the expression (26) calculate the assessment of the danger level of cyberincident (Table 13).

For cyberincident MW we get:

$$Q_1 = 3\times 2 + 5\times 3 + 8\times 3 + 9\times 1 = 54,$$

UA: $Q_2 = 3\times 2 + 5\times 4 + 8\times 3 + 9\times 1 = 59,$

BN: $Q_3 = 3\times 1 + 5\times 2 + 8\times 3 + 9\times 1 = 46.$

Standardized assessments of cyberincidents types calculated by (27): $\mathbf{IL}_1 = 0.34$, $\mathbf{IL}_2 = 0.37$, $\mathbf{IL}_3 = 0.29$, is recording in the Table 13:

Table 13. Evaluation the danger of Cyberincident

The level of danger	Cyberincident	Standardized assessment
1	BN	0,29
2	MW	0,34
3	UA	0,37

Thus, we can conclude that when implementing *buffer_overflow* cyberattack the most danger (most critical) is Botnet cyberincident, then Malware, and at last Unauthorized Access.

V. Conclusions

Thus, in this paper the method for cyberincidents network-centric monitoring was developed which by classifying of cyberattacks and comparing their parameters with standard, forming the set of basic rules and establishing of dependencies between cyberattacks subclass and cyberincidents category based on their statistical processing, identification objects of protection and expert assessment of cyberincidents impact on them, coordination of experts opinions and ranking danger degrees of cyberincidents, which allows to determine the most important objects of protection (components of ITS or cyberspace), and also to predict the categories of cyberincidents that arising because of cyberattack implementation, and their level of risk (criticality). This method and means which were formed on its basis will be useful for cyberincidents response teams of type CERT / CSIRT for efficient processing of cyberincidents (in particular dispatching) and adequate respond to them, and for units that are assigned to protect both within the ITS enterprise and within the state.

Acknowledgment

This scientific work was supported by RAMECS, CCNU16A02015 and Young Scientists Association of National Aviation University (Kyiv, Ukraine).

References

[1] Gnatyuk V., «Analysis of “incident” definitions and its interpretation in cyberspace» Ukrainian Scientific Journal of Information Security, 2013, vol. 19, issue 3, pp. 175-180.

[2] ISO/IEC 27035:2011 — Information technology — Security techniques — Information security incident management, 2011., p. 69.

[3] Gnatyuk V., Volyanska V. Gizun A., «Review of intrusion detection systems based on honeypot technology» Ukrainian Scientific Journal of Information Security, 2012, vol. 18, issue 2, pp. 75-79.

[4] Gizun A., Korchenko A., Skvortsov S., «Analysis of modern crisis management systems», Ukrainian Scientific Journal of Information Security, 2015, vol. 21, issue 1, pp. 86-99.

[5] Sinyavskiy V., «Influence of the content and principles of "network-centric warfare" in the command and control processes», Science and Military Security, 2010, vol. 4, pp. 36-45.

[6] The paradigm of network-centric management and its impact on the command and control processes [Electronic resource]. – Access to resources: http://agat.by/pres/statia%20nayka-3.pdf.

[7] Network-centric warfare and wireless communications: [Electronic resource]. — Access to resources: http://www.meshdynamics.com/military-mesh-networks.html

[8] Zatuliveter Y., «Computer basis of network-centric management, Proceedings of Russian Conference with international participation "Hardware and software in the control system, the control and measurement"», Moscow pp. 17-37, 18-20 October 2010.

[9] Shershakov V., Trahtenherts E., Kamaev D., «Computer support network-centric management practices emergencies», Moscow: Lenand, 2015, p.160.

[10] Gnatyuk S., Hohlachova Y., Ohrimenko A., Grebenkova A., «The theoretical basis of construction and operation of information security incident management», Ukrainian Information Security Research Journal, 2012, vol. 54, issue 1, pp. 121-126.

[11] Gnatyuk S. «Cyberterrorism: development history, current trends & countermeasures», Ukrainian Scientific Journal

of Information Security, 2013, vol. 19, issue 2, pp. 118-129.
[12] Grischuk R., Okhrimchuk V., Akhtyrtseva V., «The sources of primary data for the development potentially dangerous patterns of cyber-attacks», Ukrainian Information Security Research Journal, 2016. vol. 18, issue 1, pp. 21-29.
[13] KDD CUP99 [Electronic resource]. — Access to resources: https://kdd.ics.uci.edu/databases/kddcup99/task.html
[14] Official site Common Attack Pattern Enumeration and Classification [Electronic resource]. — Access to resources: https://capec.mitre.org
[15] CERT-UA. Basic course of Information Security [Electronic resource]. — Access to resources: http://cert.gov.ua
[16] The Law of Ukraine «Information security in telecommunication systems»: № 80/94-BP July 5, 1994, Parliament of Ukraine, vol. 31, p. 286.
[17] Karpinski M., Korchenko A., Akhmetova S., «The method of developmentof basic detection rules for intrusion detection systems», Ukrainian Information Security Research Journal, 2015, vol. 17, issue 4, pp. 312-324.
[18] Gizun A., Gnatyuk V., Suprun O., «Formalized model of construction heuristic rules to detect incidents», Journal of Engineering Academy of Ukraine, 2015. vol. 1, pp. 110-115.
[19] Korchenko A., Gizun A., Volyanska V., Gavrylenko O., «Heuristic rules based on logical & linguistic connection to detect and identify information security intruders», Ukrainian Information Security Research Journal, 2013, vol. 60, issue 3, pp. 251-257.
[20] Gizun A., Gnatyuk V., Balyk N., Falat P., «Approaches to Improve the Activity of Computer Incident Response Teams», Proceedings of the 2015 IEEE 8th International Conference on «Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications», (IDAACS'2015), Warsaw, Poland, September 24-26, 2015, vol. 1, pp. 442-447.
[21] Zhengbing Hu, Vadym Mukhin, Heorhii Loutskii, Yaroslav Kornaga "Stochastic RA-Network for the Nodes Functioning Analysis in the Distributed Computer Systems". International Journal of Computer Network and Information Security(IJCNIS), Vol. 8, No. 6, June 2016, PP.1-8, DOI: 10.5815/ijcnis.2016.06.01
[22] Rasmi M., Al-Qerem A. PNFE: «A proposal approach for proactive network forensics evidence analysis to resolve cyber crimes». International Journal of Computer Network and Information Security (IJCNIS), Vol. 7, No. 2, January 2015, PP.25-32. DOI: 10.5815/ijcnis.2015.02.03.
[23] Karuppanchetty C., Edmonds W., Kim S.-il, Nwanze N. Artificially augmented training for anomaly-based network intrusion detection systems. International Journal of Computer Network and Information Security (IJCNIS), Vol. 7, No. 10, September 2015, PP. 1-14. DOI: 10.5815/ijcnis.2015.10.01
[24] Govindarajan M. Hybrid Intrusion Detection Using Ensemble of Classification Methods. International Journal of Computer Network and Information Security (IJCNIS), Vol. 6, No. 2, January 2014, PP.45-53, DOI: 10.5815/ijcnis.2014.02.07
[25] Gornitska D., Volyanska V., Korchenko A. «Determining factors of importance for expert evaluation in the field of information security», Ukrainian Information Security Research Journal, 2012, vol.54, issue 1, pp. 108-121.

Authors' Profiles

Zhengbing Hu: PhD, Associate Professor of School of Educational Information Technology, Central China Normal University, M.Sc. (2002), Ph.D. (2006) from the National Technical University of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute». Postdoc (2008), Huazhong University of Science and Technology, China. Honorary Associate Researcher (2012), Hong Kong University, Hong Kong. Major research interests: Computer Science and Technology Applications, Artificial Intelligence, Network Security, Communications, Data Processing, Cloud Computing, Education Technology.

Viktor Gnatyuk: PhD Student (2012-2015), Assistant Teacher (from 2013). In 2012 he received MSc degree in Economic Cybernetic from Khmelnitsky National University (Khmelnitsky, Ukraine). He is currently working at NAU in Telecommunication Systems Academic Department. Research interests: Computer Network & Internet Security, IS Incident Management.

Viktoriia Sydorenko: PhD Student (2013-2016), Assistant Teacher (from 2014). In 2012 she received MSc degree in Information Security from NAU. She is currently working at NAU in Academic Department of IT-Security. Research interests: Computer Network & Internet Security, Cybersecurity & Critical Information Infrastructure Protection.

Roman Odarchenko: PhD, Associate Professor of Telecommunication systems academic department in NAU. M.Sc. (2010), Ph.D. (2013) from the NAU, teacher in Kyiv College of Communication. Major research interests: Network Security, Communications, Data Processing, Sensor networks, Computer networks, Education Technology.

Sergiy Gnatyuk: PhD, Associate Professor. In 2007 he received MSc degree in information security from National Aviation University (NAU, Kyiv, Ukraine). He received PhD in Eng degree in information security (quantum cryptography) from NAU in 2011. He is currently working at NAU in Academic Department of IT-Security. IEEE Member, Scientific Adviser of Engineering Academy of Ukraine, Executive Secretary of Ukrainian Scientific Journal of Information Security, Chairman in Young Scientist Association of NAU. Research interests: Cryptography, Quantum Key Distribution, Network & Internet Security, Information Security Incident Management, Cybersecurity & Critical Information Infrastructure Protection.

How to cite this paper: Zhengbing Hu, Viktor Gnatyuk, Viktoriia Sydorenko, Roman Odarchenko, Sergiy Gnatyuk,"Method for Cyberincidents Network-Centric Monitoring in Critical Information Infrastructure", International Journal of Computer Network and Information Security(IJCNIS), Vol.9, No.6, pp. 30-43, 2017.DOI: 10.5815/ijcnis.2017.06.04

