Journal of Engineering and Applied Sciences 12 (Special Issue 4): 6837-6844, 2017
ISSN: 1816-949X

Development of Message Threat Model on the Basis of Composition of Fuzzy Automations

[1]Dmitry Belomoytsev, [1]Tamara Volosatova and [2]Nikolay Chichvarin
[1]Department of CAD Systems,
[2]Department of Informational Security,
Moscow State Technical University Named after N.E. Bauman, Moscow, Russia

Abstract: The relevance of the problem under study is conditioned by the almost complete lack of preliminary works relating to the construction of models of threats to Message Transmission Links (MTL) while the corresponding threats exist. The goal of the study is to construct MTL threat model. The leading approach to the study of this problem is in most cases, building a model based on expert assessments. In this study, a method is proposed, built on the basis of the composition of fuzzy digital automations. Also, the proposed method takes into account the need for continuous modification of the linguistic processor. To simulate the MTL threats, the method of modeling was developed based on the possibility of increasing the model structure. Materials of the study can be useful for specialists in the field of information security and network technologies in assessment of various factors affecting the MTL security.

Key words: Atomation, security, fiber, channel, line, model, communication, expert system

INTRODUCTION

Carried out analysis of the available publications (Pollin and Maxim, 2014; Horev, 1998; Demidov *et al*., 2000; Lagutin, 1997) shows that threat models of message transmission links in the most cases are built on the basis of expert estimates. Thus, a model is built generally based on conventional expert system. It is extremely difficult to predict even development trends of MTL, either methods of MTL protection from UNAX (Vishnevsky and Lyakhov, 2005; Grigoryev and Lagutenko 2005; Olifer and Olifer, 2006). For example, it is very difficult to speak of threats to quantum cryptographic channels in particular, applying the FOL. It should be excessive in variety of physically feasible threats. Actually, the implementation of ideas of the quantum cryptography became available 30 years ago. It is very difficult to build an expert system with the unpredictable capacity of the knowledge base (Lukatsky, 2006). It is reasonable to assert that the method based on the possibility of increasing the model structure should be developed for MTL threat modelling.

Goal and objectives of the study: The goal of researches, carried out when preparing materials to publication is to provide an MTL threat model formal simulation method. The analysis of MTL which converts variable physical nature signals has been carried out for the formulation of the particular problems (Pollin and Maxim, 2014; Horev, 1998; Demidov *et al*., 2000; Lagutin, 1997). Analysis is based on the following key provisions:

- MTL is considered as a communication line, subject to active and passive attacks, even if it provides recording and storing information
- MTL is considered as a communication line, subject to active and passive attacks, even if it is a part of the control systems and transmits control actions
- MTL structural behavioral patterns of the following types are considered
- As the mental image of the design solution with a given degree of adequacy of the actual object
- As behavioral pattern, excessive by a set of design solutions including protection design solutions of transmitted messages

MATERIALS AND METHODS

Radio-electronic MTL: In this study, radio-electronic MTL are considered as the generalization of following systems:

- Radar control and navigation systems
- Radar stations
- Radio-electronic means of communication

Corresponding Author: Dmitry Belomoytsev, Department of CAD Systems,
Moscow State Technical University Named after N.E. Bauman, Moscow, Russia

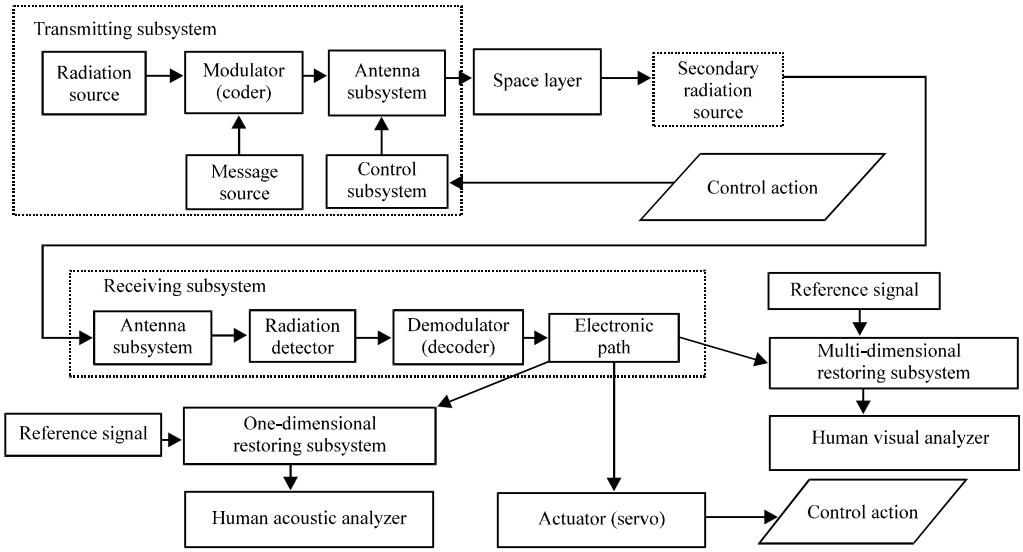

Fig. 1: Radio-electronic MTL structure

Generalized structural scheme of radio-electronic MTL is shown in Fig. 1. The special feature of this model is that, it is focused on the search for design solutions associated with protection of transformed in MTL spatiotemporal signals against UNAX. Shown subsets of design solutions are: subset of radio-electronic systems focused on transmission and reception of signals which are man-processed on the basis of the visual information. This can be television systems, radar stations with a semi-automatic signal processing. In this case, the "secondary source of radiation" block is interpreted either as interference source or the target identified by the radar station; subset of radio-electronic systems intended for transmission and transformation of timing codes in that specific case man-processed audio signals; subset of radio-electronic control and navigation systems both self-guided and remotely managed by different technical objects using man-processed signals.

It should be noted that the presented MTL Model can be considered as both model of the object protection and model of counteraction means (attack).

Optical-electronic MTL: Further, optical-electronic MTL is considered as generalization of the following objects which are subject to protection:

- Optical-electronic locational systems
- Optical-electronic means of information registration and storage
- Optical-electronic control and navigation systems
- Optical-electronic means of communication

Generalized structural model of optic-electronic MTL is presented in Fig. 2. Four subsets of design solutions are specified in the structural model:

- Subset of television, thermal imaging systems which operate only in conjunction with the human visual analyzer
- Subset of video and photographic equipment
- Subset of control systems of technical facilities
- Subset of measuring systems including the lidars, radars, gauges

It should be noted that the space layer in this case can be regarded as free and fiber link. The secondary source of radiation can be available and not available in the considered MTL.

Acoustic-electronic MTL: Acoustic-electronic MTL by analogy with radio-electronic and optical-electronic MTL is considered further as generalization of the following systems.

Acoustic locating system: Acoustic-electronic communications. Last systems are generally focused on solving specific problems of establishing acoustic contacts for obtaining unauthorized information. Generalized acoustic-electronic MTL structural model is shown in Fig. 3. This model is excessive in the totality of the following design solutions:

- Active acoustic locators
- Passive acoustic channels

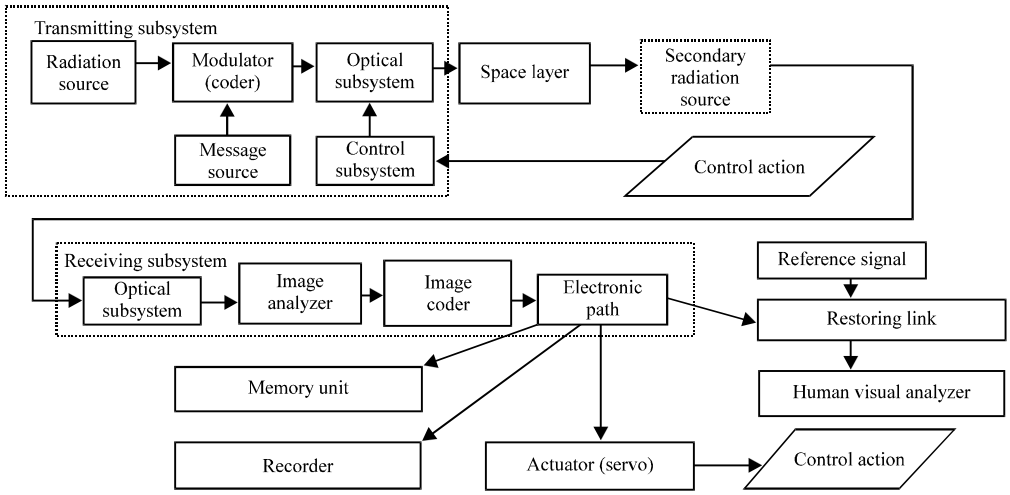

Fig. 2: Optic-electronic MTL structure

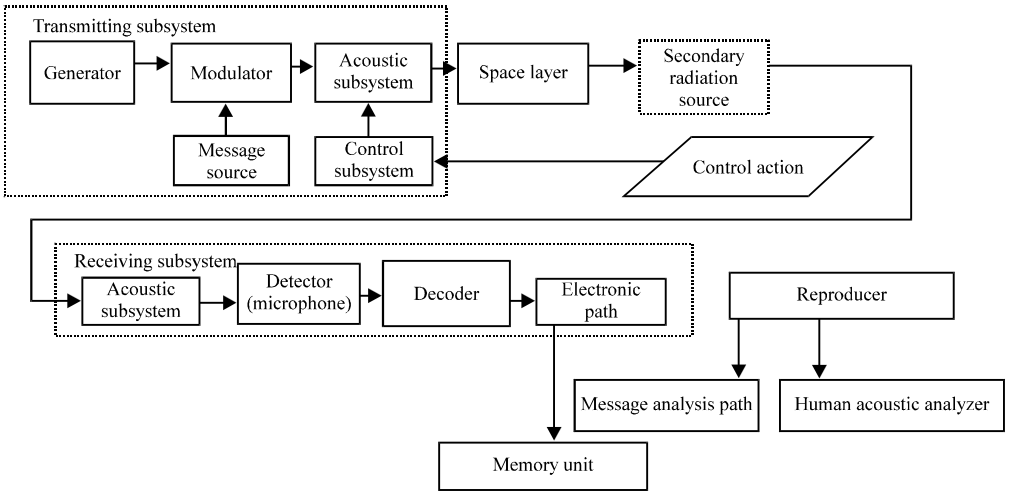

Fig. 3: Acoustic-electronic MTL structure

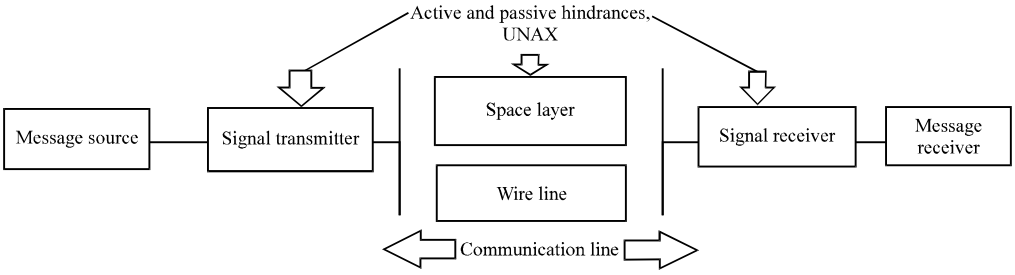

Fig. 4: The generalized MTL flow-chart

The higher degree of generalization allows constructing MTL structural model taking into account harmful influences and points of the signal interception application (Fig. 4).

Analysis of MTL is threat model formation methods: Results of the analytical review of available publications on methods of the Information System Security (ISS) threats model formation are shown in Fig. 5.

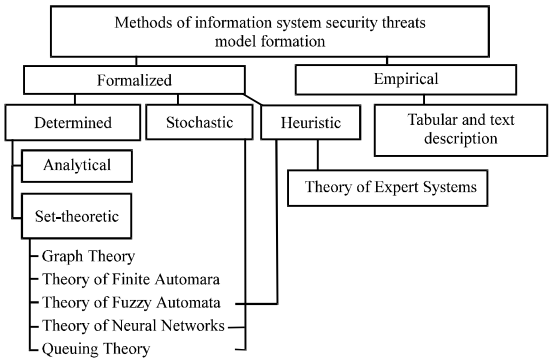

Fig. 5: Results of ISS threats formation methods review

When selecting the approach to create MTL IS threat model such MTL specific properties as permanent change of signal coding and transmitting methods and means are considered. It is considered that it is impossible to create the model of threats, excessive in the totality of design solutions for ensuring IS: parameters and all structure of MTL change continuously. Also, it is considered that the vast majority of MTL IS threats has the verbal description and is estimated in the expert way. Thus, the conclusion is drawn about the selection of threats model in the form of fuzzy automation composition. At that, the formalization of expert estimates is possible on the basis of fuzzy logic known methods too.

RESULTS

First, let us consider a one fuzzy automation with the help of which a countable set of threats and a fixed structure is simulated. The model and procedures selection method are proposed to ensure the information security, based on the use of the fuzzy automation, the application of which makes possible realization of the advanced opportunities in the formalized representation, simulation and assessment of various system parameters and factors of environment influence in conditions of the uncertainty.

This model is intended for assessment, comparison and/or monitoring of applied information security policies, reasonable selection of activities and represents a kind of the fuzzy automation which can be in several active states at once that allows considering simultaneous effect of several activities as well as their interaction and effect on system parameters with the course of time (Goncharov, 2012). The model is presented in the following form:

$$F=<\Sigma, Z, Q(R)\hat{}\delta, \omega, F\_(1)F\_2> \quad (1)$$

Where:

Σ = {a1, ..., am} finite input alphabet
Q = {q1, ..., qm} set of resulting states
Q′ = {q1, ..., qm} set of milestone states (they differ from resulting states in the fact that for them output symbols and output function are not created)
Z = {b1, ..., bk} finite output alphabet
R = Fuzzy initial state
δ = Σ [Q×(0,1)→Q] function of fuzzy transitions which describes for each ordered pair (state and input symbol) the totality of all states where in the transition by given input symbol is possible
ω = Q→Z-output function
F1 = (0,1)×(0,1)→(0,1) function of the state belonging, used in the process of calculating degree value of the new active state belonging when transition
F2 = (0,1)×(0,1)→(0,1) function of multi-belonging used at calculating degree value of the new active state belonging if the transition into it is carried out from several active states at once

At that, states of the object correspond to the states of fuzzy automation and a set of possible effects on the object due to which it changes its state corresponds to the language alphabet of the automation. Unlike conventional automations, fuzzy automations can be not in one but in several (fuzzy) states with various degrees of belonging. This gives additional opportunities in accounting conditions of non-stochastic uncertainty (Martsenyuk, 2014).

Learned fuzzy automation: Let us consider the automation with the clear input i(t) and dependent on time fuzzy transition relation δ(t). Let s(t) be the fuzzy automation state at the time t on a finite totality of states S = {s1, …, sn} and i1 estimate of i(t) value. The state of the automation at moment of time t is determined by min-max composition:

$$\mu\_\left(s\left(t+1\right)\right)\left(s\_k\right) = \sup \min\left[\mu\_\left(s\left(t\right)\right)\right]\left(s\_j\right),$$
$$\left[\left(\mu\_\left(t\right)\right)\right]\left(s\_\left(x\right)i\_1\ s\_j\right)\left(\sup = \sup j\right)$$

or similar to it. Training is aimed at changing the fuzzy matrix of transitions:

$$\mu\_\left(\delta\left(t\right)\right)\left(s\_k,i\_1s\_j\right) = \mu\_\left(\delta\left(t\text{-}1\right)\right)\left(s\_k,i\_1s\_j\right) \quad (2)$$

$$j \neq k\mu\_\left(\delta\left(t\right)\right)\left(s\_k,i\_1s\_j\right) = a\_k\mu\_\left(\delta\left(t\text{-}1\right)\right)$$
$$\left(s\_k,i\_1s\_j\right)+\left(1\text{-}a\_k\right)\lambda\_\left(k\right)\left(t\right) \quad (3)$$

where 0< ak<1, 0< λ_(k) (t)<1, k = 1, …, n. The constant λ_(k) determines training speed. Starting the automation is possible without a priori information μ_(s(0)) (s_k) = 0 or 1 as well with a priori information

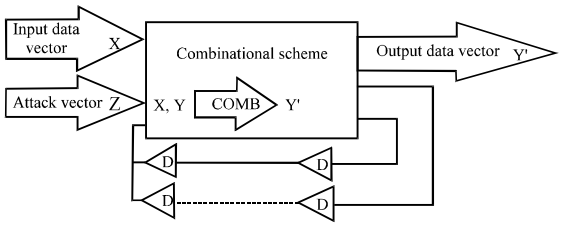

Fig. 6: Structure of the IS Automation Model

μ_(s(0)) (s_k) = λ_(k) (0). Value λ_(k) (t) depends on evaluation of the automation operation. It is proved that there is a convergence of the transition matrix, regardless of a priori information availability, i.e., μ_(s(0)) (s_j) can be any value from the interval (0, 1). Let us consider the example. Figure 6 shows the example of IS threats automaton model.

The role of input and output can be briefly explained as follows. During each time interval the classifier of attacks receives a new sample from the subsystem environment. Further, the reaction of subsystem x is processed in the receptor whereof enters both the "learned" block and the "teacher" block for assessment. The assessment criterion must be chosen, so that its minimization or maximization would reflect classification properties (classes of threats). Therefore, the criterion can be included in the system to serve as the teacher for the classifier. The model of learning is formed as follows. It is assumed that the classifier has at disposal the totality of discriminant functions of several variables. The system adapts to a best solution. The best solution reveals the totality of discriminant functions which give a minimum of consequences among the totality of discriminant functions for this totality of attacks samples.

Learning on the basis of conditional fuzzy measure. Let X = {x1, ..., xn} be a set of the reasons (inputs) and Y = {y1, ..., yn} be a set of results. If h is the function from X in the interval (0, 1), h(x1) <, ..., < h(xn) and Gx is fuzzy measure on X, then:

$$\_\int X^{\wedge}\times\left[h(x)\right]Gx(*)=\max\ \min\left[\begin{pmatrix}h(Xi),\\ Gx(Hi)\end{pmatrix}\right],i=1,\ldots,n \quad (4)$$

Where:

$$hi=\{xi,\ldots,xn\}$$

The objective is to evaluate (more precise define) reasons for the fuzzy information. Let Gy be the fuzzy measure on Y, Gy is connected with Gx by the conditional fuzzy measure σY (*Ix):

$$GY=\int\_X^{\wedge}\times\left[\sigma Y(*Ix)Gx\right] \quad (5)$$

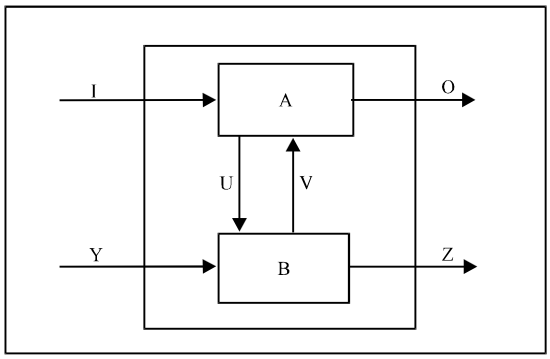

Fig. 7: The composition of automations

The following interpretation of input measures is supposed: Gx assesses the fuzziness degree of the statement "one of x factors of X threats was the reason", σY (*Ix), AϵY assesses the fuzziness degree of the statement "one of A elements is the result due to x reason"; GY({y}) characterizes the fuzziness degree of the statement: "y-actual resul". Let μA(y) describes the fidelity of A information, then by definition:

$$GY(A)=\int\_X^{\wedge}\times\left[\mu A(y)\right]Gx \quad (6)$$

The learning method has to comply with the mandatory condition: when receiving information A, the fuzzy measure Gx changes in such a way that Gy(A) would increase.

Considered models of various automations can be combined into a single model by composition. Let us consider, the composition of A and B automations in Fig. 7. Automation A has the input alphabet I×V and the output alphabet U×O; automation B has the input alphabet Y×U and the output alphabet V×Z. Thus, the language of automation A is LA⊆(I×V×U×O)*, the language of automation B is:

$$LA\subseteq(Y\times U\times V\times Z)^{*} \quad (7)$$

Synchronous composition or simply composition A×B of automations A and B has the input alphabet I×Y and the output alphabet O×Z. Input-output symbol (iyoz) ϵI×Y×O×Z belongs to the language of the composition, if and only if there is the matched pair of internal symbols uv ϵU×V such that (ivuo)ϵLA and (yuvz)ϵLB.

Synchronous composition of automations is built as follows. First, the language of the automation A is extended on the set Y×Z and the language of the automation B is extended on the set I×O through addition on each transition of all possible pairs from the expansion alphabet. Obtained languages are intercrossed and the

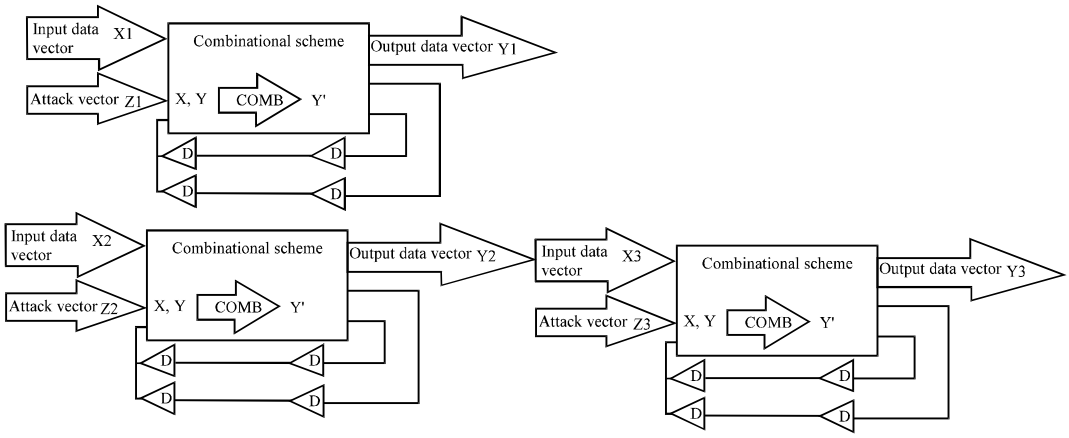

Fig. 8: Parallel-serial composition of three automations: X3-vector of input data of the third automation obtained at the output of the second automation

intersection projection is built on the alphabet of composition I×Y×O×Z. Presented automation under observation with the obtained language is called the composition A×B of automations A and B. All operations over languages can be fulfilled on the basis of relevant known methods (Mordeson and Davender, 2002; Martsenyuk, 2014; Kam *et al*., 1997). An example of the structural composition of the extensible threat model is shown in Fig. 8.

DISCUSSION

For quite a long time, many researchers are involved in issues of messaging process simulation. In particular, according to Lukatsky (2005), the communication can be perfectly summarized as the transmission of a message from a sender to a receiver in the understandable manner. The importance of the effective communication is immeasurable in the world of business and in the personal life. The communication process is the guide towards implementing effective communication. Sharing of a common meaning between the sender and the receiver takes place through the communication process. The communication process consists of four key components. These components are encoding, medium of transmission, decoding and feedback. There are also two other factors in the process and those two factors are present in the form of a sender and a receiver. The communication process begins from a sender and finishes with a receiver. The sender is an individual, group or organization who initiates the communication. This source is initially responsible for the success of the message. The sender's experiences, attitudes, knowledge, skills, perceptions and culture influence the message. "Selected written words, spoken words and nonverbal language are paramount in ensuring receiver's interpretation of the message as intended by the sender". All communication begins from the sender. The first step, the sender encounters with involves the encoding process. In order to convey the meaning, the sender must begin encoding that means translating information into a message in the form of symbols which represent ideas or concepts. This process translates the ideas or concepts into the coded message which will be communicated. Symbols can take on numerous forms such as languages, words or gestures. These symbols are used to encode ideas into messages which others can understand. When encoding a message, the sender has to begin from making decision what he/she wants to transmit. This decision of the sender is based on what he/she believes about the receiver's knowledge and assumptions, along with what additional information he/she wants the receiver to have. It is important for the sender to use symbols that are familiar to the intended receiver. A good way for the sender to improve encoding their message is to mentally visualize the communication from the receiver's point of view. To begin transmitting the message, the sender uses some kind of channel (also called the medium). The channel is mean used to convey the message. Most channels are either verbal or written but currently visual channels become more common as technology expands. Common channels include the telephone and a variety of written forms such as memos, letters and reports. The effectiveness of various channels fluctuates depending on characteristics of the communication. For example, when the immediate feedback is necessary, verbal communication channels are more effective because any uncertainties can be cleared up on the spot. In a situation, when the message must be delivered to more than a small group of people, written channels are often more effective. Although, in many

cases, both verbal and written channels should be used since one supplements the other. If a sender relays a message through an inappropriate channel, its message may not reach the right receivers. That is why, senders need to keep in mind that selecting the appropriate channel will greatly assist in the effectiveness of the receiver's understanding. The sender's decision to utilize either a verbal or a written channel for communicating a message is influenced by several factors. After the appropriate channel or channels are selected, the message enters the decoding stage of the communication process. Decoding is conducted by the receiver. Once, the message is received and examined, the stimulus is sent to the brain for interpreting in order to assign some type of meaning to it. This processing stage constitutes decoding. The receiver begins to interpret symbols sent by the sender, translating the message to his own set of experences in order to make symbols meaningful. Successful communication takes place when the receiver correctly interprets the sender's message. The receiver is the individual or individuals to whom the message is directed. The extent to which this person comprehends the message will depend on a number of factors which include the following: how much the individual or individuals know about the topic, their receptivity to the message and the relationship and the trust that exists between sender and receiver. All interpretations by the receiver are influenced by their experiences, attitudes, knowledge, skills, perceptions and culture. It is similar to the sender's relationship with encoding. Feedback is the final link in the chain of the communication process. After receiving a message, the receiver responds in some way and signals about response to the sender. The signal may take the form of a spoken comment, a long sigh, a written message, a smile or some other action. "Even, a lack of response is in a sense, a form of response". Without feedback, the sender cannot confirm that the receiver has interpreted the message correctly. Feedback is a key component in the communication process because it allows the sender to evaluate the effectiveness of the message. Feedback ultimately provides an opportunity for the sender to take corrective action for clarifying a misunderstood message. "Feedback plays an important role by indicating significant communication barriers: differences in background, different interpretations of words and differing emotional reactions".

According to Mamaev and Petrenko (2002), the transmission model of communication is very well-known model of communication developed by Shannon and Weaver as the prototype example of a transmissive model of communication: a model which reduces communication to a process of "transmitting informatio". The underlying metaphor of communication as transmission underlies "commonsense" everyday usage but is in many ways misleading and repays critical attention. Shannon and Weaver's Model is the omen which is in John Fiske's words, widely accepted as one of the main seeds, out of which communication studies has grown. Claude Shannon and Warren Weaver were not social scientists but engineers working for Bell Telephone Labs in the United States. Their goal was to ensure the maximum efficiency of telephone cables and radio waves. They developed a model of communication which was intended to assist in developing a mathematical theory of the communication. Shannon and Weaver's research proved valuable for communication engineers in dealing with such issues as the capacity of various communication channels in "bits per second". It contributed to the computer science. It led to very useful work on redundancy in language. And in making 'information' 'measurable', it gave birth to the mathematical study of 'information theory'. However, these directions are not our concern here. The problem is that some commentators have claimed that Shannon and Weaver's Model has a much wider application to human communication than a purely technical one. The C and W's original model consisted of five elements: the information source which produces a message; the transmitter which encodes the message into signals; the channel to which signals are adapted for transmission; the receiver which 'decodes' (reconstructs) the message from the signal; the destination where the message arrives. The sixth element, noise is a dysfunctional factor: any interference with the message going along the channel (such 'asstatic' on the telephone or radio) which may lead to the signal received being different from that sent. For the telephone, the channel is a wire, the signal is the electrical current in it and the transmitter and receiver are the telephone handsets. Noise would include crackling from the wire. In conversation, my mouth is the transmitter, the signal is the sound waves and your ear is the receiver. Although, in Shannon and Weaver's Model a speaker and a listener would strictly be the source and the destination rather than the transmitter and the receiver in discussions of the model the participants are commonly humanized as the sender and the receiver.

The approach to simulating message transmission and corresponding threats considered in this study differ from the approaches mentioned above.

CONCLUSION

The automation approach to formalizing the MTL IS Model building can be considered correct and theoretically reasonable. Practical implementation of the

synthesized automation is possible with the use of any known software such as using UML. Conditions and ways of the introduction of corresponding expert estimates are completely defined by fuzzy conditions of adequacy and completeness preservation which demand the separate consideration.

REFERENCES

Demidov, V., N. Silnikov and A. Shaitanov, 2000. Technique of Communication of Department of Internal Affairs. Saint Petersburg State University, Saint Petersburg, Russia, Pages: 95.

Goncharov, M., 2012. Model and method for analyzing risks of computer systems information security based on hybrid fuzzy models. Neurocomputers Dev. Appl., 5: 9-15.

Grigoryev, V. and O. Lagutenko, 2005. Networks and Wireless Access Systems. Eco-Trends, Moscow, Russian, Pages: 384.

Horev, A., 1998. Protection of Information from Leaks by Technical Channels. Gostehkomissija Rossii, Moscow, Russia, Pages: 320.

Kam, T., T. Villa, R. Brayton and A. Sangiovanni-Vincentelli, 1997. Synthesis of Finite State Machines: Functional Optimization. Kluwer Academic Publishers, Boston, Massachusetts, Pages: 282.

Lagutin, V., 1997. Leakage and Information Protection in Telephone Channels. Publisher Energoatomizdat, Moscow, Russian, Pages: 298.

Lukatsky, A., 2005. Security of wireless networks. Technol. Means Commun., 1: 45-67.

Lukatsky, A., 2006. Preventing Network Attacks: Technologies and Solutions. Ekspress-Elektronika, Moscow, Russia, Pages: 78.

Martsenyuk, M., 2014. Reduction of the final fuzzy automation to the fuzzy combinational scheme with the memory block. Sci. Tech. Bull., Vol. 6.

Mordeson, J.N. and S.M. Davender, 2002. Fuzzy Automata and Languages: Theory and Applications. CRC Press, Boca Raton, Florida, USA., Pages: 576.

Olifer, V. and N. Olifer, 2006. Computer Networks: Principles, Technologies and Protocols for Network Design. John Wiley & Sons, Hoboken, New Jersey, USA. is BN: 9780470869826, Pages: 973.

Pollin, D. and M. Maxim, 2014. Security of Wireless Networks. Dmk Press, Moscow, Russia, Pages: 288.

Vishnevsky, V. and A. Lyakhov, 2005. Broadband Wireless Data Transmission Networks. Eco-Trends, Moscow, Russian, Pages: 592.