Scientific Research Publishing

Int. J. Communications, Network and System Sciences, 2019, 12, 199-208
https://www.scirp.org/journal/ijcns
ISSN Online: 1913-3723
ISSN Print: 1913-3715

Development of the Software Application with Graphical User Interface for One Model Cyber Security

Ramaz R. Shamugia

Ilia Vekua Sokhumi Institute of Physics and Technology, Sokhumi State University, Tbilisi, Georgia
Email: rmz.shamugia@gmail.com

How to cite this paper: Shamugia, R.R. (2019) Development of the Software Application with Graphical User Interface for One Model Cyber Security. *Int. J. Communications, Network and System Sciences*, **12**, 199-208.
https://doi.org/10.4236/ijcns.2019.1212014

Received: November 12, 2019
Accepted: December 10, 2019
Published: December 13, 2019

Abstract

The article is dedicated to the development of software application with graphical user interface for analyzing of the operation of Integrated System of Data Defense from cyber-threats (ISDD) which includes subsystems of detection and elimination of vulnerabilities existing in the system, as well as Requests of Unauthorized Access (RUA). In the subsystems of eliminations of vulnerabilities and queues of unauthorized access considered as multichannel queueing systems with corresponding servers and queues, at random times there come requests to fix threats detected by the system. It is supposed that flows of requests demanding to eliminate threats coming to the mentioned subsystems of queueing systems are described with the Poisson distribution of probabilities, but processes of their elimination obey exponential law. For the system described above, there has been developed software realization of graphical interface which allows easily to change input parameters and observe graphical reflection of changes of the output indicators of the system.

Keywords

Cyber Security, Data Security, Cyber Threats, Cyber-Vulnerability, Modelling of Cyber-Threats, Cyber Space, Data Protection, Queueing Systems

1. Introduction

On the current level of development of information and communication technologies (ICT), struggling for information ownership, reaching and maintaining information dominance take prominent place in geopolitical competition of countries. States developing potential in the information space get number of competitive advantages and are able to use it as a factor of power to the disad-

vantage of the rest of participants of international processes.

In this connection, the use of Information and communication technologies (ICT) for the military and political purposes by the states is becoming especially relevant. Such characteristics of information space as being cross-border, openness, availability and anonymousness have brought about information infrastructure attractive from the point of view possibility to fulfill illegal actions with criminal and terrorist goals. Counteracting these types of threats is becoming an important part of array of actions to provide information security on the national, as well as on the global level.

Cyberspace consists of different computer systems connected to the net and integrated telecommunication systems. It has become one of distinguishing features of modern society providing with and enlarging fast communication, operation of distributed systems of command and control, storing and passing huge data files and operation of highly distributed systems. Today, all of these things are taken for granted by the society. It has become necessary for business, everyday life and service activities.

Such ubiquitousness and addiction of the cyberspace can be observed even in the military area where communication, control and administration, elements of intelligence and delivering precision guided blows rely on a large number of "cyber systems" and connected with their communication systems. Ubiquitousness of these interconnected systems causes some kind of dependence and vulnerability of separate sectors of industry and governments that are difficult to predict, weaken, prevent and control.

Some countries consider this vulnerability and dependence as new problems in the domains of national security and national defense and put forward a task for appropriate structures of their security forces to react, while other counties are setting up absolutely new organizations whose purpose is to manage and coordinate national strategies in the domain of cybersecurity. Cybersecurity has become an important interdisciplinary issue that demands the reaction of individuals, private organizations, nongovernmental organizations, "the whole government" and a number of international agencies and organs [1] [2] [3].

In accordance with abovementioned, one of the most demanded and future oriented trends of research in the domain of providing cybersecurity is development of models of cyber space and main factors influencing its operation. Among the number of different approaches and trends used for modelling cyberspace, significant role is given to creating mathematical and imitation models that enable to get numerical data of the degree of information security (degree of threat of information security, analysis of information security risks, estimation of effectiveness of protection measures etc.).

In the following sections of the article are given: statement of the research problem, justification of the choice of the analytical model and a software model with a graphical user interface, developed using the Graphical User Interface Development Environment (GUIDE), that is part of Matlab/Simulink.

2. Statement of the Problem

This article offers a user model adapted to the scopes of providing cyber security and completed with graphical interface abilities of user options, the model which is a version of complex technical system discussed in the article [4]. The target of research in this article is a complex intelligent computer system of information security (CSIS) that defends from factors destabilizing operation of information system (IS), (the factors like occurrence of vulnerabilities and requests for unauthorized access (UA)), the system comprises subsystems of detection and elimination of vulnerabilities, as well as requests of UA in order to prevent results of cyber threats.

The subsystem of detection of vulnerabilities at random time, distributed according to Exponential law, carry out the scanning of information system in order to discover abovementioned destabilizing factors, in case they are discovered, they are passed to corresponding subsystem of elimination, that happens at random time too, distributed according to exponential law. For modelling the system that has been described, approaches of queuing theory is used, the theory of Markov processes, in particular [5]-[11].

It is supposed that complex security system (CSS) shown in **Figure 1**, as QS consists of two types of homogenous means of defense, total number of which is $m = m1 + m2$, where $m1$ is the number of homogenous means of defense supposed for detecting and elimination of vulnerabilities of functional type (FP -functional protection), and $m2$ is for detecting and elimination vulnerabilities of structural type (S3—structural protection)

It is expected that the flow of arrivals coming from the subsystem of detecting vulnerabilities on the subsystem is Poisson and its total intensity equals to $O = O1 + O2$, where $O1$ is intensity of discovery of functional vulnerabilities, and $O2$- is the intensity of detecting structural vulnerabilities.

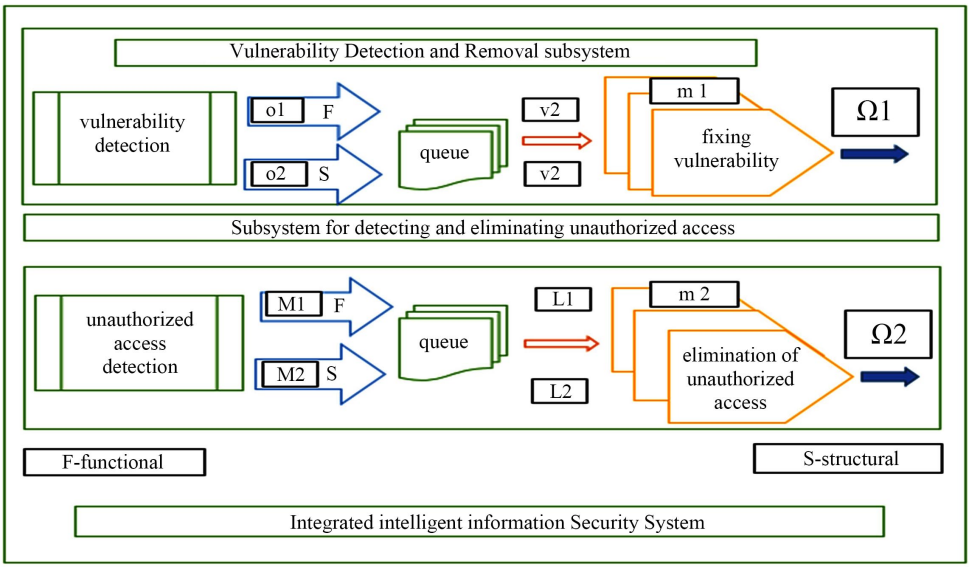

Figure 1. Functional scheme of ISDD.

Elimination of vulnerabilities coming into corresponding subsystem happens according to the exponential law with total intensity $V = V1 + V2$, where $V1$—intensity of removal of functional vulnerabilities, but $V2$—intensity of removal of structural vulnerabilities. In the above-described system there comes Poisson probable flow of requests for unauthorized access with collective intensity $M = M1 - M2$, where $M1$ and $M2$ are intensities of flow of requests for unauthorized access with the use of vulnerabilities existing correspondingly in the functional and structural parts of computer system of information security (CSIS).

Security system fulfills neutralizing attempts of unauthorized access discovered while appropriate scanning. Neutralizing time is distributed according to exponential law with total intensity $L = L1 + L2$, where $L1$—neutralization intensity of UA attempts into the functional part of CSDD, and $L2$ is neutralization intensity of attempts UA into the structural part of ISDD.

It should be taken into consideration that in the system is provided/is able to react to the existence of queues for requests coming from appropriate subsystems ISDD at the moment when equipment eliminating threats is busy with eliminating previously received requests. The total number of requests, being simultaneously in the system, is limited., and it equals to $K = K1 + K2 + K0$, where $K1$ is the number of requests on the servers for removing vulnerabilities, $K2$ is the number of requests on the servers for preventing attempts of unauthorized access and $K0$ is a total number of both type of requests in the appropriate queues.

For description of the states of the system there are introduced probability functions $P_i(t)$, which characterize the transition from one state into another, being under influence of the different flows happening in the system (flows of detection and elimination of threats), and are determined as product probability of the i-state from which the transition to the corresponding intensity takes place [12]-[19].

The use of Kolmogorov's mnemonic rule of setting up equations in the abovementioned system enables to write down the system of differential equations determining probabilities of transition between its states in the form of:

$$\frac{\mathrm{d}P_i(t)}{\mathrm{d}t} = aP_i(t) + bP_{i-1}(t) + cP_{i+1}(t), \tag{1}$$

where $P_i(t) = P_i(m1, m2; K1, K2, K0; L1, L2; M1, M2; O1, O2; V1, V2; t)$ - event probability whereby/wherein at the moment t in the system in case of fixed values of parameters $m1, m2; K1, K2, K0; L1, L2; M1, M2; O1, O2; V1, V2$ there are i-requests, but coefficient in case of unknown functions correspond to tridiagonal matrix with values being estimated by the following formulae:

$$\begin{aligned} a &= i * L * \left(1 - \left(M - O - V\right)\right); \\ b &= -\left(a + \left(i - 1\right) * \left(1 - \left(M - O - V\right)\right)\right); \\ c &= i * M * \left(1 - \left(M - O - V\right)\right); \end{aligned} \tag{2}$$

For solving this system of equations with the help of software environment

Matlab, the function *ODE*23 was used which is supposed for numerical integration of systems of homogenous differential equations (HDE). It is applicable for both: solving simple differential equations and modelling of complex dynamic systems.

As it is known any system of nonlinear homogenous differential equations (HDE) can be represented as the system of differential equations of the first order in the explicit form of Cauchy: $\mathrm{d}x/\mathrm{d}t = f(x,t)$, where x is state vector, t is time, f- nonlinear vector-function from the variables x, t.

Functions [t, X] = ode23('<function name>', t0, tf, x0, tol, trace) integrates the systems HDE using the Runge-Kutta method of the second and forth orders that have the parameters: **inputs parameters:** <function name>, that is the name of M-file in which the right parts of system HDE are being calculated; t0 is the initial value of time, t final is the final value of time; x0—the vector of initial states, tol—given precision (by default to ode23, tol = 1.e-3); trace—a flag regulating the output of intermediary results (by default equals to zero that suppresses the output of intermediary results); **outputs parameters**: t—a current time, X—two-dimensional array where every column corresponds to one variable [12]-[18].

3. The Development of Simulation Program

function varargout = MMmK_19_06_2019(varargin)

function pushbutton1_Callback(hObject, eventdata, handles)

% hObject handle to pushbutton1 (see GCBO)

% eventdata reserved - to be defined in a future version of MATLAB

% handles structure with handles and user data (see GUIDATA)

m1 = str2double(get(handles.m1,'string')); % The number of homogeneous means of protection designed to detect and eliminate functional type vulnerabilities (FZ-functional protection);

m2 = str2double(get(handles.m2,'string')); % The number of homogeneous means of protection designed to detect and eliminate structural type vulnerabilities (SZ - structural protection);

K0 = str2double(get(handles.K0,'string')); % The total number of requests of both types in the corresponding queues;

K1 = str2double(get(handles.K1,'string')); % The number of requests located on the servers to eliminate vulnerabilities;

K2 = str2double(get(handles.K2,'string')); % The number of requests on servers to prevent unauthorized access attempts;

L1 = str2double(get(handles.L1,'string')); % The intensity of the neutralization of attempts to tamper with the functional part of IISS (Integrated information security system);

L2 = str2double(get(handles.L2,'string')); % The intensity of the neutralization of attempts to unauthorized access to the structural part of the IISS;

M1 = str2double(get(handles.M1,'string')); % The intensity of the flow of

```
applications for unauthorized access using vulnerabilities existing in the functional parts of the IISS;
M2 = str2double(get(handles.M2,'string')); % The intensity of the flow of applications for unauthorized access using vulnerabilities existing in the structural parts of the IISS;
O1 = str2double(get(handles.O1,'string')); % The intensity of detection of functional vulnerabilities;
O2 = str2double(get(handles.O2,'string')); % The intensity of detection of structural vulnerabilities;
V1 = str2double(get(handles.V1,'string')); % The intensity of functional vulnerability removal;
V2 = str2double(get(handles.V2,'string')); % The intensity of functional vulnerability removal;
global A
syms m n k i a b c A L N
L=L1+L2; % The total intensity of the exponential distribution of time to neutralize threats;
set(handles.L,'string',L);
M=M1+M2; % The total intensity of the Poisson flow of unauthorized access;
set(handles.M,'string',M);
O=O1+O2; % The total intensity of the request flow from the vulnerability detection subsystem to the vulnerability removal subsystem;
set(handles.O,'string',O);
V=V1+V2; % The total intensity of the exponential vulnerability elimination flow;
set(handles.V,'string',V);
K=K1+K2+K0; % The total number of requests simultaneously located in the system;
set(handles.K,'string',K);
for i=1:K
    a=i*L;
    b=-(a+(i-1)*(M-O-V));
    c=i*M;
    A=full(gallery('tridiag',K,a,b,c));
    set(handles.a,'string',a);
    set(handles.b,'string',b);
    set(handles.c,'string',c);
%%Numerical solution of differential equations
    P0 = [1;zeros(length(A)-1,1)];
T = [0,0.01];
[t,P] = ode23(@cmo, T, P0);
end
%% Constructing of diagrams of states probabilities
```

```
line(t,P,'linew',2)
line(t,P(:,K),'linew',2, 'color','r') %% P(K-1)
grid on
N = length(A)-1;
arr = [0:N]';
str = num2str(arr);
legend(strcat('\bf\itP\rm\bf_', str, '(\itt\rm\bf)'));
title(sprintf('%s Probabilities of system states M/M/%d/%d',
'\bf\fontsize{12}',i, K));
xlabel('\bf\it\fontsize{12} Model Time ')
ylabel('\bf\fontsize{12}\itProbabilities of states P\rm\bf(\itt\rm\bf)');
set(gca,'fontweight','bold','fontsize',10);
fprintf('\n Stationary probabilities:\n');
for J = 1 : length(A);
fprintf('\tP%d = %f\n', J-1, P(end,J));
fprintf('Probabilities P = %f\n', P(end,J));
QQ(J)= P(end,J); set(handles.QQ,'string',QQ); P0=P(end,1);
set(handles.P0,'string',P0);
P1=P(end,2); set(handles.P1,'string',P1); P2=P(end,3);
set(handles.P2,'string',P2); P3=P(end,4);
set(handles.P3,'string',P3);P4=P(end,5);set(handles.P4,'string',P4);P5=P(end,6
);
set(handles.P5,'string',P5); P6=P(end,7); set(handles.P6,'string',P6);
P7=P(end,8);
set(handles.P7,'string',P7); P8=P(end,9); set(handles.P8,'string',P8);
P9=P(end,10);
set(handles.P9,'string',P9); P10=P(end,11); set(handles.P10,'string',P10);
P11=P(end,12);
set(handles.P11,'string',P11);
end
Pnot = P(end,end); set(handles.Pnot,'string',Pnot); Q = 1 - Pnot;
set(handles.Q,'string',Q);
Ab = L*Q; set(handles.Ab,'string',Ab); Pq = sum(P(end, i+1:end));
set(handles.Pq,'string',Pq);
Ps = sum(P(end, i:end)); set(handles.Ps,'string',Ps); Ns =
[0:length(A)-1]*P(end,:)';
set(handles.Ns,'string',Ns); Nq = [0:(K-i)]*P(end,i:K)';
set(handles.Nq,'string',Nq);
Ts=Ns/L; set(handles.Ts,'string',Ts); Tq=Nq/L; set(handles.Tq,'string',Tq);
function f = cmo(t,P)
%% Functions describing the right-hand sides of differential equations
global A
f = A*P;
%Results of program execution
```

%Stationary probabilities

%The diagram of states probabilities of the system

The figures below (Figures 2-4) show the appearance of the graphical user interface corresponding to various values of the input parameters.

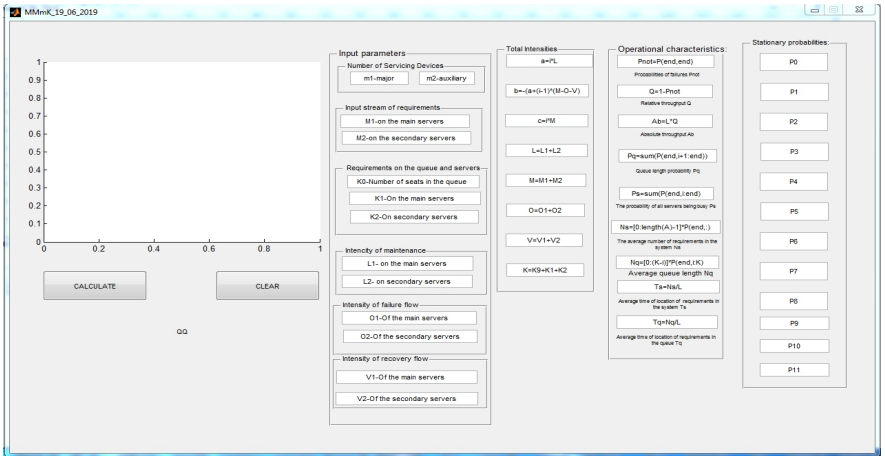

Figure 2. Interface of Graphical Application of s model before parameters input.

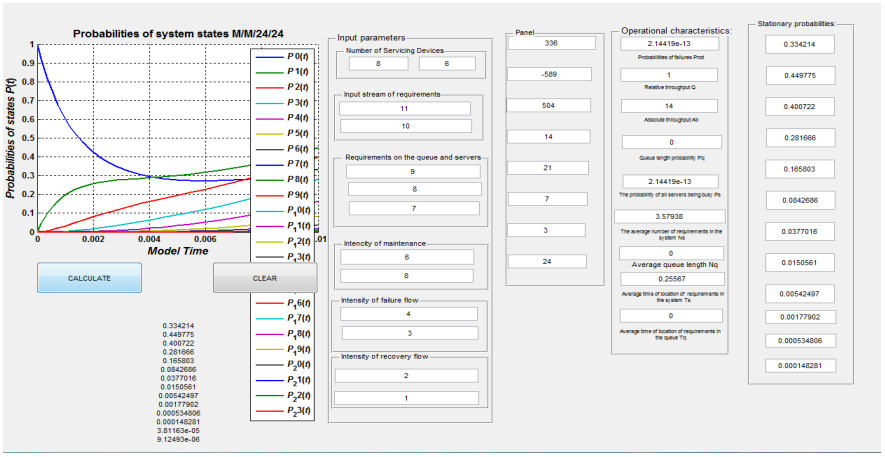

Figure 3. Interface of graphical application of model after parameters input, 1st version.

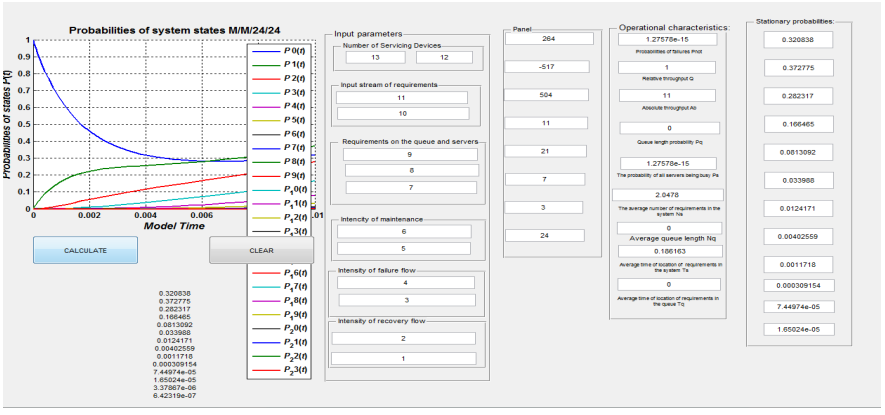

Figure 4. Interface of Graphical Application of model after parameters input. 2nd version.

4. Conclusions

The article presents with the software development of application with graphical interface for Integrated Security System from cyber-threats that consists of detection and elimination subsystems for existing in the system vulnerabilities as well as for unauthorized access requests (UA).

In the subsystems of vulnerability elimination and requests for unauthorized access, considered as multichannel queueing systems with corresponding queues, at random time, there come requests for elimination of threats detected by the system.

It is supposed that the request flow coming into the mentioned queueing system for elimination of threats is Poisson, but the flow of their elimination is exponential. The graphical interface developed in the research enables to watch the graphical reflection of changes of output indicators depending on the change of input parameters of the system.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

[1] Bezkorovainy, M. and Tatuzov, A. (2014) Cybersecurity—Approaches to the Definition. *Voprosi Kiberbezopasnosti*, No. 1.

[2] Starovojtov, A.V. (2011) Cybersecurity as an Actual Modern Problem. *Informatization and Communication*, **6**, 4-7.

[3] Bezkorovajnyj, M.M., Losev, S.A. and Tatuzov, A.L. (2011) Cybersecurity in the Modern World: Terms and Content. *Informatization and Communication*, **6**, 27-32.

[4] Shamugia, R.R. (2018) Development and Investigation of the Program Model of Multichannel Queueing System with Unreliable Recoverable Servers in Matlab Environment. *International Journal of Communications, Network and System Sciences*, **11**, 229-237. https://doi.org/10.4236/ijcns.2018.1111014

[5] Saati, T.L. (1965) Elements of Queuing Theory and Its Application. Sovetskoe Radio, Moscow, 510.

[6] Cherkesov, G.N. (1974) Dependability of Technical Systems with Time Redundancy. Sovetskoe Radio, Moscow, 296.

[7] Gnedenko, B.V. and Kovalenko, I.N. (2012) Introduction to Queuing Theory. LKT, 400.

[8] Feller, W. (1971) An Introduction to Probability Theory and Its Applications. Vol. 2, John Willey and Sons, New York, 766.

[9] Ramaswami, V. (1985) Algorithms for the Multi-Server Queue with Phase-Type Service. *Communications in Statistics. Stochastic Models*, **1**, 393-417. https://doi.org/10.1080/15326348508807020

[10] Kim, C.S. (2013) Queueing System MMAP/PH/N/N+R with Impatient Heterogeneous Customers as a Model of Call Center. *Applied Mathematical Modelling*, **37**, 958-976.

[11] Klimenok, V.I. (2006) Multi-Dimensional Asymptotically Quasi-Toeplitz Markov Chains and Their Application in Queueing Theory. *Queueing Systems*, **54**, 245-259. https://doi.org/10.1007/s11134-006-0300-z

[12] Dudina, O. (2013) Retrial Queueing System with Markovian Arrival Flow and Phase Type Service Time Distribution. *Computers and Industrial Engineering*, **66**, 360-373. https://doi.org/10.1016/j.cie.2013.06.020

[13] Shubinski, I.B. (2012) Strukturnaja nadejnost informacionnhx system-M. Jurnal Nadejnost, 216 str.

[14] Shubinski, I.B. (2012) Funkcionalnaja nadejnost informacionnhx system. Metodi analiza-M. Jurnal Nadejnost, 296 str.il.

[15] Shubinski, I.B. (2016) Nadejnie otkazoustoichivie informacionnie sistemi. Metodi sinteza-M. Jurnal Nadejnost, 546 str.il.

[16] Shamugia, R.R. (2014) On One Model of Complex Technical Queuing System with Unreliable Devices and with Time Redundancy. *International Journal of Communications, Network and System Sciences*, **7**, 257-264. https://doi.org/10.4236/ijcns.2014.78028

[17] Shamugia, R.R. (2014) On One Model of Multichannel Queuing System with Unreliable Repairable Servers and Input Memory. *International Journal of Communications, Network and System Sciences*, **7**, 279-285. https://doi.org/10.4236/ijcns.2014.78030

[18] Shamugia, R.R. (2015) On One Analytical Model of a Probability Estimation of Quality and Efficiency of Functioning of Complex Technical Queuing Systems. *International Journal of Communications, Network and System Sciences*, **8**, 295-303. https://doi.org/10.4236/ijcns.2015.88029

[19] Shamugia, R.R. (2016) Probabilistic Model of Technical Queuing Systems with Subsystems for Detection and Recovery of Failures. *International Journal of Communications, Network and System Sciences*, **9**, 305-310. https://doi.org/10.4236/ijcns.2016.98027