[Egyptian Informatics Journal 24 (2023) 61–69](https://doi.org/10.1016/j.eij.2022.11.002)

Contents lists available at [ScienceDirect](http://www.sciencedirect.com/science/journal/11108665)

Egyptian Informatics Journal

journal homepage: [www.sciencedirect.com](http://www.sciencedirect.com/)

[](http://crossmark.crossref.org/dialog/?doi=10.1016/j.eij.2022.11.002&domain=pdf)A computationally efficient method for assessing the impact of an active viral cyber threat on a high-availability cluster

Ahmed Altameem [a](#_bookmark0), Mohammed Al-Ma’aitah [a](#_bookmark0), Viacheslav Kovtun [b](#_bookmark1),[⇑](#_bookmark2), Torki Altameem [a](#_bookmark0)

a *Computer Science Department, CC, King Saud University, 11451, 95, Riyadh 11362, Saudi Arabia*

b *Computer Control Systems Department, IITA, Vinnytsia National Technical University, Khmelnitske Shose, 95, Vinnytsia 21000, Ukraine*

# a r t i c l e i n f o

*Article history:*

Received 20 July 2022

Revised 14 October 2022

Accepted 30 November 2022

Available online 10 December 2022

*Keywords:* Information security Viral cyber threat

High availability cluster Markov model Quantitative metric Computational efficiency

# a b s t r a c t

The field of computer science, like its sub-field of cyber threat modelling, is rapidly evolving. The prereq- uisites for key changes can be summarized as follows: cyber threats are evolving; there are leaks of spe- cial services tools; agile development methodology is being introduced everywhere; the boundaries of the object of protection are blurred; the scope of application of artificial intelligence is expanding; poten- tially vulnerable API integrations are increasingly being used. These factors lead to the fact that the pro- cesses of analysis of cyber threats, analysis of protective measures, generalization of data, and development of protective tools should now be considered continuous, not discrete. At the same time, the cost of cybersecurity increases like an avalanche in an attempt to avoid reputational and information losses. The only way to avoid this tendency is to apply a rational, scientific, accurate method of cognition to these processes. Thus, the creation of mathematical models of processes in the field of cybersecurity is now more relevant than ever. The article is devoted to the investigation of the process of the influence of an active viral cyber threat on a high-availability cluster in the paradigm of the provisions of the theory of Markov processes, graph theory and the theory of mathematical analysis. The main contribution of the research is a formalized computationally efficient method of approximate estimation of the average number of affected elements of the target high-availability cluster under the influence of an active viral cyber threat. Also, a criterion that allows estimating the trend of the quantitative parameter of the metric of the model of the studied process at medium and long time intervals is proposed. To obtain the declared scientific result, the authors: - formulated a Markov model of the process of the influence of an active viral cyber threat on a high availability cluster; - substantiated a compact metric for accurate assessment of the average number of cluster elements affected by an active viral cyber threat at any time; - formu- lated a computationally efficient method of approximate estimation of the parameter of the mentioned metric for the model of the target studied process; - proposed a criterion that allows researchers to eval- uate the trend of the parameter of the mentioned metric for the model of the target researched process at medium and long intervals of time. The adequacy of the formulated method has been proven empirically.

© 2023 THE AUTHORS. Published by Elsevier BV on behalf of Faculty of Computers and Artificial Intel-

ligence, Cairo University. This is an open access article under the CC BY-NC-ND license ([http://creative-](http://creativecommons.org/licenses/by-nc-nd/4.0/)

[commons.org/licenses/by-nc-nd/4.0/](http://creativecommons.org/licenses/by-nc-nd/4.0/)).

1. Introduction

\* Corresponding author.

*E-mail addresses:* [ahaltameem@ksu.edu.sa](mailto:ahaltameem@ksu.edu.sa) (A. Altameem), [malmaitah@ksu.edu.](mailto:malmaitah@ksu.edu.sa) [sa](mailto:malmaitah@ksu.edu.sa) (M. Al-Ma’aitah), [Kovtun\_v\_v@vntu.edu.ua](mailto:Kovtun_v_v@vntu.edu.ua) (V. Kovtun), [altameem@ksu.edu.sa](mailto:altameem@ksu.edu.sa) (T. Altameem).

Peer review under responsibility of Faculty of Computers and Information, Cairo University.

**Production and hosting by Elsevier**

Modern machine learning methods already make it possible to create evolving viral cyber threats that are invulnerable to typical protective mechanisms of information systems. Undoubtedly, soon the toolkit of attackers will allow the automatic creation of new viral cyber threats, hardened by pseudo-evolutionary selection to the specified properties of the target information environment. Such viral cyber threats will have developed heuristic properties and swarm organization. Creating models of the spread of such cyber threats to investigate their behavior and develop counter- measures is an urgent scientific and applied task.

The classical and still relevant conceptual basis for describing the dynamic process of the spread of viral cyber threats is the *SI* and *SIR*

<https://doi.org/10.1016/j.eij.2022.11.002>

1110-8665/© 2023 THE AUTHORS. Published by Elsevier BV on behalf of Faculty of Computers and Artificial Intelligence, Cairo University. This is an open access article under the CC BY-NC-ND license (<http://creativecommons.org/licenses/by-nc-nd/4.0/>).

models [[1–5]](#_bookmark22). When creating the *SI* model, it is assumed that an arbitrary computer in the target finite computer network can be in one of two states – vulnerable (*S*) and infected (*I*). A virus cyber- threat propagates through a network from infected to randomly selected vulnerable computers at a constant average rate. In the *SIR* model, an invulnerable state (*R*) is added to the two states already mentioned in the description of the *SI* model, in which an arbitrary computer of the network can be, to which the target com- puter can go only from the state I (overcoming a cyber infection). Accordingly, the SIR model additionally takes into account the rate of immunization of computers (nodes) in the target network. In the SIR model (to the already mentioned two states in the description of the *SI* model, in which an arbitrary computer of the network can be), an invulnerable state (*R*) is added, to which the target computer can transit only from the state *I* (overcoming a cyber infection). Accordingly, the *SIR* model additionally takes into account the rate of immunization of computers (nodes) in the target network.

Classically, *SI* and *SIR* models are formalized based on kinetic dif- ferential equations, but there are also original approaches, for exam- ple, in works [[6–9]](#_bookmark23), the differential model of the hydrodynamic process became the basis. The usual ‘‘differential” approach is based on the assumption that the number of infected nodes in a computer network is a continuous function of time. A typical *SI*- or *SIR*-like model, built based on differential equations, is a system of equations of this type (mostly nonlinear differential equations of the first order), where each equation characterizes a certain class of node of the stud- ied computer network and describes the permissible transitions between states and material balance (a set of controlled variables and free members). The coefficients for controlled variables in such equations characterize the settings of protective mechanisms. The solution of the corresponding system of differential equations is usu- ally interpreted in the context of determining recommendations for the intensity of renewal of protective mechanisms.

Without changing conceptually, *SI* and *SIR* models are develop- ing methodologically [[10–12]](#_bookmark24). For example, in the work [[10]](#_bookmark24), the concept of a computer network node is revealed as a set of two ele- ments (‘‘server” and ‘‘client”), and the speed of the spread of cyber infection is considered to be different. In this model, each com- puter is also characterized by the probability of re-infection, which, according to the authors, allows for taking into account the poly- morphic nature of modern viral cyber threats. This direction of development of *SI* and *SIR* models continues. For example, in works [[11,12]](#_bookmark25), for computer network nodes of the ‘‘server” class, the set of states includes vulnerable (*S*), infected (*I*), and immune (*A*) states, and for computer network nodes of the ‘‘client” class, the set of states includes susceptible (*S*), infected (*I*), non-susceptible (*R*) and immune (*A*) states. The mentioned works differ in their inter- pretation of the concept of ‘‘immune state” as, for example, ‘‘tem- porarily invulnerable”, ‘‘highly invulnerable”, etc.

The expansion of the nomenclature of classes of nodes and states is accompanied by a symmetrical expansion of the set of characteristic parameters that allow describing the corresponding models. For exam- ple, in well-known models [[13–16]](#_bookmark26) parameters such as the epidemio- logical threshold, waiting time for infection, replication coefficient, probabilities of infection and immunization, node invulnerability time, etc. are entered. However, the typical statement of the research prob- lem in such models is limited to the search for equilibrium points of the system of differential equations and the analysis of the asymptotic behavior of the solutions found, which are associated with the corre- sponding modes of cyber infection progress.

* 1. *A critical review of current models of the development of cyber infections*

There are known attempts to take into account the heteroge- neous architecture of modern computer networks within the con-

ceptual limits of *SI* and *SIR* models (for example, the *NSIDR* model [[17–19]](#_bookmark29)). These architectural properties are taken into account by multiplying the terms of certain differential equations in the model (system of equations) by empirically determined constant coeffi- cients. This trend also includes models aimed at describing the mechanism of controlling the number of inter-computer connec- tions in the target network in conditions of an active viral cyber threat [[20–22]](#_bookmark30). However, the mathematical apparatus of differen- tial equations do not provide researchers with sufficient freedom for an adequate description of such nuances. It was this circum- stance that led to the appearance of a wide range of *SI* and *SIR* mod- els implemented in the theoretical basis of graph theory [[12,20,23]](#_bookmark27). Undoubtedly, such models perfectly reproduce the topology of the target computer networks but lose to ‘‘differential” models in the nomenclature of effects that can be simulated. However, the situ- ation changes when combining the capabilities of graph theory with machine learning methods [[24–26]](#_bookmark31). For example, in works [[25,26]](#_bookmark31), a computer network is modelled by a probability graph, the vertices of which are described by variables that regulate the probabilities of the states of network nodes, and the edges deter- mine the interaction between the variables of the model. The influ- ence of a viral cyber threat in such a model is described as a cellular automaton, in the form of a finite set of rules.

There are also known works where the progress of the influence of a viral cyber threat is described by the method of comparisons [[12,27,28]](#_bookmark27). For example, the analysis of such influence is carried out simultaneously by the methods of autoregression and Fourier analy- sis. These methods make it possible to predict the trend of the progress of the cyber infection, and the use of different bases for creating a regression model is aimed at increasing the accuracy of the forecast (due to the increase in the computational complexity of the analysis). If a computer network focused on a critical use is investigated, then models that take into account the mechanism of the topology of blocking nodes of a conglomerate of computer networks in the event of the registration of a viral cyberthreat become relevant. A representative of the models that describe the process of function- ing of such a mechanism is a Cayley tree structure with a random number of connections [[14,15]](#_bookmark28). This mathematical apparatus allows researchers to calculate the probability of infection of speci- fic nodes depending on their distance from the source of cyber infection in the topology of a heterogeneous network, taking into account its scale. Such opportunities are provided by the authors of the works [[20,23,29]](#_bookmark30) using the large-scale graph technology, which allows for taking into account the processes of hierarchical growth of the network structure. A specific parameter that should be determined when creating such models is the percolation threshold, which is understood as the proportion of blocked nodes at which the target computer network as a whole is unable to implement its functional purpose. When defining this parameter (functional purpose), the classes to which blocked nodes or net-

work sectors belong should be taken into account.

Combining the possibility of taking into account the topology and characteristics of the investigated computer network with a mathematically justified and relatively uncomplicated background allows the mathematical apparatus of Markov chains [[11,12,20,30,31]](#_bookmark25). There are well-known models for describing the impact of viral cyber threats based on stochastic models of interac- tive Markov chains, in which the state of computer network nodes in each subsequent period does not depend (depends) on the state of a specific node and nodes connected to it in the current period. Naturally, we are talking about Markov and semi-Markov chains, which can be studied both in discrete (most often) and continuous time. It is no secret that the assumption of the continuity of the process of the spread of a viral cyberthreat over time, which is the cornerstone of the models of the development of cyber infec- tion formalized on a differential basis, does not correspond to real-

ity (especially in the short periods). This fact is taken into account in the paradigm of discrete Markov chains ‘‘by default”. However, Markov models of the process of the spread of a viral cyberthreat have a characteristic drawback, which consists of the rapid non- linear growth of the computational complexity of the process of calculating the required parameters with the growth of the scale of the investigated computer network. This circumstance determi- nes the search for a method of simplifying this computational pro- cess while maintaining the adequacy of the output result.

Taking into account the strengths and weaknesses of the men- tioned analogues, we will formulate the necessary attributes of sci- entific research.

The *object* of the research is the process of the influence of an

active viral cyber threat on a high-availability cluster.

The *subject* of the research is the provisions of the theory of Markov processes, the theory of graphs, the theory of mathemati- cal analysis, and the theory of probability and mathematical statistics.

The *aim* of the research is to formalize a computationally effi-

cient method for estimating the state of the model of the studied process at medium and long intervals of time.

of a viral cyber threat. At an arbitrary discrete moment *t* P 0, each element of the cluster can be either in a potentially vulnerable state to a viral cyberthreat *v*, or in a state affected by a viral cyber-

threat *a*. The state of all cluster elements at an arbitrary moment in

time is defined as *v*(*t*) + *a*(*t*) = *n*.

Let’s assume that during a time cycle, an arbitrary element of the cluster can freely transition into one of two permissible states:*v* → *a*,*a* → *v*. The quantitative phenomenon of such a transi-

tion can be characterized by such parameters as:

* the probability of transmission of a viral cyberthreat from an affected element to a potentially vulnerable one:*pa*+;
* the probability of transition of the affected element to a poten-

tially vulnerable state (*a* → *v*):*pav* ;

* the probability of a potentially vulnerable element transitioning

into an affected state (*v* → *a*):*pva* ;

* the connectivity of the cluster graph. The parameter *c* relates

the value of the number of vertices *n* in the studied graph to

— —

its average degree *k* by the ratio *c* = *k* /*n* (as *c* = 0 there is no

informational communication between the cluster elements, and *c* = 1 the cluster graph is fully connected).

The *objectives* of the research are:

Note that the parameter *pva*

depends on the values of the

* strict mathematical formalization of the research object model;
* determination of quantitative metrics for evaluating an arbi- trary instance of the research object in the parametric space of the created mathematical model;
* formalization of a computationally efficient method of calculat- ing the selected metric for the model of an arbitrary instance of the research object;
* formalization of the criterion for approximate assessment of the

state of the model of the research object at medium and long

parameters *a*, *pav*, c:*pva* = *f* (*a*; *pav* ; *c*). It is important to investigate

the nature of this functional dependence.

For the sake of clarity, let’s generalize the parametric descrip- tion of the state in which an arbitrary element of the cluster is with the UML state diagram presented in [Fig. 1](#_bookmark6).

We will analytically describe the process of the influence of a viral cyberthreat on the elements of a high-availability cluster by a discrete Markov chain n, the states of which are determined by the number of affected elements of the cluster *a*, that is, the total

n o

intervals of time.

number of states is equal to *n*

+ 1:*a*

—

= 0; *n* .

The *main contribution* of the research is a formalized computa- tionally efficient method of approximate estimation of the average number of affected elements of the target high-availability cluster under the influence of an active viral cyber threat. Also, a criterion that allows estimating the trend of the quantitative parameter of the metric of the model of the studied process at medium and long time intervals is proposed.

The dynamics of the chain n(*t*) is determined by the transition probabilities *pa*;*a*' ∈ *P*. Based on the provisions of the theory of Mar- kov processes [[11]](#_bookmark25), we formulate expressions for calculating parameters *pa*;*a*' in the form of expression

min {*a*;*n*—*a*'}

P

*pa a* = *Ki pi v* (1 — *pav* )*a*—*k*×

; '

*i*=max {0;*a*—*a*'}

*a*

*a*

(1)

×*Ka*'—*a*+*ipa*'—*a*+*i*(1 — *p* )*n*—*i*—*a*' ;

*n*—*a va va*

The *highlights* of the research are:

where *Ki* Ξ *a*! is a binomial coefficient whose value is equal

*a i*!(*a*—*i*)!

* a Markov model of the process of the influence of an active viral cyber threat on a high-availability cluster (expressions [(1)](#_bookmark3), [(2)](#_bookmark4));
* a metric for accurate estimation of the average number of clus-

ter elements affected by an active viral cyberthreat at an arbi-

to the number of combinations from *a* to i.

Based on expression [(1)](#_bookmark3), we formulate the expression for calcu- lating the probability *pva*:

X *i* *i* *i a i*

*a*

trary moment in time (expression [(4)](#_bookmark7));

* a computationally efficient method of approximate estimation of the parameter of the mentioned metric for the model of the target object of research (expressions [(9)](#_bookmark12), [(10)](#_bookmark13));
* a criterion that allows us to evaluate the trend of the parameter of the mentioned metric for the model of the target researched process at medium and long intervals of time (expression [(13)](#_bookmark15)).

1. Models and methods
   1. *Setting up the research*

*pva* =

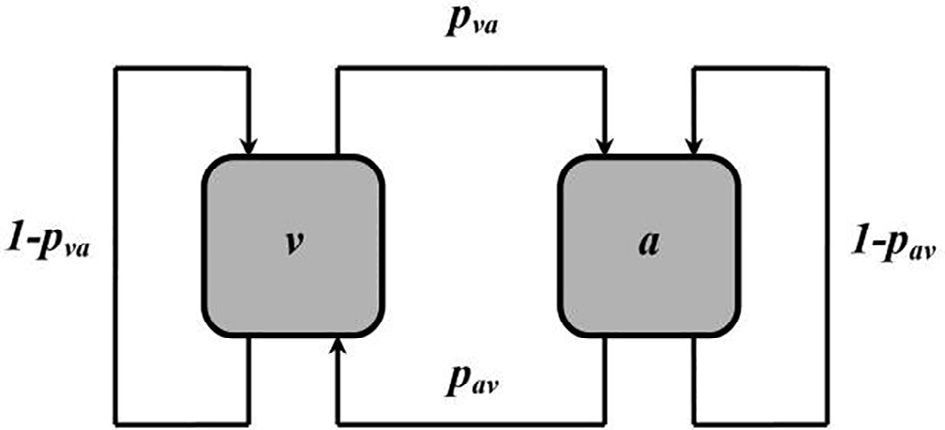
—

*Ka* 1 — 1 — *pa*+ *c* (1 — *c*)

*i*=0

(2)

Consider a connected directed graph with *n* vertices as an abstract model of a high-availability cluster architecture. The edges of the graph represent information communication channels between elements (computer servers) of the cluster. The vertices of the graph represent cluster elements that are potential targets

Fig. 1. UML state diagram of an arbitrary element of a high-availability cluster under the influence of a viral cyber threat.

If we expand the expression [(2)](#_bookmark4) into a Taylor series and discard all terms higher than the first order, we get the expression

Let’s rewrite expression [(5)](#_bookmark14) taking into account what was just obtained:

*pva*

= *pa*+

*ca*. This linear expression is an analogue of the classic

*p* = 1 — 1 — *cp*

*a* (6)

model of the progress of epidemics of viral cyber threats, proposed by Kefard and White [[32]](#_bookmark32). This circumstance indirectly confirms the adequacy of the theoretical postulates made.

A prerequisite for the quantitative characterization of the devel- opment of the researched process is the determination of all ele- ments of the matrix of transition probabilities

*va a*+

It follows from expression [(6)](#_bookmark9) that the parameter *pva* function- ally depends on the combination of parameters c and

*pa*+:*pva* = *f cpa*+ . Since the parameters c and *pa*+ enter the expres- sion [(1)](#_bookmark3) only transitively, through the parameter *pva* , we can nar-

row the set of input parameters of the model to three

*P* = *p*

*a*,*a*'

,*a*, *a*'

—

= 1, *n*, which are calculated according to expression

elements: g

= *cpa*+,

*pav* ,

*a*0}.

[(1)](#_bookmark3). In particular, considering the defined matrix P, the probability

of a state a at a time t can be calculated using the expression

It should also be noted that lim *pva* = lim 1 — (1 — g)*a* = 1 that

*p* (*t*) = X *p*

*n*

*a*

*a*'

(0)*p*(*t*)

*a*→∞

*a*→∞

*a*,*a*'

### (3)

is, the value of the parameter *pva* increases monotonically with the increase in the value of the parameter *a* (the number of affected

*a*' =0

max (*pva* ) = 1 — (1 — g)*a*.

where *pa*(0) is the probability of states of chain n at the initial moment *t* = 0:n(0); *p*(*t*) is an element of the matrix *Pt*, which is

*a*,*a*'

cluster elements). However, *a* 6 *n* therefore

Finally, if 0 < g < 1 we expand expression [(6)](#_bookmark9) into a Taylor ser- ies, we get:

the matrix P raised to the *t* th degree.

With a known number of affected elements of the cluster at the

*pva* = *a*g —

*a*(*a* — 1)

### 2

g2 +

*a*(*a* — 1)(*a* — 2)

g3 + ... (7)

moment *t* = 0 (parameter *a*0 = *a*(*t*)|*t*=0

= *a*(0)), the probability

### ! 3!

*pa* (0) is defined as

16*a* = *a*0,

The linear approximation of this polynomial will be the expres- sion *pva* = *a*g = *acpa*+, which is identical to the one already men-

*pa*(0) =

06*a*–*a*0.

tioned in section 2.1, proven adequate in the Kefard and White model. This circumstance analytically confirms that the mathe-

In turn, with known probabilities [(3)](#_bookmark8), we can estimate the aver- age number of affected cluster elements at a time *t* using the expression

X

*n*

*A*(*t*) = *apa*(*t*) (4)

*a*=0

Parameter [(4)](#_bookmark7) is a basic metric that will characterize the devel- opment of the research process. The following theoretical material will be formulated around the parameter *A*(*t*).

* 1. *Approximate estimation of the average number of affected elements of a high-availability cluster under the influence of a viral*

matical transformations of expression [(2)](#_bookmark4) we made in section 2.2 did not lead to the original model losing its adequacy.

Let’s move on to the formalization of the recurrent expression for the approximate estimation of the parameter [(4)](#_bookmark7). Let the aver- age number of affected elements in the cluster be *A*~(*t*) at an arbi- trary moment in time *t* P 0. Then the probability that at the moment *t* + 1 a potentially vulnerable element will transit to the affected state will be determined by the expression

*p* = 1 — (1 — g)*A*~(*t*) (8)

*va*

Based on expression [(8)](#_bookmark10), we can argue that at the time *t* + 1, on average,

*cyberthreat*

*pva*

(1 — *A*~(*t*)) = (*n* — *A*~(*t*)) 1 — (1 — g)*A*~(*t*)

Metric [(4)](#_bookmark7) is the most compact representative characteristic of the development of the studied process. However, to directly cal- culate the parameter *A*(*t*) using expression [(4)](#_bookmark7), it is necessary to raise the transition probability matrix P to a degree *t*. The compu- tational complexity of this operation rapidly non-linearly increases with an increase in the value of *t* (expression [(3)](#_bookmark8)) and an increase in the number of elements in the cluster *n* (the dimension of the matrix P is n × n, and the calculation of each element of this matrix according to expression [(1)](#_bookmark3) is accompanied by the calculation of

the coefficient *Ki* , where *a*(*n*), *i*(*n*)). All these circumstances

*a*

encourage the search for a computationally efficient concept for calculating the approximate value of the parameter *A*(*t*).

elements of the cluster that are potentially vulnerable at a time *t*

will transit to the affected state. At the same time, at moment

*t* + 1, *pav A*~(*t*) elements of the cluster, which were in the affected state at the moment *t*, will transit to the potentially vulnerable

state. Summarizing what has been said, we formulate an expres- sion for estimating the average number of affected elements of the cluster at the moment *t* + 1:

*A*~(*t* + 1) = (1 — *pav* )*A*~(*t*)+

+(*n* — *A*~(*t*)) 1 — (1 — g)*A*~(*t*) . (9)

Naturally, when applying expression [(9)](#_bookmark12), it should be taken into

Let’s start by writing out the multiplier 1 — 1 — *pa*+

expression [(2)](#_bookmark4):

*i* in

account that at the time *t* = 0 there are *a*0 elements of the cluster in the affected state:

*a a A*~(0) = *a*0 (10)

*p* = X *Ki ci*(1 — *c*)*a*—*i* — X *Ki ci*(1 — *c*)*a*—*i* 1 — *p*

*i* (5)

It can be expected that the function *A*~ *t*

will qualitatively

*va a*

*i*=0

*a a*+

*i*=0

( )

approximate the etalon function *A*(*t*) for a fairly wide range of val-

The minuend in expression [(5)](#_bookmark14) is the binomial expansion of the one. Let’s expand the subtrahend from expression [(5)](#_bookmark14) using New- ton’s binomial formula:

*a*

P *K c* (1 — *c*) 1 — *p* *i* =

*i i a*—*i*

*a a*+

*i*=0

*a a*

= *c* 1 — *pa*+ + 1 — *c* = 1 — *cp* .

*a*+

ues of the controlled parameters {g, *pav* , *a*0}. Moreover, the approx- imation error will decrease as the values of the parameters *a* and *t*

increase. It is rather difficult to strictly analytically estimate the error of approximation of the function *A*(*t*) by the recurrent sequence (10)-(9). However, the analytical form of the function

[(9)](#_bookmark12) allows us to predict that as the number of elements of the clus- ter *n* increases, the deviation of the values of the function *A*~(*t*) from the corresponding values of the function *A*~(*t*) will decrease.

At the same time, with the fixed values of the parameters a0 and *n*, for certain values of the parameters g and *pav* , the limit expression lim *A*(*t*) = *A* = 0 will be fulfilled. Judging by the analytical form of

*t*→∞ ∞

function [(9)](#_bookmark12), for the same range of values of the tuple

{*a*0, *n*, g, *pav* }, the limit value of the function *A*~(*t*) will be different

~

from zero:lim *A*~(*t*) = *A* –0. The contribution of this collision to the

resulting error of approximation of the function *A*(*t*) by the func-

*av*

*a*+

*n*

— ln b/*pav* 6 1 Ξ 1 — *cpa*+ P exp (—*p* ) (13)

*av*

If criterion [(13)](#_bookmark15) is fulfilled for the investigated process of the influence of an active viral cyber threat on the target cluster of high availability, then over time (*t* → ∞) the protective mechanisms of the information system will overcome the negative impact on their

own. If criterion [(13)](#_bookmark15) is not fulfilled (threshold value

*t*→∞ ∞

*T*(*p* ) = —*n* ln 1 — *cp* ), then it will not be possible to overcome

tion *A*~(*t*) should be investigated by numerical methods. Finally, based on analytical expressions [(4) and (9)](#_bookmark7), it can be asserted that the functions *A*(*t*) and *A*~(*t*) react differently to the initiating value

(parameter a ). It can be expected that the function *A t* is more

the negative influence without external intervention. It should be noted that the expression for calculating the threshold value

*T*(*pav* ) was derived based on the investigation of the limit approx-

imate value of the parameter A(t), i.e.*A*~. This means that the value

0 ( ) ∞

sensitive to the value of the parameter a0 than the function *A*~(*t*). It can also be predicted that this discrepancy will quickly level off with an increase in the value of the parameter *a*. However, this statement also needs experimental verification.

Before proceeding to the experimental verification of the hypotheses made above, let us pay attention to the analytical form

of the parameter *T*(*pav* ) is an approximate optimistic estimate of the exact threshold value. However, this circumstance does not

negate the fact that as the value *t* increases, criterion [(13)](#_bookmark15) turns from a law rule.

Therefore, based on the Markov model of the process of the influence of a viral cyberthreat on a target high-availability cluster

of the limit expression for the function *A*~ *t* , that is lim ~

~ described in [Section 2.1](#_bookmark5), a computationally efficient method of

( )

*t*→∞

*A* (*t*) = *A*.

∞

approximate estimation of the average number of affected cluster

Let’s rewrite expression [(9)](#_bookmark12) in the context of applying the notation

~

*A*:

∞

~ ~ ~ ~

1 — (1 — g)*A*

∞

∞

∞

*A* = (1 — *pav*

) *A* + *n* — *A*

∞

(11)

Equation [(11)](#_bookmark16) does not depend on the initial value [(10)](#_bookmark13). This fact allows us to state that the difference between the limit values of *A*

∞

and *A*~ is not affected by the parameter *a*0. For the convenience of

∞

further analytical operations, let’s simplify expression [(11)](#_bookmark16) to the form

*xpav* = (1 — *x*)(1 — b*x*), *pav* > 0 (12)

where *x* = *A*~ /*n* is the relative number of affected cluster ele-

∞

ments at the limiting moment *t* →∞ and b = (1 — g)*n* is an auxil- iary designation.

Expression [(12)](#_bookmark17) is a transcendental equation concerning the variable *x* ∈ [0,1], the analytical solution of which does not exist. However, the approximate solution of equation [(12)](#_bookmark17) can be obtained by numerical methods, including zero-order ones. To a large extent, this solution can be characterized in advance. In par-

ticular, the number x = 0 will always be among the roots of equa-

elements under the influence of a viral cyber threat is formulated in [Section 2.2](#_bookmark11), and a criterion is defined that allows investigating the trend of the progress of the researched process on medium and long periods.

1. Experiments

To present the functionality of the proposed method of approx- imate estimation of the average number of affected elements of the target cluster of high availability under the influence of an active viral cyber threat, we will apply the capabilities of simulation modelling.

The specialized MathWorks MATLAB software package was chosen to implement the simulation model. The justification for such a choice is that the functions of the toolboxes of this software platform have been tested worldwide and their adequacy has been empirically proven. Using mostly the Hidden Markov Model Tool- box, we created the following custom functions:

- MyPoission(a,k) is a function for modelling a stochastic value with a Poisson distribution, where a is the number of events, k is their intensity;

tion [(12)](#_bookmark17). Non-zero values *A*~

∞

will correspond only to roots

- *MyState* (*X*, K, *M*, *R*, *a*) is a function for implementing the tran-

sition of a discrete Markov chain to the next state from the cur-

belonging to the segment (0,1]. The absence of such roots will indi-

0

rent X, which is characterized by a tuple of sets ⟨K, M, *R*⟩, where

~

*A* =

∞

cate that

06*a* .

n — o

Let us introduce an infinitely differentiable function

K = k1, k*n*

is a set of intensities of viral cyberthreat flows

with a negative second derivative

*n*

affecting the studied cluster, k ≥ 0; M = nl —l o is the set of

*pa*+

*f* (*x*) = (1—*x*)(1—b*x* )

i

1,

'' b*x*

intensities of flows of cyber-immune reactions of cluster ele-

*f* (*x*) = ln b(2 — (1 — *x*) ln b) on the unit segment. The first

*p*

i

1, *n*

*av*

ments, l ≥ 0; *R* = n*r* —*r* o is the set of probabilities of neutral-

derivative of the function *f* (*x*) decreases monotonically on the unit segment. For the limit values, we write:*f* '(0) = — ln (b)/*pav* > 0,*f* '(1) = (b — 1)/*pav* < 0. This means

that there is a single point u ∈ (0, 1) at which *f* '(u) = 0, that is,

the function *f* (*x*) monotonically increases during the interval

[0, u), and monotonically decreases during the interval (u, 1].

The presented results of the analysis of the function *f*(*x*) make it possible to formulate a condition under which the solution of

equation [(12)](#_bookmark17) (equivalent to the equation *x* = *f*(*x*)) will not contain roots on the segment (0, 1]. This condition: if the tangent *y* = —*x* ln b/*pav* to the function f(x) at the point x = 0 lies under the line y = x (only under such circumstances the graphs of the

izing the effects of viral cyberthreat by protective mechanisms (returning cluster elements from an affected to a potentially vulnerable state), 0 ≤ rj ≤ 1;

*MyDMC* (K, *M*, *R*, *a0*, t = 0) is a function for implementing a parameterized instance of a discrete Markov chain with an initiat- ing effect a0 and calculating for the current moment *t* P 1 the exact value of the quantitative metric *A*(*t*) according to expression

1. and the approximate value of the quantitative metric *A*~(*t*)

according to expressions [(9)](#_bookmark12), [(10)](#_bookmark13).

Let us focus on the description of the function *MyState*. For a discrete Markov chain n, the state X is determined by a pair of

n o

functions *y* = *f*(*x*) and y = x will not intersect on the unit interval).

On this basis, the criterion for the absence of nonzero roots of

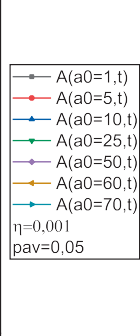
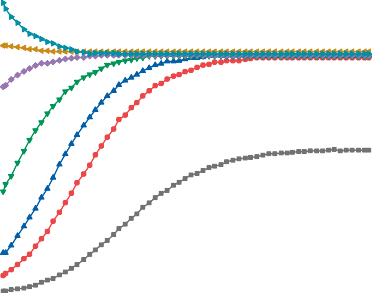
parameters (*a*, *t*), where *a*

—

∈ 0, *n* is the identifier of state X and

equation [(12)](#_bookmark17) on the unit interval looks like this: t is the moment when the system transitions to state X. The func-

tion *MyState* implements the transition of the system from the cur- rent state X=(a,t) to the next state *X*' = (*a*', *t*'):*X* → *X*'. The values of parameters a’, t’ are determined depending on the value of the parameter a. If:



* + a = 0 (all elements of the cluster are in a potentially vulnerable state / a viral cyber threat to the cluster is not implemented), then the function *MyState* generates a set of stochastic values

—

T = {s*i* },*i* = 1, *n*, using the function *MyPoisson*. Let

s min ns —s o for *j* n — o, then we take *a*' *a j* and

*j* =

1,

*n*

∈ 1, *n*

=

+

*t*' = *t* + s*j* , that is,*X*' = *j*, *t* + s*j* ;

n o

* + - *a*

—

∈ 1, *n* (the elements of the cluster are negatively affected

in the form of a viral cyberthreat), then the function *Mystate* generates, using the function *MyPoisson*, a stochastic value s distributed according to the Poisson distribution law with parameter ka. We accept *t*' = *t* + s. Using the standard MATLAB function *Rand*, we obtain a stochastic number × uniformly dis- tributed over the interval [0, 1]. If the inequality ra > *x* holds, then we take a’,=0 otherwise, we take a’=a + r;

* + a = n (all elements of the cluster are in an affected state, that is, the protective mechanisms did not cope with the viral cyber- threat), then the function *MyState* accepts a’=n and t’=t. Accordingly,*X*' = *X* = (*a* = *n*, *t*).

Functioning according to the algorithm described above, the function *Mystate* allows for the discrete Markov chain n to calculate the sequence of states of the form *X*0 = (*a*0 = 0, *t*0 = 0) ?

*X*1 = (*a*1, *t*1) ? ... ?*Xn* = (*a* = *n*, *tn*). The initialization of the model

(state X0) is implemented by the function *MyDMC* (K, *M*, *R*, *a0*, t = 0). Each subsequent iteration is implemented by calling the function and ends by calling the function, returning the output val- ues of and. Transitions occur a predetermined number of times or until the model enters the state.

To conduct experiments, it was necessary to obtain data for a tuple of sets. Such information was kindly provided by the staff of the Situation Center of the Information Technology Department of Vinnytsia City Council (Vinnytsia, Ukraine) (hereinafter referred to as SC). The staff of the SC department supports the functioning of the distributed information and communication system (high availability cluster), which manages video surveillance and traffic lights on the roads of Vinnytsia. There are more than 1000 ele- ments (servers, workstations, client computers) involved in infor- mation exchange and are potentially vulnerable to viral cyber threats in the architecture of the information and communication system of the SC.

The analysis of the SC system operation logs for the period from 09/01/2020 to 09/01/2021 (365 full days) in the context of detect- ing cases of implementation of viral cyber threats, summarized in the set, made it possible to determine the following input data for modelling:

*Na* = 3, K = (4.27, 3.96, 1.12)

## *M*(0.91, 0.41, 0.94)

*R* = (0.09, 0.39, 0.0.37)

where Na is the number of recorded cases of implementation of viral cyber threats against the SC cluster for the censored period.

The obtained data made it possible to calculate the shown in [Figs. 2 and 3](#_bookmark18) dependences of *A*(*a*0, *n*, g, *pav* ) and *A*~(*a*0, *n*, g, *pav* ), respectively. At the same time, the author’s software was launched with such initiating data as *a*0 = {1, 5, 10, 25, 50, 60, 70}. In addi- tion, such values of the established parameters of the model (1)-

(2) were specified *n* = 100,g = 0.001,*p*

*av*

= 0.05.

Fig. 2. Graphs of function *A*(*a*0, *n*, g, *pav* ) at *a*0 = {1, 5, 10, 25, 50, 60, 70},*n*, g, *pav* =

const.

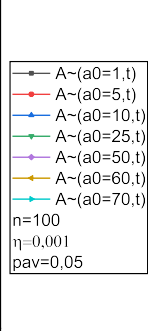
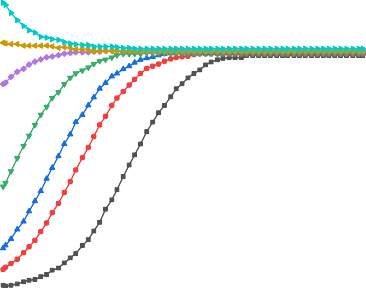


Fig. 3. Graphs of function *A*~(*a*0, *n*, g, *pav* ) at *a*0 = {1, 5, 10, 25, 50, 60, 70},*n*, g, *pav* =

const.

We did not neglect the part of the material presented in section 2.2, devoted to the formalization of the trend evaluation of the quantitative parameter of the metric of the model of the studied process (that is, the process of the influence of an active viral cyberthreat on a high-availability cluster) over medium and long periods.

∞ ∞

50}, *p*

= {0.01, 0.1, 0.2, .. . , 0.9}, *n*, g = const.



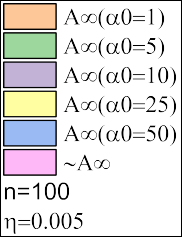


Fig. 4. Diagrams for functions *A* (*a*0, *n*, g, *pav* ), *A*e (*a*0, *n*, g, *pav* ) at *a*0 = {1, 5, 10, 25,

*av*

Table 1

Detailed presentation of information from [Fig. 4](#_bookmark20).

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| *pav* | *A*  ∞  (*a*0 = 1) | *A*  ∞  (*a*0 = 5) | *A*  ∞  (*a*0 = 10) | *A*  ∞  (*a*0 = 25) | *A*  ∞  (*a*0 = 50) | ~  *A*  ∞ |
|  |  |  |  |  |  |  |
| 0,001 | 99,658 | 99,779 | 99,779 | 99,779 | 99,779 | 99,7806 |
| 0,01 | 96,6112 | 97,8012 | 97,8012 | 97,8012 | 97,8012 | 97,8176 |
| 0,05 | 83,7142 | 89,2378 | 89,2379 | 89,2379 | 89,2379 | 89,3396 |
| 0,1 | 69,0677 | 79,0778 | 79,0808 | 79,0808 | 79,0808 | 79,268 |
| 0,2 | 44,2002 | 60,1127 | 60,2082 | 60,2084 | 60,2084 | 60,659 |
| 0,3 | 0 | 0 | 0 | 0 | 0 | 43,7863 |
| 0,4 | 0 | 0 | 0 | 0 | 0 | 28,3589 |
| 0,5 | 0 | 0 | 0 | 0 | 0 | 14,153 |
| 0,6 | 0 | 0 | 0 | 0 | 0 | 0,99239 |

For the corresponding experiment, we used already developed software, which was launched at such values of fixed parameters as *n* = 100,g = 0.005. With such a configuration of input parameter values, the threshold value *T*(*pav* ) derived from criterion [(13)](#_bookmark15) is

mate analogue of the metric (4)) of the studied process on medium and long-term time intervals.

Now let’s focus on those presented in Fig. 4 results of the inves- tigation of the limit values of metrics (4) and (9). It can be seen that

equal to 0.5023. For the parameter *pav* (probability of the transition

for values of *p*

~

*T p* , the approximate value of

*v*

of the affected element to a potentially vulnerable state) changing

*av* >>

( *av* )

*A* (*pa* ) quali-

∞

in the range (0.001, 0.1, 0.2, ... , 0.9), we calculated the value of the

~

parameter *A* (*pa* ) using equation [(12)](#_bookmark17). Further, with the help of

*v*

∞

algorithms standard for the theory of Markov processes, we calcu-

lated the valid limit values of the parameter *A* (*pa* ) for the same set

*v*

∞

of input data (*pav* = (0.001, 0.1, 0.2, ... , 0.9),*n* = 100, g = 0.005),

additionally varying the value of the parameter

*a*0 = {1, 5, 10, 25, 50} (the number of affected cluster elements at the time *t* = 0).

The calculated values of the functions *A* (*a*0, *n*, g, *pa* ) and

*v*

∞

~

*A* (*a*0, *n*, g, *pa* ) are visualized in the form of the corresponding dia-

*v*

∞

grams in [Fig. 4](#_bookmark20) and [Table 1](#_bookmark21).

1. Discussion

Let’s start the discussion of the scientific and experimental results presented in the article, focusing on [Figs. 2 and 3](#_bookmark18). The graphs shown in [Fig. 2](#_bookmark18) characterize the Markov model of type (1)-(2) of the information and communication system of SC in the metric (4), calculated by classical methods of the theory of Markov processes. In practice, this is implemented in the form of software based on globally proven Hidden Markov Model Toolbox algorithms of the specialized MathWorks MATLAB software pack- age. These prerequisites allow us to consider those shown in [Fig. 2](#_bookmark18) reference results. Accordingly, as visualized in [Fig. 3](#_bookmark19) results characterize the new mathematical apparatus proposed by the authors in section 2.2, generalized by the recurrent sequence (10)-(9), for the approximate calculation of the metric (4) for the model (1)-(2) of the target researched process.

It can be visually verified that the function *A*~(*t*) qualitatively approximates the etalon function *A*(*t*) for a fairly wide range of val- ues of the controlled parameters {g, *pav* , *a*0}. Moreover, the devia-

tion of the values of the function *A*~(*t*) from the values of the

function *A*~(*t*) decreases with the increase in the value of the parameters *a* and *t*. It is noticeable that the functions *A*(*t*) and *A*~(*t*) react differently to the initiating value (parameter *a*0). The function *A*(*t*) is more sensitive to the value of the parameter *a*0 than the function *A*~(*t*). However, this discrepancy is quickly lev- elled off with an increase in the value of the parameter *a*.

In general, comparing presented in Fig. 3 (author’s) and Fig. 2 (etalon) results, the mathematical apparatus summarized by expressions (9) and (10) can be recognized as adequate. The author’s mathematical apparatus proved to be particularly effec- tive for the calculation of the quantitative metric (9) (an approxi-

tatively approximates the exact value of *A* (*pa* ). What is more, this

∞

*v*

tendency becomes more apparent with the increasing value of the initiating parameter *a*0. This circumstance does not contradict the conclusions we made above regarding the comparison of the results shown in Figs. 2 and 3. A significant deviation of the values

~

*A* (*pav* ) from the etalon values *A* (*pav* ) is manifested when the values

∞

∞

of the parameter *pav* approach the threshold *T*(*pav* ) = 0.5023. The value of *A* (*pav* ) is exhausted already at *pav* = 0.3, while the author’s

∞

mathematical apparatus shows a similar result only at *pav* ≈ 0.55. However, at values of the parameter *pav* outside of the vicinity of the threshold value *T*(*pav* ), the author’s and reference mathemati- cal apparatus for estimating the limit value of the average number

of affected cluster elements under the influence of a viral cyber- threat show the same results.

As expected, the results of the experiments showed that the

approach to determining the threshold value *T*(*pav* ) based on crite- rion (13) is quite rough, because it is the result of ‘‘simplification

raised to the absolute.” Determination of the confidence interval for the parameter *T*(*pav* ) is a promising direction for further

research.

In summarizing, we recall that the linear approximation of the polynomial (7) is the expression *pva* = *a*g = *acpa*+, which is identi- cal to the adequate, tested model of Kefard and White. This circum-

stance analytically confirms that the mathematical transformations of expression (2) made by us in section 2.2 did not lead to the loss of adequacy of the original model presented in section 2.1.

1. Conclusions

The field of computer science, like its sub-field of cyber threat modelling, is rapidly evolving. The prerequisites for key changes can be summarized as follows: cyber threats are evolving; there are leaks of special services tools; agile development methodology is being introduced everywhere; the boundaries of the object of protection are blurred; the scope of application of artificial intelli- gence is expanding; potentially vulnerable API integrations are increasingly being used. These factors lead to the fact that the pro- cesses of analysis of cyber threats, analysis of protective measures, generalization of data, and development of protective tools should now be considered continuous, not discrete. At the same time, the cost of cybersecurity increases like an avalanche in an attempt to avoid reputational and information losses. The only way to avoid this tendency is to apply a rational, scientific, accurate method of

cognition to these processes. Thus, the creation of mathematical models of processes in the field of cybersecurity is now more rele- vant than ever.

The article is devoted to the investigation of the process of the influence of an active viral cyber threat on a high-availability clus- ter in the paradigm of the provisions of the theory of Markov pro- cesses, graph theory and the theory of mathematical analysis. The main contribution of the research is a formalized computationally efficient method of approximate estimation of the average number of affected elements of the target high-availability cluster under the influence of an active viral cyber threat. Also, a criterion that allows estimating the trend of the quantitative parameter of the metric of the model of the studied process at medium and long time intervals is proposed. To obtain the declared scientific result, the authors: - formulated a Markov model of the process of the influence of an active viral cyber threat on a high availability clus- ter; - substantiated a compact metric for accurate assessment of the average number of cluster elements affected by an active viral cyber threat at any time; - formulated a computationally efficient method of approximate estimation of the parameter of the men- tioned metric for the model of the target studied process; - pro- posed a criterion that allows researchers to evaluate the trend of the parameter of the mentioned metric for the model of the target researched process at medium and long intervals of time.

The adequacy of the formulated method has been proven empirically. visualized in [Fig. 3](#_bookmark19) results characterize the new math- ematical apparatus proposed by the authors in section 2.2, gener- alized by the recurrent sequence (10)-(9), for the approximate calculation of the metric [(4)](#_bookmark7) for the model (1)-(2) of the target researched process. It can be visually verified that the function qualitatively approximates the etalon function for a fairly wide range of values of the controlled parameters. Moreover, the devia- tion of the values of the function from the values of the function decreases with the increase in the value of the parameters and. It is noticeable that the functions and react differently to the initiat- ing value (parameter). It can be seen in [Fig. 4](#_bookmark20) that for values of, the approximate value of qualitatively approximates the exact value of. What is more, this tendency becomes more apparent with the increasing value of the initiating parameter. This circumstance does not contradict the conclusions we made above regarding the comparison of the results shown in [Figs. 2 and 3](#_bookmark18). A.

As it turned out, the simplification of the classical approach pro- posed by the authors to the calculation of the average number of cluster elements affected by an active viral cyber threat is accom- panied by a noticeable error when determining this characteristic parameter at short time intervals. Also, the results of the experi- ments showed that the author’s approach to determining the threshold value based on criterion [(13)](#_bookmark15) is quite rough. */5TtheT TeseaTch* is planned to address these limitations.

Declaration of Competing Interest

The authors declare that they have no known competing finan- cial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

This work is funded by Researchers Supporting Project number (RSP-2022R503), King Saud University, Riyadh, Saudi Arabia.

Funding

RSP-2022R503.

Institutional review board statement

Not applicable.

Informed consent statement

Informed consent was obtained from all subjects involved in the study.

Data availability statement

Most data is contained within the article. All the data are avail- able on request due to restrictions e.g. privacy or ethics.

References

1. Maloth S, Vanmathi C. Attacks on Cyber Physical System: Comprehensive Review and Challenges. Int J Wireless Microwave Technol (IJWMT) 2022;12
2. :53–73. doi: <https://doi.org/10.5815/ijwmt.2022.05.06>.
3. Aliyev AG. Technologies Ensuring the Sustainability of Information Security of the Formation of the Digital Economy and their Perspective Development Directions. Int J Inf Eng Electron Business (IJIEEB) 2022;14(5):1–14. doi: <https://doi.org/10.5815/ijieeb.2022.05.01>.
4. V. Kovtun, I. Izonin, and M. Gregus, ‘‘Reliability model of the security subsystem countering to the impact of typed cyber-physical attacks,” Scientific Reports, vol. 12, no. 1. Springer Science and Business Media LLC, Jul. 27, 2022. doi: 10.1038/s41598-022-17254-4..
5. S [ims](http://refhub.elsevier.com/S1110-8665(22)00070-6/h0020) [ek A. ‘‘Lexical sorting centrality to distinguish spreading abilities of nodes](http://refhub.elsevier.com/S1110-8665(22)00070-6/h0020) [in complex networks under the Susceptible-Infectious-Recovered (SIR)](http://refhub.elsevier.com/S1110-8665(22)00070-6/h0020) [model”, Journal of King Saud University - Computer and Information](http://refhub.elsevier.com/S1110-8665(22)00070-6/h0020) [Sciences. Elsevier BV 2022;34(8):4810–20](http://refhub.elsevier.com/S1110-8665(22)00070-6/h0020).
6. [Abhishek V, Srivastava V. SIR Epidemic Model under Mobility on Multi-layer](http://refhub.elsevier.com/S1110-8665(22)00070-6/h0025) [Networks. IFAC-PapersOnLine 2020;53(5):803–6](http://refhub.elsevier.com/S1110-8665(22)00070-6/h0025).
7. O. Bisikalo, O. Danylchuk, V. Kovtun, O. Kovtun, O. Nikitenko, and V. Vysotska, ‘‘Modeling of Operation of Information System for Critical Use in the Conditions of Influence of a Complex Certain Negative Factor,” International Journal of Control, Automation and Systems, vol. 20, no. 6. Springer Science and Business Media LLC, pp. 1904–1913, Apr. 29, 2022. doi: 10.1007/s12555- 021-0368-6..
8. [Blavatska V, Holovatch Yu. Spreading processes in ‘‘post-epidemic”](http://refhub.elsevier.com/S1110-8665(22)00070-6/h0035) [environments. II. Safety patterns on scale-free networks. Phys A: Stat Mech](http://refhub.elsevier.com/S1110-8665(22)00070-6/h0035) [Appl 2022;591:126799](http://refhub.elsevier.com/S1110-8665(22)00070-6/h0035).
9. [Huo H-F, Yang P, Xiang H. Dynamics for an SIRS epidemic model with infection](http://refhub.elsevier.com/S1110-8665(22)00070-6/h0040) [age and relapse on a scale-free network. J Franklin Inst 2019;356(13):7411–43](http://refhub.elsevier.com/S1110-8665(22)00070-6/h0040).
10. [Kovtun V, Izonin I, Gregus M. Model of Information System Communication in](http://refhub.elsevier.com/S1110-8665(22)00070-6/h0045) [Aggressive Cyberspace: Reliability, Functional Safety, Economics. IEEE Access](http://refhub.elsevier.com/S1110-8665(22)00070-6/h0045) [2022;10:31494–502](http://refhub.elsevier.com/S1110-8665(22)00070-6/h0045).
11. [Long Y, Zhang Yu, Wu M, Peng S, Kwoh CK, Luo J, et al. Heterogeneous graph](http://refhub.elsevier.com/S1110-8665(22)00070-6/h0050) [attention networks for drug virus association prediction. Methods](http://refhub.elsevier.com/S1110-8665(22)00070-6/h0050) [2022;198:11–8](http://refhub.elsevier.com/S1110-8665(22)00070-6/h0050).
12. [Hu Z, Odarchenko R, Gnatyuk S, Zaliskyi M, Chaplits A, Bondar S, et al.](http://refhub.elsevier.com/S1110-8665(22)00070-6/h0055) [Statistical Techniques for Detecting Cyberattacks on Computer Networks](http://refhub.elsevier.com/S1110-8665(22)00070-6/h0055) [Based on an Analysis of Abnormal Traffic Behavior. IJCNIS 2021;12(6):1–13](http://refhub.elsevier.com/S1110-8665(22)00070-6/h0055).
13. [Shahid N, Aziz-ur Rehman M, Khalid A, Fatima U, Sumbal Shaikh T, Ahmed N,](http://refhub.elsevier.com/S1110-8665(22)00070-6/h0060) [et al. Mathematical analysis and numerical investigation of advection-](http://refhub.elsevier.com/S1110-8665(22)00070-6/h0060) [reaction-diffusion computer virus model. Results Phys 2021;26:104294](http://refhub.elsevier.com/S1110-8665(22)00070-6/h0060).
14. [Hu Z, Khokhlachova Y, Sydorenk V, Opirskyy I. Method for Optimization of](http://refhub.elsevier.com/S1110-8665(22)00070-6/h0065) [Information Security Systems Behavior under Conditions of Influences. IJISA](http://refhub.elsevier.com/S1110-8665(22)00070-6/h0065) [2017;9(12):46–58](http://refhub.elsevier.com/S1110-8665(22)00070-6/h0065).
15. Kekül H, Ergen B, Arslan H. Comparison and Analysis of Software Vulnerability Databases. Int J Eng Manuf (IJEM) 2022;12(4):1–14. doi: [https://doi.org/](https://doi.org/10.5815/ijem.2022.04.01) [10.5815/ijem.2022.04.01](https://doi.org/10.5815/ijem.2022.04.01).
16. [Kovalskyi B, Dubnevych M, Holubnyk T, Pysanchyn N, Havrysh B. Development](http://refhub.elsevier.com/S1110-8665(22)00070-6/h0075) [of a technology for eliminating color rendering imperfections in digital](http://refhub.elsevier.com/S1110-8665(22)00070-6/h0075) [photographic images. EEJET 2019;1(2):40–7](http://refhub.elsevier.com/S1110-8665(22)00070-6/h0075).
17. [Zimba A. A Bayesian Attack-Network Modeling Approach to Mitigating](http://refhub.elsevier.com/S1110-8665(22)00070-6/h0080) [Malware-Based Banking Cyberattacks. IJCNIS 2021;14(1):25–39](http://refhub.elsevier.com/S1110-8665(22)00070-6/h0080).
18. [Long L, Zhong K, Wang W. Malicious viruses spreading on complex networks](http://refhub.elsevier.com/S1110-8665(22)00070-6/h0085) [with heterogeneous recovery rate. Phys A: Stat Mech Appl 2018;509:746–53](http://refhub.elsevier.com/S1110-8665(22)00070-6/h0085).
19. A. Doroshenko, K. Obelovska and O. Bilyk, ‘‘Risk Analysis of Personal Data Loss in Wireless Sensor Networks,” CITRisk’2021: 2nd International Workshop on Computational & Information Technologies for Risk-Informed Systems, Kherson, Ukraine, September 16-17, 2021. <http://ceur-ws.org/Vol-3101/> Paper19.pdf.
20. [Machado MR, Pantano S. Fighting viruses with computers, right now. Curr](http://refhub.elsevier.com/S1110-8665(22)00070-6/h0095) [Opin Virol 2021;48:91–9](http://refhub.elsevier.com/S1110-8665(22)00070-6/h0095).
21. [Pan W, Jin Z. Edge-based modeling of computer virus contagion on a tripartite](http://refhub.elsevier.com/S1110-8665(22)00070-6/h0100) [graph. Appl Math Comput 2018;320:282–91](http://refhub.elsevier.com/S1110-8665(22)00070-6/h0100).
22. [Liang X, Pei Y, Lv Y. Modeling the state dependent impulse control for](http://refhub.elsevier.com/S1110-8665(22)00070-6/h0105) [computer virus propagation under media coverage. Phys A: Stat Mech Appl](http://refhub.elsevier.com/S1110-8665(22)00070-6/h0105) [2018;491:516–27](http://refhub.elsevier.com/S1110-8665(22)00070-6/h0105).
23. [Ren J, Xu Y. A compartmental model to explore the interplay between virus](http://refhub.elsevier.com/S1110-8665(22)00070-6/h0110) [epidemics and honeynet potency. App Math Model 2018;59:86–99](http://refhub.elsevier.com/S1110-8665(22)00070-6/h0110).
24. [Gao W, Baskonus HM. Deeper investigation of modified epidemiological](http://refhub.elsevier.com/S1110-8665(22)00070-6/h0115) [computer virus model containing the Caputo operator. Chaos Solitons Fractals](http://refhub.elsevier.com/S1110-8665(22)00070-6/h0115) [2022;158:112050](http://refhub.elsevier.com/S1110-8665(22)00070-6/h0115).
25. Aliyev AG, Shahverdiyeva RO. Scientific and Methodological bases of Complex Assessment of Threats and Damage to Information Systems of the Digital Economy. Int J Inf Eng Electron Business (IJIEEB) 2022;14(2):23–38. doi: <https://doi.org/10.5815/ijieeb.2022.02.02>.
26. R. Tkachenko, ‘‘An Integral Software Solution of the SGTM Neural-Like Structures Implementation for Solving Different Data Mining Tasks,” Lecture Notes in Computational Intelligence and Decision Making. Springer International Publishing, pp. 696–713, Jul. 23, 2021. doi: 10.1007/978-3- 030-82014-5\_48.
27. R. Tkachenko and I. Izonin, ‘‘Model and Principles for the Implementation of Neural-Like Structures Based on Geometric Data Transformations,” Advances in Intelligent Systems and Computing. Springer International Publishing, pp. 578–587, May 12, 2018. doi: 10.1007/978-3-319-91008-6\_58.
28. [Dronyuk I, Fedevych O, Kryvinska N. Constructing of Digital Watermark Based](http://refhub.elsevier.com/S1110-8665(22)00070-6/h0135) [on Generalized Fourier Transform. Electronics 2020;9(7):1108](http://refhub.elsevier.com/S1110-8665(22)00070-6/h0135).
29. [Thu Thu Khine P, Pa Pa Win H, Ni Tun KN. New Intrusion Detection Framework](http://refhub.elsevier.com/S1110-8665(22)00070-6/h0140) [Using Cost Sensitive Classifier and Features. IJWMT 2022;12(1):22–9](http://refhub.elsevier.com/S1110-8665(22)00070-6/h0140).
30. [Gan C, Qian Yi, Liu A, Zhu Q. Search-driven virus spreading on Social Internet of](http://refhub.elsevier.com/S1110-8665(22)00070-6/h0145) [Things: A dynamical perspective. Commun Nonlinear Sci Numer Simul](http://refhub.elsevier.com/S1110-8665(22)00070-6/h0145) [2022;114:106624](http://refhub.elsevier.com/S1110-8665(22)00070-6/h0145).
31. [Surajudeen Adebayo O, Bulus Micah J, Shefiu Olusegun G, O. Alabi I,](http://refhub.elsevier.com/S1110-8665(22)00070-6/h0150) [Abdulazeez L. Development of Secure Electronic Cybercrime Cases Database](http://refhub.elsevier.com/S1110-8665(22)00070-6/h0150) [System for the Judiciary. IJIEEB 2022;14(1):1–16](http://refhub.elsevier.com/S1110-8665(22)00070-6/h0150).
32. Farman M, Akgül A, Ahmad A, Saleem MU, Ahmad MO. Modeling and analysis of computer virus fractional order model. In: Methods of Mathematical Modelling. Elsevier; 2022. p. 137–57. doi: [https://doi.org/10.1016/b978-0-](https://doi.org/10.1016/b978-0-323-99888-8.00010-3) [323-99888-8.00010-3](https://doi.org/10.1016/b978-0-323-99888-8.00010-3).
33. [B. Dissanayake M. Feature Engineering for Cyber-attack detection in Internet](http://refhub.elsevier.com/S1110-8665(22)00070-6/h0160) [of Things. IJWMT 2021;11(6):46–54](http://refhub.elsevier.com/S1110-8665(22)00070-6/h0160).