Optimal cybersecurity management of an IP video surveillance system using neural network technologies

Evgenia Tsarkova[1,2*]

[1] Research Institute of the Federal Penitentiary Service of Russia, Center for the Study of Problems of Management and Organization of Execution of Punishments in the Penal System, 125130 Moscow, Russia
[2]Tver State University, st. Zhelyabova, 33, 170100, Tver, Russia

Abstract. The aim of the study is to solve the actual problem of constructing an optimal strategy for managing a system for protecting against the spread of computer epidemics of IP video surveillance networks used in the work of distributed situational centers. The paper presents a new mathematical modeling apparatus for building an adaptive network protection system from cyber-attacks using a hybrid approach that uses both classical control and neurocontrol based on an artificial neural network. Keywords: Situational center, IP video surveillance, computer viruses, simulation of the spread of epidemics, optimal control, neurocontrol.

1 Introduction

Nowadays, the urgency of creating state distributed situational centers, which are data analytics and technological support for managerial decision-making, is increasing. The most important component of situational centers created for the needs of law enforcement agencies, departments carrying out activities in the field of security is a distributed video monitoring system that combines a huge number of devices into a single system for collecting and processing information [1]. Despite the fact that the purpose of video surveillance is to ensure security, it itself is subject to various threats, including cyber threats, the implementation of which can lead to the fact that at any unpredictable moment the video surveillance system will not perform the tasks assigned to it. Information security threats in distributed IP video surveillance systems are a separate group of risks, the implementation of which can lead to a complete freeze of the system or its individual parts. It should be noted that the more complex the system, the higher the likelihood and adverse consequences of such freezes. Similar adverse situations can occur with Windows PC-based DVRs, Stand Alone DVRs and other devices. IP cameras, encoders (video servers), and intelligent linear equipment are affected by adverse effects caused by software or hardware flaws, processor overload [2]. A separate group of destructive influences is formed by vulnerabilities that arise as a result of system infection with viruses. Such influences can, for example, lead to a

* Corresponding author: university69@mail.ru

situation where the video camera does not freeze, continues to properly display the image on the screen, but, for example, the video stream is not recorded. Due to the nature of the virus to multiply many times, infection of the video surveillance system can lead to real cyber epidemics that affect more and more nodes of the data collection and analysis system used in security systems and the operation of departmental situational centers [3].

Thus, the development of models for the spread of viruses in IP video surveillance networks is an important direction and a necessary condition for building adequate information protection systems for situational centers. In this paper, mathematical models of the spread of viruses in a distributed network of video surveillance are studied, the problem of optimal control of the cybersecurity of a video surveillance system is formulated, including for further construction of adaptive control based on neurocontrol.

IP cameras and their associated equipment, connecting to the Internet, become a potential target for various cyber attacks. In recent years, a lot of research has been devoted to the discussion of cybersecurity issues, and the problems of countering cyber threats in technical systems are regularly brought up for discussion by the scientific community. Thus, the example of the mass destruction of devices by the Mirai botnet, including video surveillance equipment, in the fall of 2016 is indicative. The victims of the implemented security threat as a result of this incident were not only thousands of private users of IoT systems, but also large commercial companies (Netflix, Spotify, Twitter, etc.).

When building a distributed IP video surveillance system based on external uncontrolled communication networks, system segments (servers, cameras, storages) are connected via the Internet and/or a private corporate network, which leads to the possibility of cyber threats from an external uncontrolled network.

As a rule, the purpose of cyber attacks on IP video surveillance systems are:

- communication channels or lines (connections between equipment, server and cloud, server and third-party equipment). So, the violator can use methods of interception, organization of counteraction during data transmission, carry out deliberate damage or change of video and audio information;
- databases, including records of video archives. As a result of purposeful actions of the intruder, the loss of files or deliberate damage to the video archive is possible; video material can be substituted, and unauthorized viewing of video information received by the system is also possible;
- equipment for video recording. Unauthorized intervention of an intruder in the settings of video equipment becomes the cause of illegal seizure of control and unauthorized viewing of video information.

For the methods of information protection used in practice in IP video surveillance systems, the following classification is possible:

- built-in software protection. This protection method may include a set of specific functions that were originally provided by the manufacturer of the video surveillance system software (traffic encryption, password protection of the archive, etc.);
- protection implemented at the level of switching equipment. In this case, communication lines are protected by installing exclusively managed switches provided with encryption, access and audit restrictions;
- direct protection of video surveillance equipment. The organization of this method of protection is largely ensured by the competent actions of the installer, since in order to ensure information security when installing video equipment, it is required to change passwords, reset default settings, disable unused functions, organize support for current updates, etc.

To create an effective system of protection against destructive effects caused by malicious software distributed within the video monitoring system, it is necessary to build an adequate model for the distribution of malicious software between system nodes. Modeling destructive impacts on the system is one of the key stages in the development and implementation of

information security tools (IST), it provides an information security specialist with the opportunity to receive reasonable suggestions regarding the presence of potential cyber threats in a particular protected system. Mathematical, simulation models allow lab testing of the manifestation of a certain cyber attack, the analysis of its characteristics in order to determine adequate means of protection to neutralize it.

Among the threats to network security, attacks of computer worms stand out – software tools that have the ability to independently search for new nodes – the targets of infection, which uses the information and communication network for its distribution. The peculiarity of this type of malicious software is that the computer worm not only causes financial damage to the department (organization), but also is the basis for the implementation of other cyber threats, including unauthorized access to data, theft of confidential information, etc. Existing means of protecting communication networks and IP video surveillance systems often do not allow you to quickly stop computer worm epidemics, and therefore it is necessary to create detection and information protection systems that would be able to prevent and contain cyber epidemics in the early stages.

Therefore, it is necessary to develop a unified approach to modeling computer worm epidemics in distributed video surveillance systems to enable a detailed study of the implementation of this cyber threat, analysis of the factors that affect the spread of computer worms, as well as determining the mechanisms for possible detection and counteraction to the epidemic.

2 Materials and methods

The initial step in building an adequate model for the spread of an epidemic of computer worms is to choose the type of model that adequately describes the process of their spread over the network. To study the security of distributed IP video surveillance systems, an effective tool for studying is the analytical modeling of virus epidemics in the global network [4].

2.1 Biological models of the spread of network epidemics

The construction of analytical models for the spread of computer worms over a network is similar to the mathematical modeling of epidemic processes among living organisms [5]. Approaches to modeling and studying the spread of computer worms on the Internet using a mathematical tool for studying the dynamics of biological epidemics were proposed in the works of J. Kephart [6] and S. White from IBM [7]. The proposed approach turned out to be especially popular in 2001 as a result of the outbreak of the Code Red and Nimda epidemics [8]. At the beginning of the 21st century, the works of N. Weaver, who considered the concept of blitzkrieg worms (Warhol) and studied the operation of various algorithms that self-reproduce malicious program code and increase the efficiency of its distribution over the network, received recognition [9].

2.2 Malicious software distribution model in the IP video surveillance system

Electronic computing facilities used in distributed IP video surveillance systems are a set of physical and virtual devices connected to a single information and telecommunications data transmission network. To describe the dynamics of the spread of computer worms in such a system, we use the deterministic model of the epidemic spread of the SIR model (Susceptible-Infected-Removed model). This model is suitable for mathematical modeling of a cyber epidemic at the stage when the number of infected hosts reaches large values and allows

analyzing the factors that ensure the attenuation of network epidemics.

In the model under consideration, various network hosts can be in one of three states: sensitive (*s*), infected (*i*), resistant (*r*), while *s*+*i*+*r*=*N*, where *N* is a constant number of network hosts. We believe that network nodes become non-sensitive only if the infection is completely cured [10].

Let us introduce a constant average rate of "immunization" carried out per unit time through γ and the following notation:

$$I = \frac{i}{N},\ R = \frac{r}{N},\ S = \frac{s}{N}.$$

Then

$$\begin{cases} \dfrac{dS(t)}{dt} = -\beta I(t)S(t), \\ \dfrac{dI(t)}{dt} = \beta I(t)S(t) - \gamma I(t), \\ \dfrac{dR(t)}{dt} = \gamma I(t). \end{cases} \quad (1)$$

Figure 1 shows the graphs of the functions *S(t), I(t), R(t),* obtained with the following values of the parameters:

$$S(0) = S_0 = 4.7, I(0) = I_0 = 0.3, R(0) = R_0 = 0.01, \beta = 0.5, \gamma = 0.1, T = 10.$$

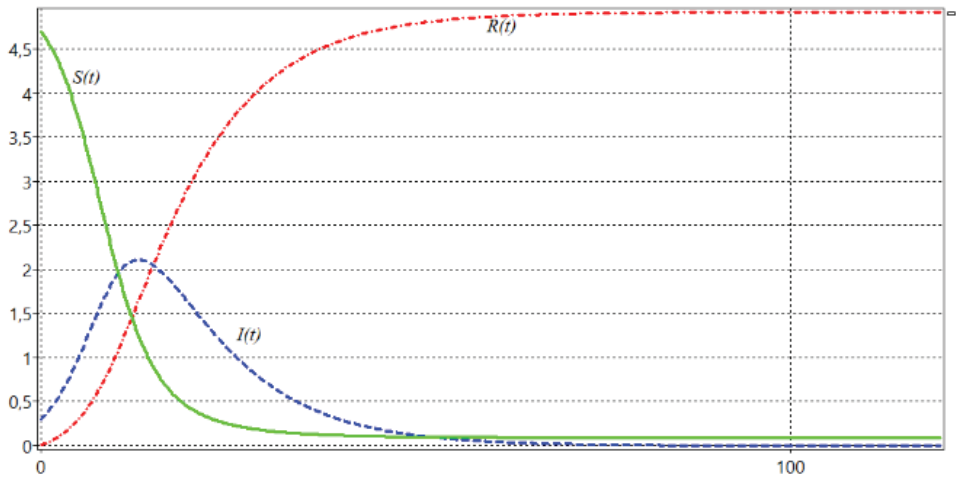

Fig. 1. Graphs of *S(t), I(t), R(t)* versus time.

The model takes into account the threshold value, which is a necessary condition for the spread of the epidemic; on the site of increasing function *I(t)*, its derivative is positive. The function *S(t)* continuously decreases as the number of infected network nodes increases. Thus, for the onset of an epidemic to occur, the following condition must be met:

$$S(0) > \frac{\gamma}{\beta} \equiv \rho. \tag{2}$$

The value of γ is a characteristic of the delay in the reaction of an information security specialist to an incident that entails the need to download the necessary "patches", β is an indicator of improving the technical characteristics of the network and the capabilities of the intruder. Thus, the intruder has the ability to pause in the reproduction cycle to avoid the situation of creating catastrophically growing traffic, which reduces the infection rate. In real conditions, by installing anti-virus software, firewalls and "patches", not only network nodes that are infected (I), but also sensitive ones (S) acquire "immunity".

Let's simplify the model. Assuming the average immunization rate to be approximately the same for nodes of these types and equal to a small value of γ, we obtain:

$$\begin{cases} \dfrac{dI(t)}{dt} = \beta I(t)(1 - R(t) - I(t)) - \gamma I(t), \\ \dfrac{dR(t)}{dt} = \gamma(1 - R(t)). \end{cases} \tag{3}$$

Taking into account the conditions for the development of the epidemic, we obtain:

$$R(t) = 1 - e^{-\gamma t}. \tag{4}$$

It follows from expression (4) that in the case when the time is long enough, it is theoretically possible to overcome the epidemic. However, the time may be unacceptably long.

Figure 2 shows the graphs of the dynamics of the development of the epidemic for given values of the parameters: $I(0) = I_0 = 0.01, R(0) = R_0 = 0, T = 10.$

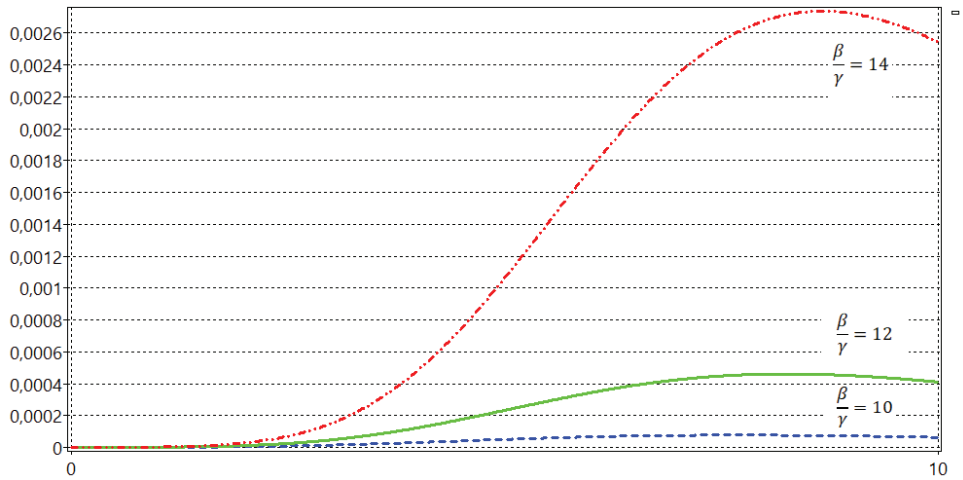

Fig. 2. The dynamics of the epidemic development according to model (3).

When "vaccinating" sensitive network nodes, in order for a noticeable epidemic outbreak to occur, when the system passes the outbreak threshold I_{thr} during an order of magnitude $\frac{1}{\gamma}$, it is required that the infection rate be two orders of magnitude or more higher than the immunization rate [10].

Since, in real conditions, immunization of uninfected nodes is much slower, and no patches are installed on some hosts with a removed worm, then due to the connection of nodes of a distributed IP video surveillance system to the Internet, new vulnerable nodes appear, which can lead to repeated epidemic outbreaks.

Let α be the growth rate of new vulnerable nodes in an IP video surveillance system connected to the Internet. Then the dynamics of the behavior of a system with a variable number of nodes is described by a system of differential equations of the following form:

$$\begin{cases} \frac{dS(t)}{dt} = -\beta I(t) - (\gamma + \alpha)S(t) + \alpha, \quad S(0) = S_0, \\ \frac{dI(t)}{dt} = \beta I(t)S(t) - (\gamma + \alpha)I(t), \quad I(0) = I_0, \\ \frac{dR(t)}{dt} = \gamma(1 - R(t)) - \alpha R(t), \quad R(0) = R_0. \end{cases} \tag{5}$$

The conditions for the development of the epidemic in this case take the form:

$$S(t) > \frac{\gamma + \alpha}{\beta}. \tag{6}$$

Graphs of the trajectories of system (5) are shown in Figure 3.

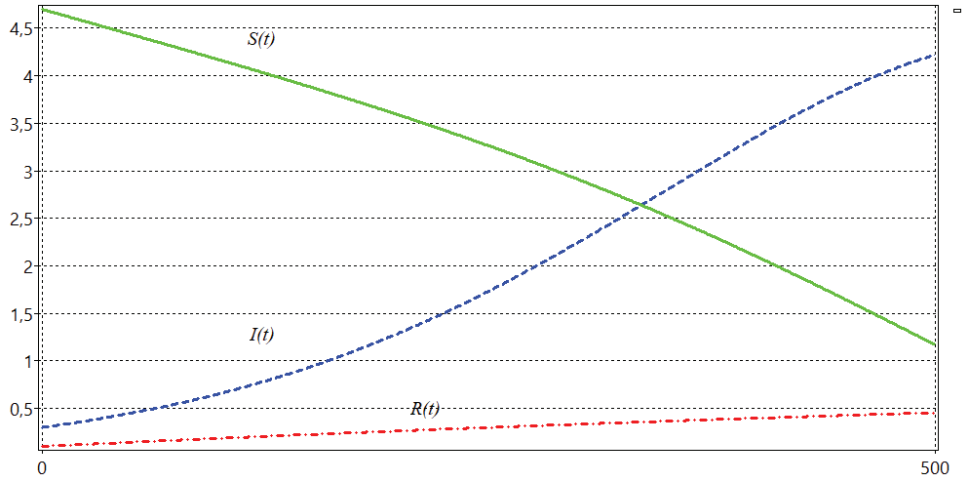

Fig. 3. The dynamics of the epidemic development according to model (5).

2.3 The problem of optimal control of IP video surveillance network protection from viruses

To build a system of protection against destructive influences, we introduce a control action equal to the coefficient $\gamma = \gamma(t)$ into the epidemic spread process, considering it as a piecewise-continuous control function at $t \in [0, T]$ that satisfies the constraint:

$$0 \le \gamma(t) \le Y_{\max}. \tag{7}$$

where Y_{max} is the maximum control rate, which characterizes the technical and economic capabilities of the company for the organization of information protection of the IP video surveillance system.

3 Results and discussion

The goal of control in the problem under consideration is to minimize the functional expressing the number of system nodes immune to infection at the final time T. So, assuming as a necessary condition that the majority of IP video surveillance network nodes (for example, more than 85%) at the final time were resistant to infection, we obtain the following problem of optimal control of the process of protecting the system from viruses: it is required to minimize the functionality

$$J(\gamma) = A \max\left\{(0.85N(T) - R(T)), 0\right\}^2 \to \min, \tag{8}$$

where *N(T)=S(T)+I(T)+R(T)* is the number of hosts in the IP video surveillance system at the end time, A>0 is the penalty factor, under dynamic and initial conditions (5), control constraint (7).

To solve this problem, its discrete approximation can be applied using explicit difference schemes and numerical trajectories can be constructed [11].

The complexity of the mathematical apparatus used in analytical modeling is associated with the unpredictability and random nature of the processes that occur during computer worm outbreaks. The characteristic properties of the process that one has to deal with in the analytical description include periods of inactivity in the worm's life cycle or its adaptive behavior. To take into account stochastic phenomena in the model and compensate them, we introduce process control into the model using an artificial neural network – neurocontrol [12]. The need to use artificial neural network (ANN) control technologies is caused by the presence of uncontrolled noise and interference in a real system, which must be compensated for in order to obtain an optimal network protection strategy.

A feature of the new model is that it considers an adaptive control system in which, in addition to classical control, neurocontrol is used, which allows you to adjust the control strategy in the presence of interference, noise, additional random factors that affect the construction of an optimal strategy for protecting the IP video surveillance system from the spread of destructive impacts. This approach makes it possible to build an adaptive protection system capable of promptly responding to an information security threat and effectively protecting the system from malware infection outbreaks.

Let us introduce the notation:

$$S(t) = x_1(t), I(t) = x_2(t), R(t) = x_3(t),$$

$$S(0) = x_1^0, I(0) = x_2^0, R(0) = x_3^0,$$

$$\beta_1(t, \gamma(t), x_1(t), x_2(t), x_3(t)) = -\beta x_2(t) - (\gamma(t) + \alpha)x_1(t) + \alpha,$$

$$\beta_2(t, \gamma(t), x_1(t), x_2(t), x_3(t)) = \beta x_2(t)x_1(t) - (\gamma(t) + \alpha)x_2(t),$$

$$\beta_3(t, \gamma(t), x_1(t), x_2(t), x_3(t)) = \gamma(t)(1 - x_3(t)) - \alpha x_3(t).$$

Taking into account the input of an artificial neural network (multilayer perceptron) into the process, the dynamics of the controlled object under consideration can be described by a system of differential equations with a retarded argument:

$$\dot{x}_i(t) = \beta_i(t, \gamma(t), x_1(t), x_2(t), x_3(t)) + F_i\left(\sum_{i=1}^{3} w_{ij}(t)x_j(t - h_j) - Q_i\right) + \\ + G_i\left(\sum_{i=1}^{3} w_{ij}(t)x_j(t) - \psi_i\right) + \sum_{i=1}^{3} b_{ij}(t)u_j(t), \tag{9}$$

where $i=1,..,3$, $t \in [0, T]$, $w_{ij}(t)$ – artificial neural network weights, $\sum_{i=1}^{3} w_{ij}(t)x_j(t - h_j)$ – total impact of a neural network with a delay on a neuron with an index i, Q_i, ψ_i – given quantities, in the general case, depending on time. In the proposed formulation of the problem, $\beta_i(t, x_i(t))$ describes the dynamics of an uncontrolled process, $\sum_{i=1}^{3} b_{ij}(t)u_j(t)$ is a classical control action, the term $F_i\left(\sum_{i=1}^{3} w_{ij}(t)x_j(t - h_j) - Q_i\right)$ introduces control of a dynamic system by means of an ANN with a delay, Q_i is a shift of the argument, and the function F_i is a differentiable activation function. If there is no delay in the control of the system by means of a neural network, the activation function $G_i\left(\sum_{i=1}^{3} w_{ij}(t)x_j(t) - \psi_i\right)$ is used, where ψ_i is the value of the shift of the argument.

4 Conclusion

Using the proposed approach, it is possible to build a cybersecurity management model for an IP video surveillance system based on machine learning in order to create a decision

support environment for preventing and eliminating threats, which makes it possible to create an adaptive protection system to detect and suppress network epidemics at an early stage, which increases the reliability of the functioning of distributed IP video surveillance systems as part of departmental situational centers.

References

1. V.M. Chibunin, Modern scientist **5**, 274-278 (2020)
2. S.A. Grechany, S.A. Romanov, Security, security, communications **6-1**, 20-24 (2021)
3. D.Y. Churakov, E.G. Tsarkova, T.Y. Vorotnikova, A.K. Belyaev, Journal of Physics: Conference Series: Applied Mathematics, Computational Science and Mechanics, 012113 (2020)
4. N.A. Semykina, I.A. Shapovalova, *Mathematical models in information security: an educational and methodological manual* (Tver State University, Tver, 2020)
5. L.A. Kunizheva, Modeling, optimization and information technologies **7.4(27)**, 45-46 (2019)
6. M.M. Williamson, *Biologically inspired approaches to computer security* (HP Labs Technical Report HPL-2002-131, HP Labs Bristol, UK, 2002)
7. V. Levtsov, N. Demidov, System administrator **4(161)**, 36-39 (2016)
8. C.C. Zou, W. Gong, D. Towsley, *Code Red worm propagation modeling and analysis* (9th ACM Symposium on Computer and Communication Security, Washington DC, 2002)
9. S. Staniford, V. Paxson, N. Weaver, *How to own the Internet in your spare time* (11th Usenix Security Symposium, San Francisco, 2002)
10. A. Zakharchenko, Information protection. Confidant **2**, 50-55 (2004)
11. M.O. Golubev, IFAC-PapersOnLine, 202-205 (2015)
12. E.A. Andreeva, L.G. Kozheko, *Prospects for the development of mathematical education in the era of digital transformation: Materials of the II All-Russian Scientific and Practical Conference* (Tver State University, Tver, 2021)