MATHEMATICAL MODEL OF THE RELIABILITY OF INFORMATION PROTECTION WITH LAYERED SECURITY SYSTEM. INTRODUCTION

A. I. Pereguda
•
Obninsk Institute for Nuclear Power
Engineering, Obninsk, Russia

e-mail: pereguda@iate.obninsk.ru

ABSTRACT

The article describes a mathematical model of reliability of the information system security systems consisting of object information protection and security of the two systems. The functioning process of the studied information security system is described as a superposition of alternating renewal processes. Upper and lower bounds for the expectation of time before unauthorized access to information.

Keywords: reliability, security system, random variables, time to failure, random process, the expectation of the time, distribution function.

1. INTRODUCTION

When building a highly reliable security systems often used layered threat protection. To protect data from unauthorized access is required to provide a certain level of reliability of such systems, including the reliability of their hardware and software. When analyzing the reliability of such systems is not enough just to take into account the structure of the security system. Mathematical models of reliability of information protection systems considered in various works, such as [1, 2]. It is also necessary to take into account the reserve time available in security systems, which arises from the fact that to overcome the successive layers of protection attacker will take some time .Here we obtain relations to assess how this extra time is a reliability of information security.

2. DESCRIPTION OF THE MODEL

Let an information system which consists of a protection and safety of the two systems, each of which saves one of the varieties to attack protection. Security systems are not foolproof and may refuse. It is assumed that the failures of safety systems are independent. Failure detection security systems occurs only during periodic monitoring her condition. After failure detection security system performed its full restoration to its original state. If the first security system was not immediately able to parry, the unauthorized access to information can only be achieved after a while though, and only provided that during this time, none of the safety systems failed.

Denote χ_1- a random time before the first attack on the object of protection, detectable first security system. Random time reflection of the first attack on the object of protection, the detected first security system, denoted γ_1. Then a random time before the second attack on the object of protection after the first attack, the reflection of the first security system detected a protection object denoted χ_2, after reflection the second attack - χ_3 etc. We assume that all χ_i, $i = 1, 2, \ldots$, as usual, are independent and identically distributed with the distribution function $F_\chi(t) = P(\chi \le t)$.

Random time of reflection on the i attack to protect, detect the first security system will be denoted γ_i, $i = 1, 2, \ldots$,, as to which assume that - γ_i, $i = 1, 2, \ldots$ independent identically distributed random variables with distribution function $F_\gamma(t) = P(\gamma \le t)$.Denote δ_i a random time between the i attack on the object of protection, which was not detected the first security system, and unauthorized access. It is obvious that δ_i, $i = 1, 2, \ldots$, - independent identically distributed random variables with distribution function $F_\delta(t) = P\{\delta \le t\}$. Thus, the first security system can still prevent unauthorized access time interval $[\chi_i, \chi_i + \delta_i)$

Since the process of operation of the first security system consists of cycles "attack - a reflection attack", and, consequently, the moments of the completion of attack to protect, detect the first security system are regenerative information system.

If the first security system and has not worked in the specified time interval, the second security system can still prevent unauthorized access at the moment $\chi_i + \delta_i$. The duration of the second reflection attack security system after the first attack is denoted α_1, after the second attack - α_2, etc. Believe that α_i, $i = 1, 2, \ldots$- independent identically distributed random variables with distribution function $F_\alpha(t) = P\{\alpha \le t\}$.

Random time before the i attack on the object of protection, security system detects a second denote φ_i, $i = 1, 2, \ldots$.Let φ_i, $i = 1, 2, \ldots$- independent identically distributed random variables with distribution function $F_\varphi(t) = P\{\varphi \le t\}$. Duration reflection i-attack on the object of protection, which was discovered a second security system, denoted ψ_i, $i = 1, 2, \ldots$. Believe that ψ_i, $i = 1, 2, \ldots$ - independent identically distributed random variables with distribution function $F_\psi(t) = P\{\psi \le t\}$. Assume that the end points of reflection of such attacks are regenerative process of information system. Moreover, let the expectations χ_i, $i = 1, 2, \ldots$, γ_i, $i = 1, 2, \ldots$, δ_i, $i = 1, 2, \ldots$, α_i, $i = 1, 2, \ldots$, φ_i, $i = 1, 2, \ldots$and ψ_i, $i = 1, 2, \ldots$, exist and are finite .

Since the process of reflection attacks consists of cycles "attack - a reflection attack", and, consequently, the moments of the completion of the attack on the object of protection, first detected as a security system, and the second system security are regenerative information system.

We now consider the processes of safety systems. Let $\xi_i^{(1)}$, $i = 1, 2, \ldots$ for the i time between failure of the first security system. We assume that the time to failure of the first security system $\xi_i^{(1)}$, $i = 1, 2, \ldots$ - independent identically distributed random variables with distribution function $F_{\xi_i^{(1)}}(t) = P\{\xi_i^{(1)} \le t\}$. Duration of the first system restore security after the i-failure is denoted $\eta^{(1)}$, $i = 1, 2, \ldots$ Here $\eta^{(1)}$, $i = 1, 2, \ldots$– independent identically distributed random variables with distribution function $F_{\eta_i^{(1)}}(t) = P\{\eta_i^{(1)} \le t\}$. Fault detection security systems occurs only during periodic condition monitoring. So serviceability first security system update to the period $T^{(1)}$ and the duration of the periodic control requires time equal $\theta^{(1)}$.

If the first security system (SS) functioned properly random time $\xi^{(1)}$, for this time $\left[\frac{\xi^{(1)}}{T^{(1)} + \theta^{(1)}}\right]$ period was performed preventive control, and during these periods the first SS was operational $T^{(1)}\left[\frac{\xi^{(1)}}{T^{(1)} + \theta^{(1)}}\right]$ units of time. Between the last before giving up control prevention,

which occurred at the time $(T^{(1)}+\theta^{(1)})\left[\frac{\xi^{(1)}}{T^{(1)}+\theta^{(1)}}\right]$, and the denial of time $\xi^{(1)}$ is still time $\xi^{(1)}-(T^{(1)}+\theta^{(1)})\left[\frac{\xi^{(1)}}{T^{(1)}+\theta^{(1)}}\right]$, during which the first SS is still OK.

On the last loop prevention control security system is idle time $(T^{(1)}+\theta^{(1)})-(T^{(1)}+\theta^{(1)})\left\{\frac{\xi^{(1)}}{T^{(1)}+\theta^{(1)}}\right\}$, because rejection has occurred in its time $\xi^{(1)}$, but was detected after the cycle test prophylaxis. Failure of the first security system will be detected in time $(T^{(1)}+\theta^{(1)})\left(\left[\frac{\xi^{(1)}}{T^{(1)}+\theta^{(1)}}\right]+1\right)$, and after the repair work lasting $\eta^{(1)}$ SS starts functioning correctly again.

Believe $\xi_i^{(2)}$, $i=1,2,\ldots$ – time between i-failure of the second-security, where $\xi_i^{(2)}$, $i=1,2,\ldots$ are independent and identically distributed random variables with distribution function $F_{\xi_i^{(2)}}(t)=P\left\{\xi_i^{(2)}\le t\right\}$. Duration of recovery the second security system after i-failure denote $\eta_i^{(2)}$, $i=1,2,\ldots$, where $\eta_i^{(2)}$, $i=1,2,\ldots$

then independent identically distributed random variables with distribution function $F_{\eta_i^{(2)}}(t)=P\left\{\eta_i^{(2)}\le t\right\}$.

Monitor the status of the second period the security system is denoted $T^{(2)}$, and the duration of its periodic monitoring – $\theta^{(2)}$. Failure of the second security system is detected in time $(T^{(2)}+\theta^{(2)})\left(\left[\frac{\xi^{(2)}}{T^{(2)}+\theta^{(2)}}\right]+1\right)$. After the repair work with duration equal to $\eta^{(2)}$ the second SS will again operate correctly. Thus, the processes of the functioning of the first and second security system to control prevention have alternating renewal process. Here we assume that during the control state security not perform their functions .

Moreover, let the expectations $\xi_i^{(1)}$, $i=1,2,\ldots$, $\eta_i^{(1)}$, $i=1,2,\ldots$, $\xi_i^{(2)}$, $i=1,2,\ldots$and $\eta_i^{(2)}$, $i=1,2,\ldots$ exist and are finite, and the distribution function of these random variables are not arithmetic.

Functioning processes of the first and second security systems appears as alternating intervals "work - restoration", which consist of independent, identically distributed random variables $\left\{\xi_i^{(1)}, i\ge 1\right\}$, $\left\{\eta_i^{(1)},\ i\ge 1\right\}$и $\left\{\xi_i^{(2)}, i\ge 1\right\}$, $\left\{\eta_i^{(2)},\ i\ge 1\right\}$ forming two alternating renewal process $\left\{(\xi_i^{(1)},\eta_i^{(1)}),\ i\ge 1\right\}$ and $\left\{(\xi_i^{(2)},\eta_i^{(2)}),\ i\ge 1\right\}$..

We introduce some notation and explanations of the process of preventive control, which will be further taken into account in the mathematical model. Through $[x]$ and $\{x\}$ denote the integral and fractional parts of a number x, $x^+=max(x,0), x\wedge a=min(x,a)$, $J_{x<a}$ — indicator of the event $x<a$.

Random time to unauthorized access denoted ω. Our task is to construct a mathematical model of reliability of information security systems with layered security system and obtain an estimate of the average time $M\omega$ to unauthorized access to information.

3. MAIN RESULTS

Since the process of functioning of the system of protection of information is described as a superposition of alternating renewal processes, the random time to unauthorized access can be written as the sum of the following:

$$\omega = \sum_{i=1}^{\nu-1} \sigma_i + \sigma'_\nu , \tag{1}$$

where the duration of the regeneration process, the information system, which has not happened unauthorized access, equal

$$\sigma_i = \chi_i \wedge \varphi_i + \left((\beta_i + \gamma_i) J_{B_i} + (\delta_i + \alpha_i) J_{\overline{B}_i} \right) J_{\chi_i \le \varphi_i} + \psi_i J_{\varphi_i < \chi_i} ,$$

and duration of the regeneration process, the information system, which occurred unauthorized access, equal

$$\sigma'_i = \chi_i \wedge \varphi_i + \delta_i J_{\chi_i \le \varphi_i} .$$

In relation σ_i use the following notation: β_i - the length of time between the implementation of an attack on the object of protection, which should be parried the first security system, and actuation of this safety system, provided that it was able to parry; B_i -the event consists in the fact that the regeneration of the i-cycle process, the information system for the implementation of attack corresponding to the first security system, the security system retorted this wave in the time interval $\left[\sum_{j=1}^{i-1} \sigma_i + \chi_i , \sum_{j=1}^{i-1} \sigma_i + \chi_i + \delta_i \right)$; $\overline{B}_i$ - denotes the opposite event - first security system is not countered this attack on the object of protection in that time interval. For this model, it is obvious $0 \le \beta_i < \delta_i$.

For the distribution function of time to unauthorized access, obviously, we have the following relationship:

$$F_\omega(t) = P(\omega \le t) = P\left(\sum_{i=1}^{\nu-1} \sigma_i + \sigma'_\nu \le t \right).$$

For further transformations of $F_\omega(t)$ we use the method of conditional probability distributions and express complex events through the conditional probability of this event under the appropriate conditions. If the conditions are incompatible and form a complete group of events, the absolute transformation of the distribution function $F_\delta(t)$ for the total probability formula

$$\widetilde{F}_\omega(s) = Me^{-s\omega} = \sum_{n=1}^{\infty} M\left(e^{-s\omega} \mid \nu = n \right) P(\nu = n) ,$$

where $\widetilde{F}_\omega(s) = \int_0^\infty e^{-st} dF_\omega(t) = E\left[e^{-s\omega} \right]$.

Since all χ_i and γ_i are independent random variables, given that $\widetilde{F}_\sigma(s) = Me^{-s\sigma}$ and $\widetilde{F}_{\sigma'}(s) = Me^{-s\sigma'}$, and the process in the regeneration, the $P(\nu = n) = q(1-q)^{n-1}$, where q - likelihood of unauthorized access to the regeneration process, the information system. Easy to see that

$$M\left(e^{-s\omega} \mid \nu = n\right) = M\left(e^{-s\left(\sum_{i=1}^{\nu-1}\sigma_i + \sigma'_\nu\right)} \middle| \nu = n \right) = \left(\widetilde{F}_\sigma(s)\right)^{n-1} \widetilde{F}_{\sigma'}(s).$$

Consequently, the Laplace-Stieltjes $F_\omega(t)$ rewrite

$$\widetilde{F}_\omega(s) = \sum_{n=1}^{\infty} \left(\widetilde{F}_\sigma(s)\right)^{n-1} \widetilde{F}_{\sigma'}(s) q(1-q)^{n-1} = \frac{q\widetilde{F}_{\sigma'}(s)}{1-(1-q)\widetilde{F}_\sigma(s)}.$$

Expression for the expectation of time before unauthorized access can be directly calculated from the ratio of (1) or by using the well-known relation $M\omega = -\left.\frac{d\widetilde{F}_\omega(s)}{ds}\right|_{s=0}$. We obtain

$$M\omega = M\sigma' + \frac{1-q}{q} M\sigma. \qquad (2)$$

To find the expectation of use of the complex to the first accident is necessary to calculate separately the expectations $M\sigma'$ and $M\sigma$. In calculating the expectation $M\sigma'$, we consider that these random variables are mutually independent. Then, the mathematical expectation $M\sigma'$, we can write as follows:

$$M\sigma' = M((\chi \wedge \varphi) + \delta J_{\chi \le \varphi}) = M(\chi \wedge \varphi) + M\delta P(\chi \le \varphi) =$$

$$= \int_0^\infty (1 - F_\chi(t))(1 - F_\varphi(t)dt + \int_0^\infty (1 - F_\delta(t))dt \int_0^\infty F_\chi(t)dF_\varphi(t).$$

By analogy with $M\sigma'$ compute the expectation σ, which is equal to

$$M\sigma = M((\chi \wedge \varphi) + ((\beta + \gamma)J_B + (\delta + \alpha)J_{\overline{B}})J_{\chi \le \varphi} + \psi J_{\chi > \varphi}) = M(\chi \wedge \varphi) +$$

$$+ M((\beta + \gamma)J_B + (\delta + \alpha)J_{\overline{B}})J_{\chi \le \varphi}) + M(\psi J_{\chi > \varphi}) = \int_0^\infty (1 - F_\chi(t))(1 - F_\varphi(t)dt +$$

$$+ P(\chi \le \varphi)((M\beta + M\gamma)P(B) + (M\delta + M\alpha)P(\overline{B})) + M\psi P(\varphi < \chi).$$

Substituting the calculated expectations $M\sigma'$ and $M\sigma$ in (2) we have

$$M\omega = M(\chi \wedge \varphi) + \delta J_{\chi \le \varphi}) + \frac{1-q}{q} M((\chi \wedge \varphi) + ((\beta + \gamma)J_B + (\delta + \alpha)J_{\overline{B}})J_{\chi \le \varphi} + \psi J_{\chi > \varphi}).$$

Note that the record of the distribution function for the random variables β_i, which depend on the magnitude of σ_i, it is not possible, but it is possible to obtain upper and lower bounds for the expectation of time before unauthorized access to information by using the order relation on the set of distribution functions [3]. This assessment is written as follows:

$$M\sigma' + \frac{1-q}{q}\left(M(\chi \wedge \varphi) + \left(M\gamma P(B) + (M\delta + M\alpha)P(\overline{B})\right)P(\chi \le \varphi)\right) + M\psi P(\varphi < \chi) \le M\omega \le \qquad (3)$$

$$\le M\sigma' + \frac{1-q}{q}\left(M(\chi \wedge \varphi) + \left((M\delta + M\gamma)P(B) + (M\delta + M\alpha)P(\overline{B})\right)P(\chi \le \varphi)\right) + M\psi P(\varphi < \chi).$$

In order to calculate the upper and lower bounds, you must first assess the probability q unauthorized access to the regeneration process of the information system. To get an estimate of the probability of a closer look at the processes of the safety systems [3,6].

Consider a single cycle of the functioning of the information system and compute $P(\overline{B})$, by considering two auxiliary random variables $\mathrm{U_n}$ and $\mathrm{V_n}$,, defined by the relations

$$U_n = \sum_{i=1}^{n} \xi_i^{(1)} + \sum_{i=1}^{n-1} \left((T^{(1)} + \theta^{(1)}) - \left\{ \frac{\xi_i^{(1)}}{T^{(1)} + \theta^{(1)}} \right\} (T^{(1)} + \theta^{(1)}) \right) + \sum_{i=1}^{n-1} \eta_i^{(1)},$$

$$V_n = \sum_{i=1}^{n} \xi_i^{(1)} + \sum_{i=1}^{n} \left((T^{(1)} + \theta^{(1)}) - \left\{ \frac{\xi_i^{(1)}}{T^{(1)} + \theta^{(1)}} \right\} (T^{(1)} + \theta^{(1)}) \right) + \sum_{i=1}^{n} \eta_i^{(1)},$$

Where U_n - the time of n-failure of the first security, and V_n - the end of the first security system recovery after an-failure.

Because the process is functioning security system is alternating renewal process, we can write

$$U_n = \sum_{i=1}^{n} \xi_i^{(1)} + \sum_{i=1}^{n-1} \left((T^{(1)} + \theta^{(1)}) - \left\{ \frac{\xi_i^{(1)}}{T^{(1)} + \theta^{(1)}} \right\} (T^{(1)} + \theta^{(1)}) \right) + \sum_{i=1}^{n-1} \eta_i^{(1)},$$

$$V_n = \sum_{i=1}^{n} \xi_i^{(1)} + \sum_{i=1}^{n} \left((T^{(1)} + \theta^{(1)}) - \left\{ \frac{\xi_i^{(1)}}{T^{(1)} + \theta^{(1)}} \right\} (T^{(1)} + \theta^{(1)}) \right) + \sum_{i=1}^{n} \eta_i^{(1)}.$$

Then unauthorized access to the cycles of regeneration process, the information system provided if

$$U_n \le \chi < V_n - \delta,\ \delta \le V_n - U_n,$$

or if

$$V_{n-1} + T^{(1)} \le \chi < V_{n-1} + T^{(1)} + \theta^{(1)} - \delta;$$

$$V_{n-1} + (T^{(1)} + \theta^{(1)}) + T^{p} \le \chi < V_{n-1} + 2(T^{p} + \theta^{p}) - \delta;$$

$$\dots$$

$$V_{n-1} + \left(\left[\frac{\xi_n^{(1)}}{T^{(1)} + \theta^{(1)}} \right] - 1 \right) (T^{(1)} + \theta^{(1)}) + T^{(1)} \le \chi < V_{n-1} + \left[\frac{\xi_n^{(1)}}{T^{(1)} + \theta^{(1)}} \right] (T^{(1)} + \theta^{(1)}) - \delta;$$

$$\delta < \theta^{(1)}.$$

For further exposition must enter non-negative random variables

$$\varepsilon_n = (T^{(1)} + \theta^{(1)}) - \left\{ \frac{\xi_n^{(1)}}{T^{(1)} + \theta^{(1)}} \right\} (T^{(1)} + \theta^{(1)})$$

$$\Delta_n = \eta_n^{(1)} + \varepsilon_n - \delta,\ \zeta = \theta^{(1)} - \delta,$$

Here ε_n - the length of time from the moment of first refusal to security failure detection and recovery is started.

Taking into account the circumstances of the unauthorized access to information, write the expression for the probability of $P(\overline{B})$:

$$P(\overline{B}) = \sum_{n=1}^{\infty} \int_0^{\infty} M \left(J_{U_n \le x < V_n - \delta} J_{\Delta_n > 0} + \sum_{i=1}^{\left[\frac{\xi_n^{(1)}}{T^{(1)} + \theta^{(1)}} \right]} J_{V_{n-1} + (i-1)(T^{(1)} + \theta^{(1)}) \le x < V_{n-1} + i(T^{(1)} + \theta^{(1)}) - \delta} J_{\zeta > 0} \right) dF_{\chi}(x).$$

It follows that

$$P(\overline{B}) = \sum_{n=1}^{\infty}\int_0^{\infty} P\{U_n \wedge (U_n + \Delta_n) \le x\} dF_\chi(x) - \sum_{n=1}^{\infty}\int_0^{\infty} P\{U_n + \Delta_n \le x\} dF_\chi(x) +$$

$$+ \sum_{n=1}^{\infty}\int_0^{\infty} M\left\{ \sum_{i=1}^{\left[\frac{\xi_n^{(1)}}{T^{(1)}+\theta^{(1)}}\right]} P\{(V_{n-1} + i(T^{(1)}+\theta^{(1)}) - \theta^{(1)}) \wedge (V_{n-1} + i(T^{(1)}+\theta^{(1)}) - \theta^{(1)} + \zeta) \le x\} \right\} dF_\chi(x) -$$

$$- \sum_{n=1}^{\infty}\int_0^{\infty} M\left\{ \sum_{i=1}^{\left[\frac{\xi_n^{(1)}}{T^{(1)}+\theta^{(1)}}\right]} P\{V_{n-1} + i(T^{(1)}+\theta^{(1)}) - \theta^{(1)} + \zeta \le x\} \right\} dF_\chi(x) = q_1 + q_2.$$

Note that

$$q_1 = \sum_{n=1}^{\infty}\int_0^{\infty}\int_0^{\infty} \left((F_{\xi^{(1)}} * (F_{\xi^{(1)}} * F_{\eta^{(1)}} * F_\varepsilon)^{*(n-1)})(x) - (F_{\xi^{(1)}} * (F_{\xi^{(1)}} * F_{\eta^{(1)}} * F_\varepsilon)^{*(n-1)})(x-y) \right) dF_\Delta(y) dF_\chi(x),$$

where $F_{\xi^{(1)}} * F_{\eta^{(1)}}(t) = \int_0^t F_{\xi^{(1)}}(t-z) dF_{\eta^{(1)}}(z)$ – convolution of the distribution functions $F_{\xi^{(1)}}(t)$ and $F_{\eta^{(1)}}(t)$, $F^{*(n)}(t) = F * F^{*(n-1)}(t)$ – n-fold convolution of functions $F(t)$.

Probability q_1

$$q_1 = \int_0^{\infty}\int_0^{\infty} (H_0(x) - H_0(x-y))\, dF_\Delta(y) dF_\chi(x),$$

where $H_0(x) = \sum_{n=1}^{\infty} F_{\xi^1} * (F_{\xi^1} * F_{\eta^1} * F_\varepsilon)^{*(n-1)}(x)$ - 0-function recovery process operation of the first security system. The second term is converted analogously

$$q_2 = \sum_{n=1}^{\infty}\int_0^{\infty}\int_0^{\infty} M\left\{ \sum_{i=1}^{\left[\frac{\xi_n^{(1)}}{T^{(1)}+\theta^{(1)}}\right]} \left(P(V_{n-1} + i(T^{(1)}+\theta^{(1)}) - \theta^{(1)} \le x) - P(V_{n-1} + i(T^{(1)}+\theta^{(1)}) - \theta^{(1)} \le x-y) \right) \right\} dF_\xi(y) dF_\chi(x)$$ The resulting

expression can be written using functions 0-recovery:

$$q_2 = \int_0^{\infty}\int_0^{\infty} M\left\{ \sum_{i=1}^{\left[\frac{\xi^{(1)}}{T^{(1)}+\theta^{(1)}}\right]} \left(H_{0i}(x) - H_{0i}(x-y) \right) \right\} dF_\xi(y) dF_\chi(x),$$

where $H_{0i}(x) = \sum_{n=1}^{\infty} F_{2i,n}(x)$, and $F_{2i,n}(x) = P(V_{n-1} + i(T^{(1)}+\theta^{(1)}) - \theta^{(1)} \le x)$..

Further simplify the obtained relations is not possible, but you can get the asymptotic estimates, using the limit theorems of renewal theory [4,5]:

$$q_1 \approx \frac{1}{M\eta^{(1)} + (T^{(1)} + \theta^{(1)})M\left(\left[\frac{\xi^{(1)}}{\mathrm{T}^{(1)} + \theta^{(1)}}\right] + 1\right)} \int_0^\infty y dF_\Delta(y) = \tag{4}$$

$$= \frac{\left(M\eta^{(1)} + (T^{(1)} + \theta^{(1)}) + M\left\{\frac{\xi^{(1)}}{\mathrm{T}^{(1)} + \theta^{(1)}}\right\}(T^{(1)} + \theta^{(1)} - \delta)\right)^+}{M\eta^{(1)} + (T^{(1)} + \theta^{(1)})M\left(\left[\frac{\xi^{(1)}}{\mathrm{T}^{(1)} + \theta^{(1)}}\right] + 1\right)}$$

and

$$q_2 \approx \frac{M\left[\frac{\xi^{(1)}}{\mathrm{T}^{(1)} + \theta^{(1)}}\right]}{M\eta^{(1)} + (T^{(1)} + \theta^{(1)})M\left[\frac{\xi^{(1)}}{\mathrm{T}^{(1)} + \theta^{(1)}}\right] + (T^{(1)} + \theta^{(1)})} \int_0^\infty y dF_\zeta(y) = \tag{5}$$

$$= \frac{M\left[\frac{\xi^{(1)}}{\mathrm{T}^{(1)} + \theta^{(1)}}\right] M\left(\theta^{(1)} + \delta\right)^+}{M\eta^{(1)} + (T^{(1)} + \theta^{(1)})M\left[\frac{\xi^{(1)}}{\mathrm{T}^{(1)} + \theta^{(1)}}\right] + (T^{(1)} + \theta^{(1)})}.$$

Summing (5) and (4) we obtain the probability that the first security system is not to parry by protection time interval $[\chi, \chi + \delta)$

$$\mathrm{P}(\overline{\mathrm{B}}) \approx \frac{M\left(\eta^{(1)} + (T^{(1)} + \theta^{(1)}) - \left\{\frac{\xi^{(1)}}{T^{(1)} + \theta^{(1)}}\right\}(T^{(1)} + \theta^{(1)}) - \delta\right)^+}{M\eta^{(1)} + (T^{(1)} + \theta^{(1)}) + (T^{(1)} + \theta^{(1)})M\left[\frac{\xi^{(1)}}{T^{(1)} + \theta^{(1)}}\right]} +$$

$$+ \frac{\mathrm{M}\left[\frac{\xi^{(1)}}{T^{(1)} + \theta^{(1)}}\right]\mathrm{M}\left(\theta^{(1)} - \delta\right)^+}{\mathrm{M}\eta^{(1)} + (T^{(1)} + \theta^{(1)}) + (T^{(1)} + \theta^{(1)})\mathrm{M}\left[\frac{\xi^{(1)}}{T^{(1)} + \theta^{(1)}}\right]}.$$

Written explicitly $\int_0^\infty y dF_\Delta(y)$ and $\int_0^\infty y dF_\zeta(y)$ is quite difficult even for the relatively simple case of exponential distributions of random variables, but you can use the Monte - Carlo method to obtain the desired numerical estimates. Note also that

$$P(B) = 1 - P(\overline{B}).$$

Probability q unauthorized access to the regeneration process of the information system in accordance with the formula of total probability we can write

$$q = P\left(accident \text{ on the regenaration cycle}\Big|_{\chi\le\varphi}\right)P(\chi \le \varphi) +$$
$$+ P\left(accident \text{ on the regenaration cycle}\Big|_{\chi>\varphi}\right)P(\chi > \varphi) =$$
$$= q^{(1,2)}P(\chi \le \varphi) + q^{(2)}P(\chi > \varphi) = q^{(1,2)}\int_0^\infty F_\chi(t)dF_\varphi(t) + q^{(2)}\left(1 - \int_0^\infty F_\chi(t)dF_\varphi(t)\right),$$

Where $q^{(1,2)}$ - it's likely that the first regeneration cycle, followed by a second security system will not be able to parry, and $q^{(2)}$ - the likelihood that the second regeneration cycle security system will not be able to fend off the corresponding type of attack. Taking into account that the safety systems are independent from each other, we can write

$$q^{(1,2)} = P(\overline{B})q^{(2)}.$$

And finally, the estimate for the probability of $q^{(2)}$ can be obtained using the same approach that was used in calculating the above mentioned $P(\overline{B})$. Omit the intermediate calculations and present the final result immediately:

$$q^{(2)} \approx 1 - \frac{M\xi^{(2)} - \theta^{(2)}M\left[\dfrac{\xi^{(2)}}{T^{(2)}+\theta^{(2)}}\right]}{M\eta^{(2)} + (T^{(2)}+\theta^{(2)}) + (T^{(2)}+\theta^{(2)})M\left[\dfrac{\xi^{(2)}}{T^{(2)}+\theta^{(2)}}\right]}$$

Note that $q^{(2)}$ - factor unavailability second security system that takes the minimum value during the control period with optimal prevention $T_{onm}^{(2)}$ [6].

Optimal prevention period determined by the formula

$$T_{onm}^{(2)} = \sqrt{2\theta^{(2)}(M\xi^{(2)} + M\eta^{(2)})}$$

Thus, we managed to get the upper and lower asymptotic bounds (3) for the mean time to unauthorized access.

The proposed mathematical model of reliability of information security systems with layered security system with recoverable elements allows to take into account the temporal redundancy, when one security system "insures" the other. The proposed two-sided estimate for the expectation to unauthorized access to information provides a fairly narrow range of values for this indicator system reliability, simply calculated and takes into account a large number of different parameters of functioning of the system of information protection. The relations obtained are valid without any assumptions regarding the distribution functions of random variables.

REFERENCES

1. Corneliussen, K. & Hokstad, P. 2003. *Reliability Prediction Method for Safety Instrumented Systems; PDS Method Handbook, 2003 Edition.* SINTEF report STF38 A02420, SINTEF, Trondheim, Norway.

2. Gnedenko, B.V., Ushakov, I.A. 1995. *Probabilistic Reliability Engineering*. John Wiley & Sons, Inc.

3. Pereguda, A.I. 2001. Calculation of the Reliability Indicators of the System Protected Object-Control and Protection System. *Atomic Energy* 90: 460-468.

4. Rausand, M., Høyland, A. 2004 *System Reliability Theory: Models, Statistical Methods and Applications.* John Wiley & Sons, Inc.

5. Stoyan, D. 1983 *Comparison Methods for Queues and Other Stochastic Models*. Wiley-Interscience.

6. Pereguda, A.I., Timashov D.A. Mathematical model of reliability of security information systems.// Information . — 2009. —№8. —c.10–17.