DOI: 10.51790/2712-9942-2022-3-1-5

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ НАДЕЖНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ С СИСТЕМАМИ БЕЗОПАСНОСТИ

А. И. Перегуда

Обнинский институт атомной энергетики — филиал федерального государственного автономного образовательного учреждения высшего профессионального образования «Национальный исследовательский ядерный университет «МИФИ», г. Обнинск, Российская Федерация

Pereguda@iate.obninsk.ru

Аннотация: статья посвящена созданию математической модели надежности информационных систем, состоящих из объекта защиты и систем безопасности. С целью получения несанкционированного доступа к объекту защиты предпринимаются различного рода атаки. Поскольку процесс функционирования рассматриваемой системы имеет стохастический характер, математической моделью является случайный процесс, представляющий собой наложение альтернирующих процессов восстановления. Анализ модели, рассматриваемой в этой статье, позволил получить асимптотические соотношения оценок: вероятность того, что на цикле регенерации рассматриваемого процесса аварии не было; среднее время наработки информационной системы до аварии.

Статья рассчитана на инженеров и математиков, занимающихся вопросами надежности систем, состоящих из объекта защиты и систем безопасности.

Ключевые слова: информационная система, функция распределения, система безопасности, останов, авария, альтернирующий процесс восстановления, среднее время наработки, цикл регенерации.

Для цитирования: Перегуда А. И. Математическая модель надежности информационных систем с системами безопасности. *Успехи кибернетики*. 2022;3(1):39–43. DOI: 10.51790/2712-9942-2022-3-1-5.

A SIMULATION MODEL OF IT SYSTEMS WITH SECURITY FEATURES

A. I. Pereguda

Obninsk Institute for Nuclear Power Engineering, a branch of the National Research Nuclear University MEPhI, Obninsk, Russian Federation

Pereguda@iate.obninsk.ru

Abstract: the paper covers the development of a simulation model for the reliability of IT systems consisting of a protected asset and a security module. There are various types of attacks to obtain unauthorized access to the protected asset. Since the system under consideration operates stochastically, the simulation model is a random process as overlapping of alternating recovery processes. We analyzed the proposed model and obtained asymptotic estimate ratios: the probability of no-accident state during the recovery stage of the process; IT system mean time between failures.

The paper is intended for engineers and mathematicians dealing with the reliability of systems consisting of a protected asset and a security module.

Keywords: information system, distribution function, security system, outage, accident, alternating recovery process, MTBF, recovery cycle.

Cite this article: Pereguda A. I. A Simulation Model of IT Systems with Security Features. *Russian Journal of Cybernetics*. 2022;3(1):39–43. DOI: 10.51790/2712-9942-2022-3-1-5.

Введение

Использование различных автоматизированных систем, построенных на базе вычислительной техники, сделало актуальной проблему надежности информационной безопасности. Для обеспечения защиты информации от несанкционированного доступа требуется обеспечить определенный уровень надежности таких систем, включая надежность их аппаратных средств и программного обеспечения. Математические модели надежности систем защиты информации рассматривались в различных работах, например в [1].

Рассмотрим вначале структуру предлагаемой модели. Будем считать, что информационная система состоит из объекта защиты и системы безопасности. Предполагается, что могут быть предприняты различные виды атак с целью получения несанкционированного доступа к объекту защиты. Система безопасности призвана парировать эти атаки, тем самым обеспечивая защиту от несанкционированного доступа. Отметим, что система безопасности не является абсолютно надежной, причем она может оказаться в неисправном состоянии из-за двух видов ее отказа, влияние которых необходимо учитывать. Во-первых, это *скрытые отказы*, при которых система теряет способность при необходимости вырабатывать адекватное защитное воздействие. Это такие отказы системы безопасности, которые не могут быть обнаружены без проведения профилактических мероприятий. Во-вторых, это ложные отказы, при которых система безопасности вырабатывает защитное воздействие без каких-либо причин, т.е. системы безопасности формирует ложные срабатывания, которые приводят к *останову* информационной системы. Заметим, что скрытые отказы и ложные срабатывания несовместны, т.е. они одновременно не могут быть реализованы. Таким образом, несанкционированный доступ к информации с использованием определенного класса атак возможен только тогда, когда атака приходится на период неработоспособности соответствующей подсистемы системы безопасности. Данное событие есть *авария* информационной системы.

Поскольку в такой сложной технической системе, какой является система безопасности, невозможно сразу обнаружить отказы отдельных подсистем, то для целей обнаружения неисправностей применяются различные диагностические процедуры, которые контролируют состояние подсистем в заданные моменты времени. Таким образом, необходимо рассматривать процедуру контрольных профилактик, которые выполняются не мгновенно. Структура подсистем системы безопасности, как правило, достаточно сложна. Поэтому необходимо также включить в рассмотрение структуры этих подсистем.

Целью данной работы является создание математической модели надежности информационной системы с системами безопасности с учётом контрольных профилактик. Поставленную задачу будем решать, используя методы, аналогичные тем, которые применяются в [2].

Введем следующие обозначения. Предполагаем, что имеется несколько типов атак и при этом атаки разных видов статистически независимы. Заметим, что после отражения атаки либо после восстановления исправного состояния после ложного срабатывания системы безопасности случайный процесс, соответствующий процессу функционирования, как бы возвращается в исходное состояние с теми же вероятностными характеристиками, что и в начальный момент времени, а это означает, что процесс генерации атак на систему и их парирования можно описать с помощью альтернирующего процесса восстановления. Также будем предполагать, что одновременное воздействие двух и более атак маловероятно, т.е. такие события являются практически невозможными событиями. Следует отметить, что хотя данные ограничения и являются, вообще говоря, достаточно строгими, но указанные предположения, как правило, выполняются.

Пусть случайные времена до очередной атаки i-го вида на каждом цикле рассматриваемого случайного процесса независимы и одинаково распределены с функцией $F_{\chi_i}(t)$. Соответственно, случайные времена отражения атаки i-го вида на каждом цикле рассматриваемого случайного процесса независимы и распределены с одной и той же функцией распределения $F_{\gamma_i}(t)$. Также будем предполагать, что все наработки i-ой подсистемы системы безопасности до ложного отказа φ_i на каждом цикле рассматриваемого случайного процесса так же независимы и одинаково распределены с функцией распределения $F_{\varphi_i}(t)$ и, наконец, все времена восстановления после ложного срабатывания i-ой подсистемы системы безопасности (СБ) ψ_i на каждом цикле рассматриваемого случайного процесса независимы и одинаково распределены с функцией распределения $F_{\psi_i}(t)$.

Структуру подсистем СБ по отношению к ложным отказам будем учитывать следующим образом. Пусть i-ая подсистема СБ состоит из M_i элементов. Считаем, что все наработки j-го элемента i-ой подсистемы СБ до ложного отказа на каждом цикле рассматриваемого случайного процесса независимы и одинаково распределены с функцией $F_{\varphi_i^j}(t)$. При этом восстановление производится только после ложного отказа. Тогда время наработки подсистемы СБ до ложного отказа можно записать в виде функции $\varphi_i = \varphi_i\left(\varphi_i^1, \ldots, \varphi_i^{M_i}\right)$, вид которой будем записывать исходя из следующих определений.

Ложным сечением назовем такое множество элементов подсистемы системы безопасности, ложный отказ которых приводит к ложному отказу подсистемы.

Минимальным ложным сечением назовем такое ложное сечение, ни одно из подмножеств элементов которого не является ложным сечением.

Тогда время наработки до ложного отказа минимального ложного сечения определяется как максимум из всех времен наработки до ложного отказа его элементов. Для заданной структуры подсистемы системы безопасности необходимо выделить все минимальные ложные сечения. Время наработки до ложного отказа подсистемы в таком случае представляет собой минимум из наработок до ложного отказа всех имеющихся минимальных ложных сечений.

Рассмотрим теперь подробнее процесс функционирования системы безопасности. Как уже упоминалось ранее, i-ая подсистема системы безопасности состоит из M_i элементов, каждый из которых может находиться только в одном из двух состояний — исправном и неисправном, также и подсистема системы безопасности может находиться только в одном из этих двух состояний. Для описания состояния j-го элемента i-ой подсистемы системы безопасности можно ввести бинарные или булевы переменные:

$$x_i^j = \begin{cases} 1, & \text{если j-й элемент i-й подсистемы работоспособен,} \quad j = 1,2,\ldots,M_i, \\ 0, & \text{если j-й элемент i-й подсистемы неработоспособен.} \end{cases}$$

Функция $g_i(x_i^1, x_i^2, \ldots, x_i^{M_i})$ называется структурной функцией [3] i-ой подсистемы системы безопасности. Функция надежности i-ой подсистемы системы безопасности — это функция

$$h_i(P_i^1, P_i^2, \ldots, P_i^{M_i}) = Mg_i(x_i^1, x_i^2, \ldots, x_i^{M_i}) = P(g_i(x_i^1, x_i^2, \ldots, x_i^{M_i}) = 1),$$

где $P_i^j = P(x_i^j = 1) = Mx_i^j$ — вероятность безотказной работы j-го элемента i-ой подсистемы системы безопасности.

Время безотказного функционирования до скрытого отказа ξ_i^j j-го элемента i-ой подсистемы системы безопасности есть случайная величина. Будем считать, что восстановление подсистемы системы безопасности проводится только после того, как будет обнаружен отказ этой подсистемы. Время наработки подсистемы системы безопасности до скрытого отказа с учетом ее структуры запишем в виде $\xi_i = \xi_i\left(\xi_i^1, \ldots, \xi_i^{M_i}\right)$. Вид этой функции будем записывать, руководствуясь следующими определениями.

Скрытым сечением назовем такое множество элементов подсистемы системы безопасности, скрытый отказ которых приводит к скрытому отказу подсистемы.

Минимальным скрытым сечением назовем такое скрытое сечение, ни одно из подмножеств элементов которого не является скрытым сечением.

Время наработки скрытого сечения до скрытого отказа следует определять, как максимум из времен наработок до скрытого отказа его элементов. Время наработки подсистемы системы безопасности до скрытого отказа определяется как минимум из времен наработок до скрытого отказа всех имеющихся минимальных скрытых сечений. После обнаружения отказа i-ой подсистемы системы безопасности производится восстановление ее работоспособности в течение времени η_i, также случайного, причем восстановление системы безопасности полное. Пусть, кроме того, для оперативного обнаружения, а, следовательно, и восстановления системы после скрытого отказа составляющей ее подсистемы применяются процедуры периодических профилактик подсистем системы безопасности. Предположим, что промежуток времени между двумя профилактиками i-ой подсистемы системы безопасности равен T_i, а продолжительность профилактики этой подсистемы составит величину θ_i.

Математическая модель надежности систем защиты информации

Очевидно, что при данных предположениях процесс функционирования информационной системы можно описывать с помощью наложения двух альтернирующих процессов восстановления. Один из этих процессов описывает атаки на объект защиты, которые либо парируются системой безопасности, либо приводят к аварии, и ложные отказы подсистем системы безопасности. Прочие же процессы описывают скрытые отказы элементов подсистем системы безопасности, восстановление после этих отказов, а также периодическую профилактику системы безопасности.

Рассмотрим первый из упомянутых процессов. Представим длительность цикла регенерации

этого процесса, на котором не было аварии, в следующем виде:

$$\tau = (\chi_1 + \gamma_1) J_{\chi_1 < \chi_2 \wedge \ldots \wedge \chi_N \wedge \varphi_1\left(\varphi_1^1,\ldots,\varphi_1^{M_1}\right) \wedge \ldots \wedge \varphi_N\left(\varphi_N^1,\ldots,\varphi_N^{M_N}\right)} + \ldots +$$
$$+ (\chi_N + \gamma_N) J_{\chi_N < \chi_1 \wedge \ldots \wedge \chi_{N-1} \wedge \varphi_1\left(\varphi_1^1,\ldots,\varphi_1^{M_1}\right) \wedge \ldots \wedge \varphi_N\left(\varphi_N^1,\ldots,\varphi_N^{M_N}\right)} +$$
$$+ \left(\varphi_1\left(\varphi_1^1,\ldots,\varphi_1^{M_1}\right) + \psi_1\right) J_{\varphi_1\left(\varphi_1^1,\ldots,\varphi_1^{M_1}\right) < \chi_1 \wedge \ldots \wedge \chi_N \wedge \varphi_2\left(\varphi_2^1,\ldots,\varphi_2^{M_2}\right) \wedge \ldots \wedge \varphi_N\left(\varphi_N^1,\ldots,\varphi_N^{M_N}\right)} + \ldots +$$
$$+ \left(\varphi_N\left(\varphi_N^1,\ldots,\varphi_N^{M_N}\right) + \psi_N\right) J_{\varphi_N\left(\varphi_N^1,\ldots,\varphi_N^{M_N}\right) < \chi_1 \wedge \ldots \wedge \chi_N \wedge \varphi_1\left(\varphi_1^1,\ldots,\varphi_1^{M_1}\right) \wedge \ldots \wedge \varphi_{N-1}\left(\varphi_{N-1}^1,\ldots,\varphi_{N-1}^{M_{N-1}}\right)},$$

где $J_A = J(w \in A) = \begin{cases} 1, w \in A, \\ 0, w \notin A. \end{cases}$ — индикатор события $w \in A$, $\varphi \wedge \chi = \min(\varphi,\chi)$ — обозначение для операции взятия минимума от двух случайных величин.

Если же происходит авария, то время работы информационной системы от начала цикла до аварии определяется так:

$$\tau' = \chi_1 \wedge \ldots \wedge \chi_N \wedge \ \varphi_1(\varphi_1^1,\ldots,\varphi_1^{M_i}) \wedge \ldots \wedge \varphi_{\mathrm{N}}(\varphi_N^1,\ldots,\varphi_N^{M_N}).$$

Все время работы информационной системы до аварии есть сумма циклов регенерации, произошедших за это время:

$$\omega = \sum_{k=1}^{\nu-1} \tau_k + \tau'_\nu,$$

где ν — номер цикла регенерации, на котором произошла авария.

Поскольку рассматриваемый процесс является альтернирующим процессом восстановления, то вероятность того, что авария произошла на n-ом цикле регенерации, можно представить в виде $P(\nu = n) = r_1^{n-1} r_2$, где r_1 — вероятность того, что на цикле регенерации рассматриваемого процесса аварии не было, r_2 — вероятность того, что на цикле регенерации рассматриваемого процесса произошла авария ($r_1 + r_2 = 1$).

Используя ранее записанные соотношения, можно записать среднее время наработки информационной системы до аварии $M\omega$ в виде:

$$M\omega = M\tau' + \frac{1 - r_2}{r_2} M\tau.$$

Не останавливаясь на подробностях вычисления математических ожиданий $M\tau$, $M\tau'$, приведем их конечные выражения, так:

$$M\tau' = \int_0^\infty (1 - F_{\tau'}(t))dt = \int_0^\infty \left(\prod_{i=1}^N (1 - F_{\chi_i}(t))\right) \prod_{i=1}^N \left(1 - F_{\varphi_{\mathrm{i}}(\varphi_i^1,\ldots,\varphi_i^{M_i}}(t)\right) dt,$$

$$M\tau = \int_0^\infty \left(\prod_{i=1}^N (1 - F_{\chi_i}(t)) \prod_{i=1}^N (1 - F_{\phi_i\left(\phi_i^1,\ldots,\phi_i^{M_i}\right)}(t))\right) dt +$$
$$+ \sum_{i=1}^N M\gamma_i \int_0^\infty \prod_{\substack{j=1 \\ j \neq i}}^N (1 - F_{\chi_j}(t)) \prod_{j=1}^N (1 - F_{\phi_j\left(\phi_j^1,\ldots,\phi_j^{M_j}\right)}(t)) dF_{\chi_i}(t) +$$
$$+ \sum_{i=1}^N M\psi_i \int_0^\infty \prod_{j=1}^N (1 - F_{\chi_j}(t)) \prod_{\substack{j=1 \\ j \neq i}}^N (1 - F_{\phi_j\left(\phi_j^1,\ldots,\phi_j^{M_j}\right)}(t)) dF_{\phi_i\left(\phi_i^1,\ldots,\phi_i^{M_i}\right)}(t),$$

и $r_2 = \int\limits_0^\infty \prod\limits_{i=1}^N (1 - F_{\varphi_i\left(\varphi_i^1,\ldots,\varphi_i^{M_i}\right)}(t))dF_{\chi_1\wedge\ldots\wedge\chi_N}(t) \times \sum\limits_{i=1}^N q_i \int\limits_0^\infty \prod\limits_{\substack{j=1\\ j\neq i}}^N (1 - F_{\chi_j}(t))dF_{\chi_i}(t)$, где

$$F_{\chi_1\wedge\ldots\wedge\chi_N}(t) = 1 - \prod_{i=1}^N (1 - F_{\chi_i}(t)), \quad q_i \approx 1 - \frac{M\xi_i\left(\xi_i^1,\ldots\xi_i^{M_i}\right)}{M\eta_i + (T_i+\theta_i) + (T_i+\theta_i)M\left[\xi_i\left(\xi_i^1,\ldots\xi_i^{M_i}\right)\Big/(T_i+\theta_i)\right]},$$

$\left[\xi_i\left(\xi_i^1,\ldots\xi_i^{M_i}\right)\Big/(T_i+\theta_i)\right]$ — целая часть числа $\xi_i\left(\xi_i^1,\ldots\xi_i^{M_i}\right)\Big/(T_i+\theta_i)$.

Очевидно, что получить точное аналитическое выражение для вероятности аварии не представляется возможным, но можно записать экспоненциальную оценку для функции распределения времени до первой аварии. Для этого применим известные результаты [6]:

$$\lim_{\frac{r_2\tau}{M\tau}\xrightarrow{E}0} P\left\{\frac{r_2\omega}{M\tau} > x\right\} = e^{-x},$$

где r_2 — вероятность аварии на полуинтервале $[t_n,t_{n+1})$, являющемся периодом регенерации; τ — длительность периода регенерации при условии, что на этом периоде аварии не произошло, ω — момент первой аварии. Здесь $\xi \xrightarrow{X} 0$ означает сходимость ξ к нулю по Хинчину. Кроме того, известно [4], что если

$$\frac{M\left(\frac{r_2\tau}{M\tau}\right)^2}{M\left(\frac{r_2\tau}{M\tau}\right)} = \frac{M\tau^2 r_2}{(M\tau)^2} \to 0,$$

то $\frac{r_2\tau}{M\tau} \xrightarrow{X} 0$.

Тогда можно записать:

$$F_\omega(t) \approx 1 - e^{-\frac{r_2 t}{M\tau}}$$

при условии $\frac{M\tau^2 r_2}{(M\tau)^2} \to 0$, т.е. при $r_2 \ll 1$.

Рассмотрим теперь пример, когда все случайные величины распределены экспоненциально. Тогда: $F_{\chi_i}(t) = 1 - e^{-\lambda_{\chi_i} t}$, $F_{\gamma_i}(t) = 1 - e^{-\lambda_{\gamma_i} t}$, $F_{\varphi_i}(t) = 1 - e^{-\lambda_{\varphi_i} t}$, $F_{\psi_i}(t) = 1 - e^{-\lambda_{\psi_i} t}$, $F_{\xi_i}(t) = 1 - e^{-\lambda_{\xi_i} t}$, $F_{\eta_i}(t) = 1 - e^{-\lambda_{\eta_i} t}$. Будем считать, что имеется два вида атак и две подсистемы системы безопасности. При этом каждая подсистема системы безопасности состоит из двух параллельно соединенных элементов. Опуская несложные преобразования, запишем сразу результат:

$$M\left[\frac{\xi}{T+\theta}\right] = \frac{2e^{-\lambda_\xi(T+\theta)}}{1-e^{-\lambda_\xi(T+\theta)}} - \frac{e^{-2\lambda_\xi(T+\theta)}}{1-e^{-2\lambda_\xi(T+\theta)}}, \quad q = 1 - \frac{\frac{3}{2}\frac{1}{\lambda_\xi}}{\frac{1}{\lambda_\eta} + (T+\theta) + (T+\theta)M\left[\frac{\xi}{T+\theta}\right]},$$

$$M\tau' = \frac{1}{2\lambda_\chi}, \quad M\tau = \frac{1}{(\lambda_\chi + 2\lambda_\varphi)}\left(\frac{1}{2} + \frac{\lambda_\chi}{\lambda_\gamma} + \frac{2\lambda_\varphi}{\lambda_\psi}\right), \quad r_2 = \frac{\lambda_\chi}{\lambda_\chi + 2\lambda_\varphi} q, M\omega = M\tau' + \frac{1-r_2}{r_2} M\tau.$$

Заключение

В данной работе удалось получить асимптотические оценки для показателей надежности систем защиты информации. Предложенные оценки достаточно просто вычисляются и учитывают большое число различных параметров процесса функционирования информационной системы.

ЛИТЕРАТУРА

1. Щеглов А. Ю. *Защита компьютерной информации от несанкционированного доступа*. СПб.: Наука и техника; 2004. 384 с.
2. Перегуда А. И., Тимашов Д. А. Моделирование процесса функционирования АТК «ОЗ-СБ» с периодически контролируемой системой безопасности. *Надежность*. 2007;2:38–48.
3. Байхельт Ф., Франкен П. *Надежность и техническое обслуживание. Математический подход*. Пер. с нем. М.: Радио и связь; 1988. 393 с.
4. Барзилович Е. Ю., Беляев Ю. К., Каштанов В. А. и др. *Вопросы математической теории надежности* / Под ред. Б.В. Гнеденко. М.: Радио и связь; 1983. 376 с.