Труды Карельского научного центра РАН
№ 8. 2016. С. 34–44
DOI: 10.17076/mat388

УДК 519.218

ОБ ОДНОЙ МАТЕМАТИЧЕСКОЙ МОДЕЛИ БЕЗОПАСНОСТИ

В. А. Каштанов, Е. С. Длиннова

Национальный исследовательский университет «Высшая школа экономики»

В статье исследуется модель технического обслуживания системы, которая обеспечивает безопасность функционирования некоторой охраняемой системы. Для этого используется математическая модель управляемого полумарковского процесса с катастрофами. Особенности модели заключаются в учете особенностей самостоятельной индикации отказа (время самостоятельной индикации имеет произвольное распределение) и особенностей возникновения катастрофы (учет времени, необходимого для нанесения невосполнимого ущерба, и возможность нанесения невосполнимого ущерба не только первым проникновением в охраняемую систему). Устанавливается связь характеристик надежности (безотказности и ремонтопригодности) и характеристик безопасности. Решена задача оптимизации периодичности проведения восстановительных работ, при которой математическое ожидание времени до катастрофы максимально.

Ключевые слова: безопасность; управляемый полумарковский процесс с катастрофами; однородная Марковская рандомизированная стратегия управления; надежность; безотказность; ремонтопригодность; оптимальное управление.

V. A. Kashtanov, E. S. Dlinnova. ON A MATHEMATICAL SECURITY MODEL

A model of system maintenance which ensures secure operation of the system is investigated. To this end, mathematical model of a controlled semi-Markov process with catastrophes is used. The model allows to take into account the features of self-manifestation of failure (the time has an arbitrary distribution) and features of disaster occurrence (the time required to inflict irreparable harm and the possibility of irreparable harm not only at the first penetration into the system). Connection between reliability characteristics (failure-free operation and maintainability) and security features is established. The problem of optimization of the frequency of restoration work, in which the expectation for time until disaster is maximal, is solved.

Keywords: security; controlled semi-Markov process with disasters; homogeneous Markov randomized control strategy; reliability; failure-free operation; maintainability, optimal control.

Введение

Актуальность проблемы безопасности функционирования технических, экономических, социальных и других систем делает актуальной проблему разработки математических моделей безопасности, поскольку анализ

этих моделей позволяет построить прогноз развития реальных процессов функционирования различных систем, предпринять меры при неблагоприятном прогнозе, количественно оценить возникающие опасности.

Если обратиться к основному нормативному документу по безопасности – Федеральному закону «О безопасности» от 28.12.2010 № 390-ФЗ, то можно определить основные особенности моделей и требования к вновь разрабатываемым математическим моделям.

В упомянутом выше федеральном законе безопасность определяется как состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз.

Таким образом, имеем некий объект, который может находиться в различных состояниях, причем элементы этого множества состояний различаются по степени опасности (высокая, низкая опасность и т. п., и обычно эта классификация ассоциируется с цветовой гаммой – красный, оранжевый, зеленый уровень опасности). С другой стороны, есть факторы (противники, злоумышленники или объективные обстоятельства), создающие угрозы штатному течению процесса функционирования и выводящие процесс из подмножества безопасных состояний. Поэтому нужно принимать меры, то есть управлять этим процессом функционирования. Отметим еще одно важное обстоятельство – на процесс функционирования системы оказывают влияние различные случайные факторы.

Из вышеизложенного можно сделать вывод, что математической моделью для описания моделей безопасности и исследования ее характеристик может служить класс управляемых случайных процессов.

В работе [5] для анализа моделей безопасности используется модель управляемого полумарковского процесса с катастрофами, который введен и исследован в [7, 8].

В настоящей работе исследуется модель функционирования системы, которая обеспечивает защиту некоторой технической (информационной, энергетической и т. п.) системы от атак злоумышленников. Причем предполагается, что поток атак описывается пуассоновским процессом с заданным параметром.

Такую ситуацию можно наблюдать при функционировании системы защиты информации, при охране военных и различных специальных объектов и в других подобных обстоятельствах.

Важным фактором при функционировании системы защиты являются ее возможные отказы и переходы в состояния, когда она не способна успешно отражать атаки злоумышленников. Для повышения эффективности функционирования системы защиты предусматривается техническое обслуживание – проведение различных предупредительных восстановительных работ, сокращающих время пребывания системы защиты в состоянии неработоспособности.

Отличие исследуемой в настоящей работе модели технического обслуживания от рассмотренных ранее [2, 3] состоит в том, что появившийся в системе защиты отказ самостоятельно проявляется через случайное время ζ с распределением $\Phi(x) = P\{\zeta < x\}$. Кроме этого, ранее обычно предполагалось [5], что атака считается успешной, если момент атаки попадает на период неработоспособности системы защиты. Однако реальная ситуация значительно сложнее. Во-первых, для успешности атаки (превращение атаки в катастрофу) необходимо не только проникновение в охраняемую систему, когда система защиты не смогла парировать атаку, но и необходимо некоторое время, возможно случайное, для того чтобы злоумышленник смог вскрыть информацию или нанести невосполнимый ущерб охраняемой системе. Это первая особенность исследуемой модели.

Вторая особенность заключается в том, что не только первое преодоление системы защиты на периоде ее неработоспособности может перерасти в катастрофу, но и последующие.

Учет этих особенностей делает исследование технически более сложным, с одной стороны, но, с другой стороны, делает модель адекватно описывающей реальную ситуацию.

Математическая задача, решаемая в настоящей работе, заключается в построении управляемого случайного процесса, описывающего эволюцию исследуемой технической системы, определении количественного показателя безопасности – математического ожидания времени до катастрофы и определении оптимальной стратегии управления, обеспечивающей максимальное значение этого математического ожидания.

Ниже мы дадим решение поставленной задачи в новых предположениях.

Описание процесса эволюции системы защиты

Пусть задана система, у которой время безотказной работы ξ распределено по закону $F(x) = \mathsf{P}\{\xi < x\}$, $\bar{F}\{x\} = 1 - F(x) = \mathsf{P}\{\xi \geqslant x\}$.

Выше мы предположили, что появившийся при функционировании системы отказ само-

стоятельно обнаруживается (проявляется) через случайное время ζ с распределением $\Phi(x)$.

В начальный момент $t_0 = 0$ начинается эксплуатация системы защиты и назначается начало планового предупредительного обновления (профилактика) системы через время $v \geqslant 0$, распределенное по закону

$$G(x) = \mathbf{P}\{v < x\}, G(0) = 0.$$

Назначение плановых предупредительных обновлений системы через случайное время $v \geqslant 0$ означает введение рандомизации в процесс принятия решений, т. е. в тот момент, когда нужно принимать решение, строится реализация u случайной величины v, $\{v = u\}$, распределенной по закону $G(x)$, и плановое предупредительное обновление системы производится через время u.

Если к назначенному моменту v система не отказала (произошло событие $\{v < u\}$), то в момент v начинается плановое предупредительное обновление системы, которое, по предположению, полностью обновляет систему. Обозначим длительность этого планового предупредительного (профилактического) обновления через γ_1, а через $F_1(x) = \mathbf{P}\{\gamma_1 < x\}$ обозначим функцию распределения этой длительности, далее будем использовать обозначения $\bar{F}_1(x) = \mathbf{P}\{\gamma_1 \geqslant x\}$.

Если отказ системы наступил до назначенного момента времени v (произошло событие $\{v \geqslant \xi\}$), но самостоятельно не проявился до назначенного момента (произошло событие $\{v < \zeta + \xi\}$), то в назначенный момент устанавливается, что система находится в состоянии отказа, и начинается плановое аварийное обновление системы. Длительность этого восстановления обозначим через γ_2, а закон распределения обозначим через $F_2(x) = \mathbf{P}\{\gamma_2 < x\}$, $\bar{F}_2(x) = \mathbf{P}\{\gamma_2 \geqslant x\}$.

Если отказ системы наступил до назначенного момента времени и самостоятельно проявился до назначенного момента (произошло событие $\{v \geqslant \zeta + \xi\}$), то в момент проявления отказа $(\zeta + \xi)$ начинается внеплановое аварийное обновление системы. Длительность этого восстановления обозначим через γ_3, а распределение обозначим $F_3(x) = \mathbf{P}\{\gamma_3 < x\}$, $\bar{F}_3(x) = \mathbf{P}\{\gamma_3 \geqslant x\}$.

После проведения возможных восстановительных работ, когда, по предположению, система полностью обновляется, осуществляется перепланирование момента проведения следующей предупредительной восстановительной работы независимо от прошлого течения процесса, и весь процесс обслуживания повторяется заново.

Из вышеприведенного описания следует, что система защиты не может парировать атаки в периоды проведения восстановительных работ и в периоды пребывания системы в состоянии скрытого отказа, а парирует атаки в периоды исправной работы (функционирования).

Описание процесса атак и определение их успешности

Как уже было отмечено выше, на охраняемую систему злоумышленниками осуществляются атаки и попытки нанести невосполнимый ущерб.

Опишем алгоритм осуществления этих атак. Пусть атаки на систему совершаются периодически, через случайные интервалы времени, имеющие экспоненциальные распределения, параметры которых зависят от состояния системы защиты. Обозначим λ_i, $i = 1, 2, 3$, параметр экспоненциального распределения времени между интервалами атак на нашу систему, когда в ней проводится плановая предупредительная профилактика, плановый аварийный ремонт или внеплановый аварийный ремонт соответственно, λ_0 – параметр экспоненциального распределения времени между моментами атак на нашу систему, когда система находится в состоянии скрытого отказа. Заметим, что дифференциация интенсивности атак при различных состояниях системы защиты определяется тем, что, даже находясь в неработоспособном состоянии, система защиты может парировать часть атак.

Самый неблагоприятный исход для функционирования исследуемой системы состоит в том, что злоумышленники смогли атаковать, проникнуть в охраняемую систему и получить достаточное время для ее взлома или нанесения недопустимого ущерба. Поэтому введем еще одну случайную величину, характеризующую время, которое злоумышленник потратит на то, чтобы взломать систему защиты. Обозначим эту величину через η, ее распределение обозначим через $\Psi(x) = \mathbf{P}\{\eta < x\}$ и будем считать ее независимой от других случайных величин.

Итак, атака будет считаться успешной (катастрофой) при выполнении следующих условий: система находилась в неисправном состоянии (проводились какие-то восстановительные работы или система находилась в состоянии скрытого отказа), а злоумышленник сумел попасть на период неработоспособности и успел взломать систему до момента перехода в состояние, когда эти угрозы парируются.

Для дальнейшего исследования потребуется выразить характеристики момента возник-

новения успешной атаки в зависимости от исходных характеристик. Решая эту проблему, прежде всего заметим, что поток атак описывается стационарным процессом Пуассона, параметр которого зависит от состояния системы (вида восстановительной работы или наличия скрытого отказа). В силу однородности и отсутствия последействия пуассоновского процесса, а также предположения о том, что периоды времени, которое надо затратить на взлом, есть независимые случайные величины, можно утверждать, что распределение момента возникновения успешной атаки будет зависить от состояния системы и длительности периода неработоспособности.

Обозначим через $\varkappa$ случайное время, через которое одна из атак, прошедших на периоде неработоспособности системы защиты длительности z, превратится в успешную, то есть произойдет катастрофа (это время отсчитывается от начала периода неработоспособности), а через $F_i(x,z)$ – вероятность того, что эта случайная величина $\varkappa$ меньше x при условии, что система находится в состоянии i, а период неработоспособности равен z.

Если обозначить через $A_i(z)$ событие, состоящее в том, что процесс пребывает в состоянии i и период неработоспособности равен z, то условное распределение случайной величины $\varkappa$ можно записать в виде равенств

$$\mathbf{P}\{\varkappa < x | A_i(z)\} = F_i(x,z), \tag{1}$$

$$\mathbf{P}\{\varkappa \geqslant x | A_i(z)\} = \bar{F}_i(x,z) = 1 - F_i(x,z). \tag{2}$$

Выразим эти вероятности через исходные характеристики. При принятых обозначениях имеем равенство

$$\bar{F}_i(x,z) = \begin{cases} e^{-\lambda_i z}(1 + \sum_{n=1}^{\infty} \lambda_i^n \int_0^z \int_0^{z-x_1} ... \int_0^{z-\sum_{k=1}^{n-1} x_k} \prod_{k=1}^{n} \bar{\Psi}(x - \sum_{s=0}^{k} x_s) dx_1 ... dx_n), x \geqslant z, \\ e^{-\lambda_i x}(1 + \sum_{n=1}^{\infty} \lambda_i^n \int_0^x \int_0^{x-x_1} ... \int_0^{x-\sum_{k=1}^{n-1} x_k} \prod_{k=1}^{n} \bar{\Psi}(x - \sum_{s=0}^{k} x_s) dx_1 ... dx_n), x < z. \end{cases} \tag{3}$$

При выводе равенства (3) использовалась формула полной вероятности и полная группа несовместных событий определялась условиями: за время $min\{x,z\}$ прошло n, $n = 0,1,2,...$, атак в моменты

$$0 < \sum_{s=1}^{n} x_s < min\{x,z\},\ x_s > 0,$$

и каждая из них за время $x - \sum_{s=1}^{n} x_s$ не стала успешной. При этом мы использовали независимость приращений процесса Пуассона и тот факт, что интервалы между соседними моментами атак в процессе Пуассона – независимые случайные величины, распределенные по экспоненциальному закону.

Соотношения (3) преобразуем, используя свойства условного распределения моментов скачков при условии, что на интервале $(0,x)$ произошло n скачков (в терминах задачи безопасности – на интервале $(0,x)$ произошло n атак, в дальнейшем это событие обозначим через $B_n(x)$).

Известно [4], что совместное условное распределение моментов скачков пуассоновского процесса совпадает с совместным распределением членов вариационного ряда, построенного для n реализаций независимых равномерно распределенных на $(0,x)$ случайных величин.

Сделаем замену переменных $y_k = \sum_{s=1}^{k} x_s$ и получим цепочку равенств

$$\int_0^x \int_0^{x-x_1} ... \int_0^{x-\sum_{k=1}^{n-1} x_k} \prod_{k=1}^{n} \bar{\Psi}(x - \sum_{s=0}^{k} x_s) dx_1 ... dx_n = \int_0^x \int_{y_1}^x ... \int_{y_{n-1}}^x \prod_{k=1}^{n} \bar{\Psi}(x - y_k) dy_1 ... dy_n =$$

$$= \frac{1}{n!} \int_0^x \int_0^x ... \int_0^x \prod_{k=1}^{n} \bar{\Psi}(x - y_k) dy_1 ... dy_n = \frac{1}{n!} (\int_0^x \bar{\Psi}(x-y) dy)^n = \frac{1}{n!} (\int_0^x \bar{\Psi}(y) dy)^n, \tag{4}$$

которая справедлива, так как для подынтегральной функции

$$\psi_x(y_1, y_2, ... y_n) = \prod_{k=1}^{n} \bar{\Psi}(x - y_k)$$

выполняются условия

$$\psi_x(y_1, y_2, ... y_n) = \psi_x(y_{i_1}, y_{i_2}, ... y_{i_n})$$

для любой перестановки $(i_1, i_2, ..., i_n)$.

Тогда из (3) получаем

$$\bar{F}_i(x,z) = e^{-\lambda_i \int_0^x \Psi(y) dy}, z \geqslant x \geqslant 0. \tag{5}$$

Определение управляемого полумарковского процесса с катастрофами

При построении управляемого полумарковского процесса с катастрофами будем использовать принятые в [5, 6] обозначения и терминологию и использовать алгоритм, изложенный в этих работах, который определяет следующие этапы:

- определение марковских моментов и пространства состояний процесса;
- построение пространства управлений и стратегий управления;
- определение полумарковского ядра управляемого полумарковского процесса;
- определение условных распределений моментов катастроф;
- вычисление математического ожидания момента катастрофы;
- оптимизация математического ожидания момента катастрофы и определение оптимальной стратегии технического облуживания.

Определение марковских моментов и пространства состояний процесса.

Из описания эволюции процесса функционирования, изложенного выше, следует, что в рассматриваемом случае марковские моменты — это моменты начала и окончания восстановительных работ. По определению первая компонента управляемого полумарковского процесса с катастрофами $\xi(t)$ между марковскими моментами не изменяется.

Кроме этого, заметим, что в работе нас будет интересовать первый момент успешной атаки, и поэтому при построении управляемого полумарковского процесса введем состояние поглощения – состояние катастрофы.

Будем считать, что $\xi(t) = 1$, если в ближайший марковский момент, предшествующий t, началась плановая предупредительная профилактика системы.

Будем считать, что $\xi(t) = 2$, если в ближайший марковский момент, предшествующий t, началось плановое аварийное восстановление системы.

Будем считать, что $\xi(t) = 3$, если в ближайший марковский момент, предшествующий t, началось внеплановое аварийное восстановление системы.

Полагаем $\xi(t) = 0$, если ближайший марковский момент, предшествующий t, является моментом обновления системы или моментом окончания любой восстановительной работы.

Наконец, будем считать, что в момент возникновения успешной атаки процесс переходит в состояние 4, или $\xi(t) = 4$.

Следовательно, первая компонента управляемого полумарковского процесса с катастрофами $\xi(t)$ принимает значения из конечного множества $E = \{0, 1, 2, 3, 4\}$.

Построение пространства управлений и стратегий управления.

В исследуемой модели управление осуществляется только в состоянии $i = 0$ выбором периода, через который следует проводить плановую предупредительную профилактику. Следовательно, пространство управлений определяется равенством

$$U_0 = [0, \infty),$$

а рандомизированные стратегии управления определяются выбором вероятностной меры $G(x)$.

Определение полумарковского ядра управляемого полумарковского процесса.

По определению полумарковское ядро – матрица $Q_{ij}(t, u),\ i, j \in E,\ t \geqslant 0,\ u \in U_i$, есть вероятность того, что следующим состоянием процесса $\xi(t)$ будет состояние j, и переход в это состояние произойдет до момента t при условии, что в момент $t = 0$ процесс перешел в состояние i, $\xi(0) = i$, и принято решение $u \in U_i$. Отметим в этом определении независимость вероятности $Q_{ij}(t, u)$ от календарного времени. Поэтому при определении полумарковского ядра $Q_{ij}(t, u)$ будем считать, что переход в состояние i произошел в момент ноль.

Выпишем первую строку матрицы $Q_{ij}(t, u)$, когда $i = 0$.

Если известно, что в момент перехода процесс принимает значение ноль, $\xi(0) = 0$, и в этот момент принято решение v, то время пребывания процесса $\xi(t)$ в состоянии i разбивается на два периода – период исправной работы системы Θ_1 и период скрытого отказа Θ_2, длительности которых соответственно равны

$$\Theta_1 = min(\xi, v), \tag{6}$$

$$\Theta_2 = max(0, min(v - \xi, \zeta, \varkappa)). \tag{7}$$

Известно [10], что для положительной случайной величины τ математическое ожидание определяется равенством

$$M\tau = \int_0^\infty \mathbf{P}\{\tau \geqslant x\} dx.$$

В силу независимости случайных величин ξ, v выполняется равенство

$$\mathbf{P}\{min(\xi, v) \geqslant x\} = \bar{F}(x)\bar{G}(x),$$

и для математического ожидания имеем

$$M\Theta_1 = \int_0^\infty \bar{F}(x)\bar{G}(x) dx. \tag{8}$$

Если на каком-то периоде выполняется равенство $\Theta_2 = 0$, то значит, произошел переход в состояние 1. Если на каком-то периоде выполняется равенство $\Theta_2 = v - \xi$, то значит, произошел переход в состояние 2. Если на каком-то периоде выполняется равенство $\Theta_2 = \zeta$, то значит, произошел переход в состояние 3. Если на каком-то периоде выполняется равенство $\Theta_2 = \varkappa$, то значит, произошел переход в состояние 4.

Случайные величины ξ, v, ζ – независимые случайные величины. Поэтому

$$\mathbf{P}\{min(v-\xi,\zeta) \geqslant y\} = \mathbf{P}\{v-\xi \geqslant y\}\bar{\Phi}(y) =$$

$$= \bar{\Phi}(y)\int_0^\infty \bar{G}(z+y)dF(z).$$

Случайная величина $\varkappa$ зависит от ξ, v, ζ. Условное распределение $\varkappa$ при условии $\{min(v-\xi,\zeta) = y, y > 0\}$ задается равенством (3), из которого следует $\bar{F}_0(x,y) = \bar{F}_0(x,x)$ при $z \geqslant x$.

Поэтому

$$\mathbf{P}\{min(v-\xi,\zeta,\varkappa) \geqslant x\} = \tag{9}$$

$$= \bar{F}_0(x,x)\bar{\Phi}(x)\int_0^\infty \bar{G}(z+x)dF(z),$$

и искомое математическое ожидание определяется равенством

$$M\Theta_2 = \int_0^\infty\int_0^\infty \bar{F}_0(x,x)\bar{\Phi}(x)\bar{G}(z+x)dF(z)dx. \tag{10}$$

Пусть $j = 0$. Из приведенного выше описания процесса функционирования исследуемой технической системы следует чередование моментов начала и окончания восстановительных работ. Так как в момент окончания восстановительной работы (и только в эти моменты) процесс принимает значение ноль, $\xi(t) = 0$, то очевидно

$$Q_{00}(t,u) = 0. \tag{11}$$

Пусть $j = 1$. При $t < u$ переход в состояние $j = 1$ невозможен, поскольку предупредительная профилактика должна начаться только в момент u. Если $t \geqslant u$, то переход в состояние $j = 1$ произойдет тогда и только тогда, когда будет выполняться событие $\{\xi \geqslant u\}$ (заметим, что в этом случае $\Theta_2 = 0$, и все атаки парируются). Следовательно, при $j = 1$ справедливо соотношение

$$Q_{01}(t,u) = \mathbf{P}\{v < t, v \leqslant \xi | v = u\} =$$

$$= \begin{cases} 0, & u > t, \\ \bar{F}(u), & u \leqslant t. \end{cases} \tag{12}$$

Если $j = 2$, то при $t < u$ вероятность того, что система до момена t перейдет в состояние планового аварийного ремонта, равна нулю, поскольку данный переход должен осуществиться ровно в назначенный момент u, и никак не раньше.

При $t \geqslant u$ для перехода в состояние $j = 2$ должны выполняться условия $\{\xi < u \leqslant \xi + \zeta\}$ и за положительное время скрытого отказа $\Theta_2 = u - \xi > 0$ ни одна из прошедших атак не стала успешной, то есть выполняется неравенство $\varkappa > u - \xi$.

Тогда имеем

$$Q_{02}(t,u) =$$

$$= \mathbf{P}\{\xi < v < \xi + \zeta, \varkappa > v - \xi, t \geqslant v | v = u\} =$$

$$= \begin{cases} 0, u > t, \\ \\ \int_0^u \bar{\Phi}(u-x)\bar{F}_0(u-x,u-x)dF(x), u \leqslant t. \end{cases} \tag{13}$$

Функция $\bar{F}_0(z,z)$ в равенстве (13) определяется соотношением (5).

Если $j = 3$, то справедливы следующие рассуждения.

При $t < u$ для перехода в состояние $j = 3$ должны выполняться условия $\{\xi + \zeta < t\}$ и за положительное время скрытого отказа $\Theta_2 = \zeta > 0$ ни одна из прошедших атак не стала успешной, то есть выполняется неравенство $\varkappa > \zeta$.

При $t \geqslant u$ для перехода в состояние $j = 3$ должны выполняться условия $\{\xi + \zeta < u\}$ и за положительное время скрытого отказа $\Theta_2 = \zeta > 0$ ни одна из прошедших атак не стала успешной, то есть выполняется неравенство $\varkappa > \zeta$.

Таким образом, получаем

$$Q_{03}(t,u) =$$

$$= \mathbf{P}\{\xi + \zeta < min(v,t), \varkappa > \zeta | v = u\} =$$

$$= \begin{cases} \int_0^t \int_0^{t-x} dF(x)d\Phi(y)\bar{F}_0(y,y), u > t, \\ \int_0^u \int_0^{u-x} dF(x)d\Phi(y)\bar{F}_0(y,y), u \leqslant t, \end{cases} \tag{14}$$

где функция $\bar{F}_0(y,y)$ также определяется равенством (5).

Наконец, если $j = 4$, то справедливы следующие рассуждения.

При $t < u$ для перехода в состояние $j = 4$ должны выполняться два несовместных события:

- либо реализуется событие $\{\xi + \zeta < t\}$ и за положительное время скрытого отказа $\Theta_2 = \zeta > 0$ хотя бы одна из прошедших атак

стала успешной, то есть выполняется неравенство $\varkappa < \zeta$;

- либо реализуется событие $\{\xi < t < \xi + \zeta\}$ и за положительное время $t - \xi$ скрытого отказа хотя бы одна из прошедших атак стала успешной, то есть выполняется неравенство $\varkappa < t - \xi$;

При $t \geqslant u$ для перехода в состояние $j = 4$ должны выполняться два несовместных события:

- либо реализуется событие $\{\xi + \zeta < u\}$ и за положительное время скрытого отказа $\Theta_2 = \zeta > 0$ хотя бы одна из прошедших атак стала успешной, то есть выполняется неравенство $\varkappa < \zeta$;

- либо реализуется событие $\{\xi < u < \xi + \zeta\}$ и за положительное время скрытого отказа $\Theta_2 = u - \xi > 0$ хотя бы одна из прошедших атак стала успешной, то есть выполняется неравенство $\varkappa < u - \xi$.

Объединяя вышеприведенные рассуждения, для вероятности $Q_{04}(t,u)$ можно записать равенство

$$Q_{04}(t,u) = \begin{cases} \int_0^u \int_0^{u-x} dF(x)d\Phi(y)F_0(y,y) + \int_0^u \bar{\Phi}(u-x)F_0(u-x,u-x)dF(x), \ t \geqslant u, \\ \int_0^t \int_0^{t-x} dF(x)d\Phi(y)F_0(y,y) + \int_0^t \bar{\Phi}(t-x)F_0(t-u,t-u)dF(x), t < u, \end{cases} \tag{15}$$

в котором функции $F_0(t,z),\ z \geqslant t$, определяются соотношением (5).

Для других строк полумарковской матрицы при $i = 1,2,3$ имеем

$$Q_{ij}(t,u) = 0,\ j \neq 0,4,$$

$$Q_{i0}(t,u) = \int_0^t \bar{F}_i(x,x)dF_i(x), \tag{16}$$

$$Q_{i4}(t,u) = \int_0^\infty F_i(t,x)dF_i(x) =$$

$$= \int_0^t F_i(x,x)dF_i(x) + F_i(t,t)\bar{F}_i(t).$$

Нетрудно проверить очевидное равенство

$$\lim_{t\to\infty} \sum_{j\in E} Q_{ij}(t,u) = 1, \tag{17}$$

справедливое при любом $u > 0$ для $i \in \{0,1,2,3\}$.

Из равенств (11)–(16) получаем интегрированием по мере $G_0(u) = G(u)$ полумарковское ядро стандартного полумарковского процесса [9].

При $i \neq 0$ для функций $Q_{ij}(t) = \int_0^\infty Q_{ij}(t,u)dG_i(u)$ остаются справедливы равенства (16), поскольку нет зависимости от управления u функций (16).

Для состояния $i = 0$ имеем равенства

$$Q_{00}(t) = 0,$$

$$Q_{01}(t) = \int_0^t \bar{F}(u)dG(u), \tag{18}$$

$$Q_{02}(t) =$$

$$= \int_0^t \int_0^u \bar{\Phi}(u-x)\bar{F}_0(u-x,u-x)dF(x)dG(u),$$

$$Q_{03}(t) =$$

$$= \int_0^t \int_0^u \int_0^{u-x} dF(x)d\Phi(y)\bar{F}_0(y,y)dG(u) +$$

$$+ \int_0^t \int_0^{t-x} dF(x)d\Phi(y)\bar{F}_0(y,y)\bar{G}(t),$$

$$Q_{04}(t) = \int_0^\infty Q_{04}(t,u)dG(u).$$

Предельным переходом при $t \to \infty$ получаем переходные вероятности состояний вложенной цепи Маркова

$$p_{ij} = \lim_{t\to\infty} Q_{ij}(t), \quad i,j \in \{0,1,2,3\}.$$

Для исследуемой модели из равенств (18) находим, что

$$p_{00} = 0,\ p_{01} = \int_0^\infty \bar{F}(u)dG(u),$$

$$p_{02} = \tag{19}$$

$$= \int_0^\infty \int_0^u \bar{\Phi}(u-x)\bar{F}_0(u-x,u-x)dF(x)dG(u),$$

$$p_{03} =$$

$$= \int_0^\infty \int_0^u \int_0^{u-x} dF(x)d\Phi(y)\bar{F}_0(y,y)dG(u).$$

Равенство (19) и равенство (17) доказывают, что переход из состояния $i \in \{0,1,2,3\}$ в состояние катастрофы $j = 4$ происходит с положительной вероятностью

$$p_{04} = \int_0^\infty Q_{04}(\infty,u)dG(u) > 0,$$

$$p_{i4} = \int_0^\infty F_i(x,x)dF_i(x) > 0,\ i = 1,2,3.$$

Состояния $i \in \{0,1,2,3\}$ вложенной марковской цепи сообщающиеся и несущественные, а состояние $j = 4$ является поглощающим, достижимым из любого несущественного состояния.

Если использовать терминологию, введенную в [5], то состояния $i \in \{0,1,2,3\}$ есть опасные состояния, а состояние $j = 4$ есть состояние катастрофы. Тогда можно утверждать, что математическое ожидание времени до катастрофы конечно [5].

Обозначим через $M_i,\ i \in \{0,1,2,3\}$, математическое ожидание времени до катастрофы при условии, что полумарковский процесс стартует из состояния $i \in \{0,1,2,3\},\ \xi(0) = i$.

Тогда для введенных математических ожиданий по формуле полного математического ожидания получаем неоднородную систему алгебраических уравнений

$$M_i = m_i + \sum_{j=0}^{3} p_{ij} M_j,\ i \in \{0,1,2,3\}, \qquad (20)$$

где математическое ожидание m_i времени непрерывного пребывания процесса $\xi(t)$ в состоянии i определяется равенством при $i \in \{0,1,2,3\}$

$$m_i = \sum_{j=0}^{4} \int_0^\infty t dQ_{ij}(t)dt = \int_0^\infty \{1 - \sum_{j=0}^{4} Q_{ij}(t)\}dt,$$

в котором функции $Q_{ij}(t)$ определяются равенствами (16) и (18).

Поэтому получаем

$$m_i = \int_0^\infty \bar{F}_i(t,t)\bar{F}_i(t)dt,\ i = 1,2,3, \qquad (21)$$

и

$$m_0 = M\Theta_1 + M\Theta_2, \qquad (22)$$

где математические ожидания $M\Theta_i,\ i = 1,2$, определяются равенствами (8) и (10)

Выпишем решение системы (20) при $i = 0$, то есть считаем, что процесс стартует из состояния $i = 0,\ \xi(0) = i$.

Тогда получаем выражение математического ожидания времени до катастрофы через исходные характеристики:

$$M_0 = \frac{m_0 + \sum_{j=1}^{3} m_j p_{0j}}{1 - \sum_{j=1}^{3} p_{0j} p_{j0}}. \qquad (23)$$

Математическое ожидание m_0 и вероятности $p_{0j}, j \in \{1,2,3\}$, суть линейные функционалы относительно вероятностного распределения $G(u)$, определяющего периодичность проведения плановых восстановительных работ (соотношения (8), (10) и (18)). Следовательно, математическое ожидание $M_0(G)$ есть дробно-линейный функционал

$$M_0(G) = \frac{\int_0^\infty A(u)dG(u)}{\int_0^\infty B(u)dG(u)}, \qquad (24)$$

где функции $A(u)$ и $B(u)$ определяются равенствами

$$A(u) = \int_0^u \bar{F}(x)dx + \int_0^u \bar{F}_0(x,x)F(u-x)\bar{\Phi}(x)dx + \bar{F}(u)\int_0^\infty \bar{F}_1(t,t)\bar{F}_1(t)dt +$$
$$+ \int_0^\infty \bar{F}_2(t,t)\bar{F}_2(t)dt \int_0^u \bar{\Phi}(u-x)\bar{F}_0(u-x,u-x)dF(x) + \qquad (25)$$
$$+ \int_0^\infty \bar{F}_3(t,t)\bar{F}_(t)dt \int_0^u \bar{F}_0(y,y)F(u-y)d\Phi(y),$$

$$B(u) = 1 - \bar{F}(u)\int_0^\infty \bar{F}_1(z,z)dF_1(z) +$$
$$+ \int_0^\infty \bar{F}_2(z,z)dF_2(z)\int_0^u \bar{\Phi}(u-x)\bar{F}_0(u-x,u-x)dF(x) + \qquad (26)$$
$$+ \int_0^\infty \bar{F}_3(z,z)dF_3(z)\int_0^u \bar{F}_0(y,y)F(u-y)d\Phi(y).$$

Оптимальную стратегию управления можно искать в классе детерминированных стратегий [1]

$$G(x) = \begin{cases} 0, x \leqslant u, \\ 1, x > u. \end{cases} \qquad (27)$$

Таким образом, получаем, что если процесс стартует из состояния ноль, когда система защиты новая, то математическая задача сводится к определению максимума функции

$$M_0(u) = \frac{A(u)}{B(u)}$$

и точки u_0, в которой этот максимум достигается,

$$M_0(u_0) = \max_{u \geqslant 0} \frac{A(u)}{B(u)}. \qquad (28)$$

Вывод. Нужно назначать проведение предупредительных профилактик через время u_0, тогда получим максимальное значение математического ожидания времени до катастрофы.

Алгорим определения оптимальной стратегии управления

Исходные данные:
- функция распределения времени безотказной работы системы $F(x)$;
- функция распределения времени самостоятельного проявления отказа $\Phi(x) = 1 - e^{-\lambda x}$;
- функция распределения времени планового предупредительного ремонта $F_1(x)$;
- функция распределения времени планового аварийного ремонта $F_2(x)$;
- функция распределения времени внепланового аварийного ремонта $F_3(x)$;
- интенсивность атак в состоянии скрытого отказа λ_0;
- интенсивность атак в состоянии планового предупредительного ремонта λ_1;
- интенсивность атак в состоянии планового аварийного ремонта λ_2;
- интенсивность атак в состоянии внепланового аварийного ремонта λ_3;
- функция распределения времени, необходимого для вскрытия информации, $\Psi(x)$.

Этапы построения оптимальной стратегии:
1. Вычисление функций $\bar{F}_i(x,x), i = 0,1,2,3$ (равенство (5));
2. Вычисление функций $A(u), B(u)$ (равенства (25),(26));
3. Определение максимума функции $M_0(u)$ (равенство (30)).

Пример

Приведем пример расчета оптимальной периодичности проведения плановых восстановительных работ для следующих исходных данных:
- функция распределения времени безотказной работы системы $F(x) = 1 - e^{-\lambda x}$;
- функция распределения времени самостоятельного проявления отказа $\Phi(x) = 0, x < \infty$ (самостоятельно отказ не проявляется);
- функция распределения времени планового предупредительного ремонта $F_1(x) = 1 - e^{-\mu_1 x}$;
- функция распределения времени планового аварийного ремонта $F_2(x) = 1 - e^{-\mu_2 x}$;
- функция распределения времени внепланового аварийного ремонта $F_3(x) = 1 - e^{-\mu_3 x}$;
- интенсивность атак в состоянии скрытого отказа λ_0;
- интенсивность атак в состоянии планового предупредительного ремонта λ_1;
- интенсивность атак в состоянии планового аварийного ремонта λ_2;
- интенсивность атак в состоянии внепланового аварийного ремонта λ_3;
- необходимо фиксированное время τ для вскрытия информации, функция распределения времени, необходимого для вскрытия информации,

$$\Psi(x) = \begin{cases} 0, x \leqslant \tau, \\ 1, x > \tau. \end{cases} \qquad (29)$$

Этап 1. Вычисление функций $\bar{F}_i(x,x)$. Из равенства (5) получаем при $i = 0,1,2,3$ для заданных исходных данных

$$F_i(x,x) = \begin{cases} 1, \ x \leqslant \tau, \\ e^{-\lambda_i(x-\tau)}, \ x > \tau. \end{cases} \qquad (30)$$

Этап 2. Вычисляем функцию $A(u)$.
Обозначим

$$\alpha_i = \int_0^\infty \bar{F}_i(z,z)\bar{F}_i(z)dz, \ i = 1,2,3.$$

При исходных данных примера имеем

$$\alpha_i = \alpha_i(\tau) = \frac{1 - e^{-\mu_i \tau}}{\mu_i} + \frac{e^{-(\lambda_i + \mu_i)\tau}}{\lambda_i + \mu_i}.$$

Из равенства (25) получаем при заданных исходных данных:
при $u < \tau$

$$A(u) = u + e^{-\lambda u}\alpha_1(\tau) + (1 - e^{-\lambda u})\alpha_2(\tau),$$

при $u > \tau$

$$A(u) = \frac{1 - e^{-\lambda u}}{\lambda} + \tau + \frac{e^{-\lambda\tau}}{\lambda} - \frac{e^{-\lambda_0(u-\tau)}}{\lambda} +$$

$$+ \frac{e^{\lambda_0(u-\tau)} - e^{\lambda(u-\tau)}}{\lambda - \lambda_0} + e^{-\lambda u}\alpha_1(\tau) +$$

$$+ \{1 - e^{-\lambda\tau} + \frac{\lambda}{\lambda - \lambda_0}[e^{\lambda_0(u-\tau)} - e^{\lambda(u-\tau)}]\}\alpha_2(\tau).$$

Обозначим

$$\beta_i = \int_0^\infty \bar{F}_i(z,z)dF_i(z), \ i = 1,2,3.$$

При исходных данных примера имеем

$$\beta_i = \beta_i(\tau) = 1 - \frac{\lambda_i e^{-\mu_i \tau}}{\mu_i + \lambda_i}.$$

Из равенства (26) получаем при заданных исходных данных:

при $u < \tau$

$$B(u) = 1 - e^{-\lambda u}\beta_1(\tau) + (1 - e^{\lambda u})\beta_2(\tau),$$

при $u < \tau$

$$B(u) = 1 - e^{-\lambda u}\beta_1(\tau) +$$

$$+ \{1 - e^{-\lambda\tau} + \frac{\lambda}{\lambda - \lambda_0}[e^{\lambda_0(u-\tau)} - e^{\lambda(u-\tau)}]\}\beta_2(\tau).$$

Исследование завершается поиском максимума отношения функций $A(u)$ и $B(u)$ и точки u_0, в которой этот максимум достигается.

Литература

1. Вопросы математической теории надежности / Под ред. Б. В. Гнеденко. М.: Радио и связь, 1983. 376 с.

2. *Зайцева О. Б.* Анализ безопасности функционирования технических систем // Обозрение прикладной и промышленной математики. 2011. Т. 18, вып. 1. С. 94–95.

3. *Зайцева О. Б.* Анализ полумарковской модели безопасности // Обозрение прикладной и промышленной математики. 2011. Т. 18, вып. 2. С. 223–225.

4. *Карлин С.* Основы теории случайных процессов. М.: Мир, 1971. 536 с.

5. *Каштанов В. А., Зайцева О. Б.* О минимаксных подходах в задачах безопасности // Труды Карельского научного центра РАН. 2013. № 1. Вып. 4. С. 55–67.

6. *Каштанов В. А.* Элементы теории случайных процессов. М.: МИЭМ, 2010. 113 с.

7. *Каштанов В. А., Янишевский И. М.* Исследование функционалов на траекториях полумарковского процесса с конечным множеством состояний // Кибернетика и системный анализ. АН Украины. 1998. № 1. С. 145–156.

8. *Каштанов В. А., Янишевский И. М.* Совместное распределение времени до момента катастрофы и аддитивного функционала доходов // Теория вероятностей и ее применения. 1996. Т. 41, вып. 3. С. 145–152.

9. *Королюк В. С., Турбин А. Ф.* Полумарковские процессы и их приложения. Киев: Наукова думка, 1976. 182 с.

10. *Феллер В.* Введение в теорию вероятностей и ее приложения (том 2). М.: Мир, 1967. 751 с.

Поступила в редакцию 15.05.2016

References

1. Voprosy matematicheskoj teorii nadezhnosti [Problems of mathematical theory of reliability]. Ed. B. V. Gnedenko. Moscow: Radio i svyaz', 1983. 376 p.

2. *Zajceva O. B.* Analiz bezopasnosti funkcionirovaniya tekhnicheskih sistem [Security analysis of technical systems]. *Obozrenie prikladnoj i promyshlennoj matematiki* [*Review of applied and industrial mathematics*]. 2011. Vol. 18, iss. 1. P. 94–95.

3. *Zajceva O. B.* Analiz polumarkovskoj modeli bezopasnosti [A study of semi-Markov safety model]. *Obozrenie prikladnoj i promyshlennoj matematiki* [*Review of applied and industrial mathematics*]. 2011. Vol. 18, iss. 2. P. 223–225.

4. *Karlin S.* Osnovy teorii sluchajnyh processov [Fundamentals of the theory of stochastic processes]. Moscow: Mir, 1971. 536 p.

5. *Kashtanov V. A., Zajceva O. B.* O minimaksnyh podhodah v zadachah bezopasnosti [On minimax approaches to problems of safety]. *Trudy Karel'skogo nauchnogo centra RAN* [*Transactions of KarRC of RAS*]. 2013. No. 1. P. 55–67.

6. *Kashtanov V. A.* Elementy teorii sluchajnyh processov [Elements of the theory of stochastic processes]. Moscow: MIEHM, 2010. 113 p.

7. *Kashtanov V. A., Yanishevskij I. M.* Issledovanie funkcionalov na traektoriyah polumarkovskogo processa s konechnym mnozhestvom sostoyanij [The study of functionals on trajectories of semi-Markov process with a finite set of states]. *Kibernetika i sistemnyj analiz. AN Ukrainy* [*Cybernetics and systems analysis. Academy of sciences of Ukraine*]. 1998. No. 1. P. 145–156.

8. *Kashtanov V. A., Yanishevskij I. M.* Sovmestnoe raspredelenie vremeni do momenta katastrofy i additivnogo funkcionala dohodov [Joint distribution of catastrophe time and of the additive functional of profits]. *Teoriya veroyatnostej i ee primeneniya* [*Theory of probability and its applications*]. 1996. Vol. 41, iss. 3. P. 145–152.

9. *Korolyuk V. S., Turbin A. F.* Polumarkovskie processy i ih prilozheniya [Semi-Markov processes and their applications]. Kiev: Naukova dumka, 1976. 182 p.

10. *Feller V.* Vvedenie v teoriyu veroyatnostej i ee prilozheniya [Introduction to the probability theory and its applications] (vol. 2), Moscow: Mir, 1967. 751 p.

Received May 15, 2016

СВЕДЕНИЯ ОБ АВТОРАХ:

Каштанов Виктор Алексеевич
профессор департамента прикладной математики,
д. ф.-м. н.
Национальный исследовательский университет
«Высшая школа экономики»
ул. Таллинская, 34, Москва, Россия, 123458
эл. почта: vakashtan@yandex.ru

Длиннова Екатерина Сергеевна
магистрант департамента прикладной математики,
Национальный исследовательский университет
«Высшая школа экономики»
ул. Таллинская, 34, Москва, Россия, 123458
эл. почта: <es.ekaterina@gmail.com>

CONTRIBUTORS:

Kashtanov, Victor
National Research University
Higher School of Economics
34 Tallinskaya St., 123458 Moscow, Russia
e-mail: vakashtan@yandex.ru

Dlinnova Ekaterina
National Research University
Higher School of Economics
34 Tallinskaya St., 123458 Moscow, Russia
e-mail: <es.ekaterina@gmail.com>