УДК 20.15.05

ПОЛУМАРКОВСКАЯ МОДЕЛЬ ИНФОРМАЦИОННОЙ СИСТЕМЫ С ПЕРЕМЕННОЙ ВЕРОЯТНОСТЬЮ ПОЛУЧЕНИЯ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ИНФОРМАЦИИ

А.И. Коваленко

Самарский государственный технический университет
Россия, 443100, г. Самара, ул. Молодогвардейская, 244

E-mail: annushka199@bk.ru

Рассмотрена информационная система с защитой от несанкционированного доступа к информации. Попытки получить несанкционированный доступ к защищенной информации образуют рекуррентный поток и с переменной во времени вероятностью заканчиваются успехом. В системе проводится обновление системы безопасности, которое восстанавливает достоверность защиты системы. Найдено стационарное распределение вложенной цепи Маркова как решение системы интегральных уравнений. Сформулирована и решена задача двухкритериальной оптимизации проведения обновления. Рассмотрен численный пример решения этой задачи с использованием линейной свертки экономических критериев.

Ключевые слова*: информационная система, обновление системы безопасности, стационарное распределение вложенной цепи Маркова, стационарные характеристики, двухкритериальная оптимизация.*

Моделирование процессов, связанных с информационной безопасностью, является важной составляющей обеспечения безопасного функционирования информационных систем [1-4]. Одним из видов моделирования является стохастическое моделирование функционирования систем. Большинство работ в этой области посвящено лишь оценке рисков, надежностных и вероятностных показателей; возможность управления этими показателями практически не рассматривается.

В настоящей работе построена полумарковская модель функционирования информационной системы в условиях попыток несанкционированного доступа к защищенной информации. Применение техники, представленной в [5] В.С. Королюком и А.Ф. Турбиным, позволяет допустить общий вид всех функций и вероятностных распределений и определить явный вид стационарных характеристик.

В работе показано, что особенно важным в данной системе является рассмотрение переменной (убывающей со временем) функции – вероятности успешного доступа к защищенной информации. Построенная в работе модель используется для управления периодичностью обновления системы безопасности (например, смены ключа в криптосистеме).

Постановка задачи

Рассмотрим следующую информационную систему. Попытки злоумышленника получить доступ к информации образуют рекуррентный поток, порожденный случайной величиной (СВ) β с функцией распределения $G(t) = P\{\beta \le t\}$.

Анна Игоревна Коваленко, аспирант.

При этом с вероятностью $p(t)$, зависящей от времени, прошедшего с момента обновления системы безопасности, попытка не удается, а с вероятностью $q(t)=1-p(t)$ завершается успехом. С целью повышения надежности информационной системы через время, равное СВ α с функцией распределения $F(t)=P\{\alpha \le t\}$, проводится обновление системы безопасности. Оно длится время, равное СВ γ с функцией распределения $\Phi(t)=P\{\gamma \le t\}$. После этого обновления вероятность успешной атаки становится равной 0 и отсчет времени для функции вероятности успеха попыток начинается заново. Попытки атак прекращаются либо в случае получения доступа к информации, либо в момент начала обновления системы безопасности. В момент окончания обновления системы безопасности атаки возобновляются.

Предполагается, что случайные величины α, β, γ независимы, имеют плотности распределения вероятностей $f(t)$, $g(t)$, $\varphi(t)$, конечные математические ожидания E_α, E_β, E_γ и дисперсии соответственно.

Целью работы является нахождение стационарных характеристик информационной системы и оптимизация периодичности проведения обновления системы безопасности для улучшения надежности и экономических показателей функционирования системы.

Полумарковская модель системы

Для описания функционирования системы используем процесс марковского восстановления $\{\xi_n, \theta_n, n \ge 0\}$ и соответствующий ему полумарковский процесс $\xi(t)$ с дискретно-непрерывным множеством состояний.

Для этого определим фазовое пространство состояний системы:

$$E=\{1,\ 1xp,\ \ 1xq,\ \ 2,\ \ 2x;\ x>0,\ 0<p<1,\ 0<q<1\}.$$

1 – ИС начала функционировать, защита включена;

$1xp$ – осуществлена попытка доступа к информации, которая закончилась неудачей; с момента начала функционирования системы прошло время x;

$1xq$ – осуществлена успешная попытка доступа к информации; с момента начала функционирования системы прошло время x;

2 – начинается обновление системы безопасности, при этом доступ к информации получен;

$2x$ – начинается обновление системы безопасности, при этом доступ к информации не получен; с момента предыдущей попытки доступа к информации прошло время x.

Времена однократного пребывания системы в соответствующих состояниях определяются формулами

$$\theta_1=\alpha\ \Lambda\gamma,\quad \theta_{1xp}=\beta\wedge[\alpha-x]_+,\quad \theta_{1xq}=[\alpha-x]_+,\ \ \theta_{2x}=\theta_2=\gamma,$$

где Λ – знак минимума; $[\alpha-x]_+$ – прямое остаточное время до обновления системы безопасности.

Временная диаграмма функционирования системы изображена на рис. 1. Плотности вероятностей переходов из состояний определяются формулами

$$p_1^{2x} = f(x)\overline{G}(x)dx,\ \ p_1^{1dxp} = p(x)g(x)\overline{F}(x)dx,\ p_1^{1dxq} = q(x)g(x)\overline{F}(x)dx,\ \ x > 0;$$

$$p_{1xp}^{1dyp} = \frac{p(y)}{\overline{F}(x)}g(y-x)\overline{F}(y)dy,\ \ p_{1xp}^{1dyq} = \frac{q(y)}{\overline{F}(x)}g(y-x)\overline{F}(y)dy,\ \ y > x;$$

$$p_{1xp}^{2dy} = f(x+y)\frac{\overline{G}(y)}{\overline{F}(x)}dy,\ \ y > 0;\ P_{1xq}^{2} = P_2^1 = P_{2x}^1 = 1.$$

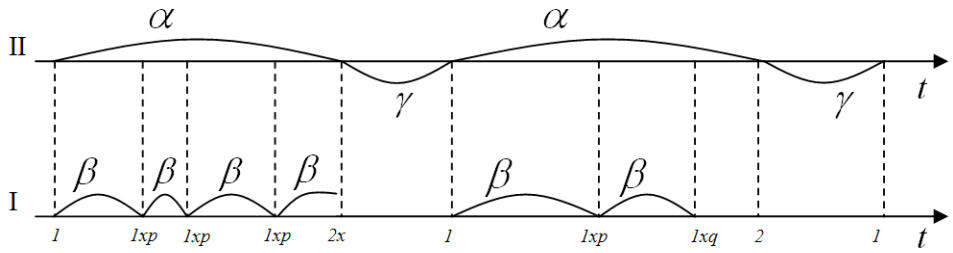

Рис. 1. Временная диаграмма функционирования системы:
I – атаки злоумышленника; II – обновление системы безопасности

Нахождение стационарного распределения вложенной цепи Маркова

Обозначим через ρ_1 и ρ_2 значения стационарного распределения для состояний 1 и 2, а $\rho(1xp)$, $\rho(1xq)$ и $\rho(2x)$ – плотности стационарного распределения вложенной цепи Маркова для состояний $1xp$, $1xq$ и $2x$ соответственно.

Составим и решим методом сжатых отображений (как в работе [6]) систему интегральных уравнений для стационарного распределения:

$$\rho(1xp) = \rho_1 p(x)\overline{F}(x)h_g^{(p)}(x),\ \rho(1xq) = \rho_1 q(x)\overline{F}(x)h_g^{(p)}(x),$$

$$\rho(2x) = \rho_1 f(x)\overline{G}(x) + \rho_1\overline{G}(x)\int_0^\infty p(y)f(x+y)h_g^{(p)}(y)dy,\ \rho_2 = \rho_1\int_0^\infty q(y)\overline{F}(y)h_g^{(p)}(y)dy.$$

Здесь функция $h_g^{(p)}(x)$ определяется рекуррентно следующим образом:

$$h_g^{(p)}(x) = \sum_{n=0}^{\infty} g_p^{(n)}(x), \qquad g_p^{(n)}(x) = \int_0^x p(y)g(x-y)g_p^{(n-1)}(y), \qquad g_p^{(0)}(x) = g(x).$$

Постоянная ρ_1 определяется условием нормировки

$$\rho_1 = [2 + \int_0^\infty h_g^{(p)}(x)\,\overline{F}(x)dx]^{-1}.$$

Введем СВ δ – количество предпринятых атак для получения доступа к информации. Плотность распределения этой СВ $\omega(x) = q(x)h_g^{(p)}(x)$, функция распределения $\Omega(x) = \int_0^x \omega(y)dy.$

Стационарные характеристики информационной системы

Разобьем фазовое пространство состояний E на непересекающиеся подмножества состояний, соответствующие различным физическим состояниям си-

стемы: $E_1^+ = \{1, 1xp\}$ – система функционирует, информация в безопасности; $E_1^- = \{1xq\}$ – система функционирует, получен доступ к информации; $E_2 = \{2, 2x\}$ – осуществляется обновление системы безопасности.

Определим следующие надежностные и экономические показатели функционирования рассматриваемой системы по формулам из [7]:

– вероятность $P^+(\tau)$ безопасного функционирования системы,

– средний удельный доход $S(\tau)$ в единицу календарного времени,

– средние удельные затраты $C(\tau)$ в единицу времени безопасного функционирования системы.

С учетом найденного стационарного распределения вложенной цепи Маркова получаем следующие формулы характеристик при условии, что обновление службы безопасности проводится через определенный период времени τ:

$$P^+(\tau) = \frac{1}{\tau}\int_0^\tau \overline{\Omega}(x)dx,\ S(\tau) = \frac{c_1^+\int_0^\tau \overline{\Omega}(x)dx - c_1^-\int_0^\tau \Omega(x)dx - c_2 E_\gamma}{\tau + E_\gamma};$$

$$C(\tau) = \frac{c_1^-\int_0^\tau \Omega(x)dx + c_2 E_\gamma}{\int_0^\tau \overline{\Omega}(x)dx}.$$

Здесь c_1^+ – доход в единицу времени безопасного функционирования информационной системы; c_1^- – затраты в единицу времени функционирования системы, к которой получен доступ злоумышленника; c_2 – затраты в единицу времени обновления службы безопасности.

Определение оптимальной периодичности обновления службы безопасности

В качестве критериев оптимальности функционирования рассматриваемой системы приняты:

– средний удельный доход в единицу календарного времени $S(\tau)$ (позитивный критерий);

– средние удельные затраты в единицу времени безопасного функционирования системы $C(\tau)$ (негативный критерий);

$$\begin{cases} S(\tau) \to \max\limits_{\tau\in(0,\infty)} \\ C(\tau) \to \min\limits_{\tau\in(0,\infty)} \end{cases}.$$

Одним из способов сведения многокритериальной задачи к однокритериальной является использование в качестве целевой функции линейной свертки частных критериев [9].

Целевой будет функция $V(\tau)$:

$$V(\tau) = a_s S_n(\tau) - a_c C_n(\tau).$$

Здесь a_s и a_c – положительные весовые коэффициенты, определяющие «показатели относительной важности» критериев $S(\tau)$, $C(\tau)$ соответственно. Таким образом, задача оптимизации сводится к нахождению точки τ_{opt}^V максимума функции $V(\tau)$.

Пример 1

Рассмотрим пример оптимизации периодичности проведения обновления службы безопасности для системы, в которой среднее время между моментами попыток доступа к информации (простейший поток) – 1 сутки, среднее время проведения обновления – 1 час, а вероятность доступа к информации при каждой попытке определяется функцией $p(t) = e^{-\frac{1}{8}t}$; $c_{11} = 1500$ ден. ед./сут., $c_{10} = 3800$ ден. ед./сут., $c_2 = 2450$ ден. ед./сут.

Численное решение задачи в пакете Maple приводит к следующим результатам. Линейная свертка частных критериев при весовых коэффициентах $a_s = a_c = 1/2$ достигает наибольшего значения в точке $\tau_{opt}^V = 20{,}88$ час; при этом $S(\tau_{opt}^V) = 1238{,}5$ ден. ед./час, $C(\tau_{opt}^V) = 177{,}25$ ден. ед./час, $P(\tau_{opt}^V) = 0{,}9878$. Графики зависимостей частных критериев от периодичности проведения ТО прибора представлены на рис. 2.

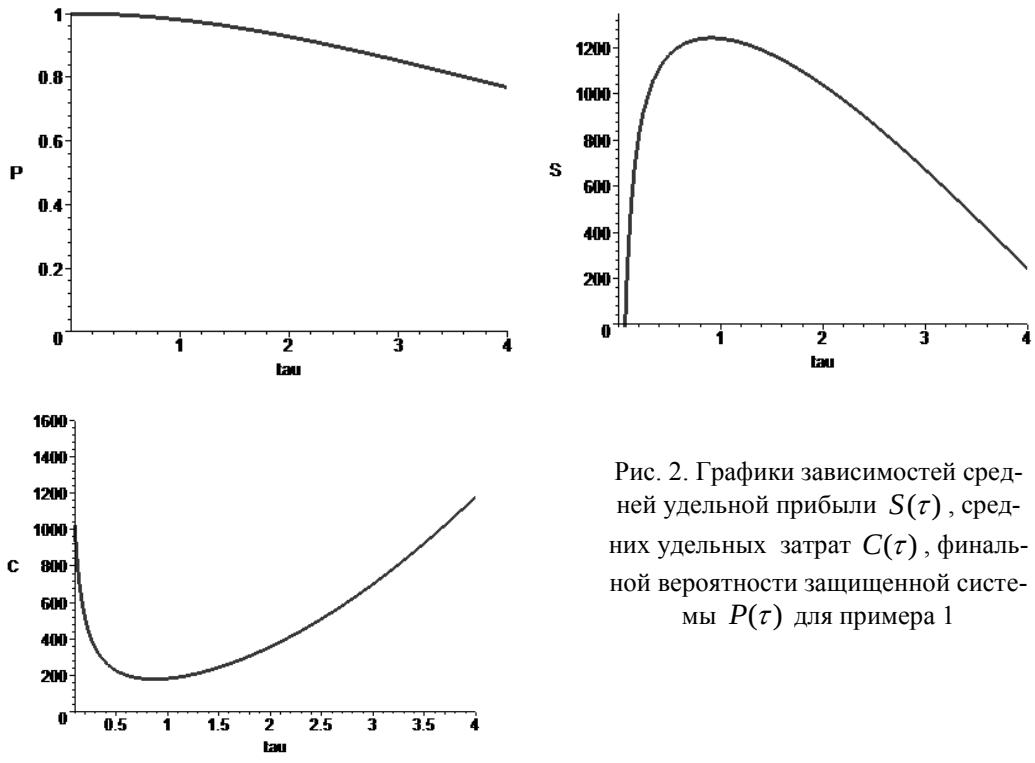

Рис. 2. Графики зависимостей средней удельной прибыли $S(\tau)$, средних удельных затрат $C(\tau)$, финальной вероятности защищенной системы $P(\tau)$ для примера 1

Пример 2

Для сравнения результатов приведем пример с теми же условиями при постоянной вероятности успешной попытки доступа к информации, равной 0,98.

Линейная свертка частных критериев при весовых коэффициентах $a_s = a_c = 1/2$ достигает наибольшего значения в точке $\tau_{opt}^V = 49{,}68$ час. При данном значении периода обновления «реальные» показатели эффективности (рассчитанные по формулам примера 1): $S(\tau_{opt}^V) = 1017{,}32$ ден. ед./час, $C(\tau_{opt}^V) = 179{,}32$ ден. ед./час, $P(\tau_{opt}^V) = 0{,}9796$. То есть если для упрощения моделирования и возможности использования марковских моделей полагать вероятность успеха атаки злоумышленника постоянной (что является приближением к реальности), получим при оптимизации следующие потери: 18 % средней удельной прибыли, 2 % средних удельных затрат, увеличение на 0,082 вероятности доступа к конфиденциальной информации.

Заключение

Рассмотрена информационная система с защитой от несанкционированного доступа к информации, в которой предполагается обновление системы безопасности. Найдено стационарное распределение вложенной цепи Маркова как решение системы интегральных уравнений. Получены математические выражения для определения финальной вероятности защищенного функционирования системы, средних удельных дохода и затрат. Сформулирована задача двухкритериальной оптимизации проведения обновления. Рассмотрен численный пример решения задачи двухкритериальной оптимизации с использованием линейной свертки экономических критериев для сужения Парето-оптимальных решений. Для рассмотренного примера допущение о постоянной вероятности доступа к информации ухудшает все показатели эффективности и надежности функционирования информационной системы: среднюю удельную прибыль на 18 %, средние удельные затраты на 2 %; увеличивает вероятность доступа к конфиденциальной информации на 0,082. Применение аппарата полумарковских процессов с общим фазовым пространством состояний позволяет проводить более эффективную оптимизацию этих процессов и избегать указанных потерь.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Росенко А.П.* Марковские модели оценки безопасности конфиденциальной информации с учетом воздействия на автоматизированную информационную систему внутренних угроз // Вестник Ставропольского государственного университета. – 2005. – № 43. – С. 34–40.
2. *Росенко А.П.* Некоторые аспекты построения систем защиты информации на основе динамических экспертных систем // Электромагнитная совместимость и имитационное моделирование инфокоммуникационных систем: Сборник Поволжской государственной академии телекоммуникаций и информатики. – М.: Радио и связь, 2002. – С. 243-247.
3. *Росенко А.П.* Математическое моделирование влияния внутренних угроз на безопасность конфиденциальной информации, циркулирующей в автоматизированной информационной системе // Известия ЮФУ. Технические науки. Тематический выпуск «Информационная безопасность». – Таганрог: Изд-во ТТИ ЮФУ, 2008. – № 8 (85). – С. 71-81.
4. *Кулагина Л.В.* Математическая модель распределенной базы данных для корпоративных информационных систем // Информатика и системы управления: Труды Нижегородского государственного технического университета им. Р.Е. Алексеева. – 2011. – № 1(86). – С. 83-88.
5. *Королюк В.С., Турбин А.Ф.* Процессы марковского восстановления в задачах надежности систем. – К.: Наук. думка, 1982. – 236 с.
6. *Песчанский А.И., Коваленко А.И.* Полумарковская модель однолинейной системы обслужива-

ния с потерями и учетом технического обслуживания ненадежного канала // Оптимізація виробничих процесів: зб. наук. пр. – Севастополь, 2014. – № 15. – С. 63-70.
7. *Каштанов В.А., Медведев А.И.* Теория надежности сложных систем. – М.: Физматлит, 2010. – 606 с.
8. *Ногин В.Д.* Принятие решений в многокритериальной среде: количественный подход. – М.: Физматлит, 2002. – 144 с.

Статья поступила в редакцию 5 мая 2015 г.

SEMI-MARKOV MODEL OF INFORMATIONAL SYSTEM WITH VARIABLE PROBABILITY OF ILLEGAL ACCESS TO INFORMATION

A.I. Kovalenko

Samara State Technical University
244, Molodogvardeyskaya st., Samara, 443100, Russian Federation

Informational system secured from illegal access to information is studied. Attempts to get illegal access to secured information make a recurrent flow. And the probability of their success varies in time. Security system is restored. It results in restoration of security reliability. The embedded Markov chain stationary distribution is obtained as the solution of the system of integral equations. The problem of two-criterial restoration period optimization is set and solved. A numeric example of this problem solution with the help of linear convolution of economical criteria is given.

Keywords: *informational system, security system restoration, embedded Markov chain stationary distribution, stationary indexes, two-criterial optimization.*

Anna I. Kovalenko, Postgraduate Student.