V. Обсуждение результатов

Исходя из представленных выше результатов эксперимента, можно сделать вывод, что метод последовательного анализа вариантов даёт количественный выигрыш, и на практике использование данного метода целесообразно. Тем не менее, для более точных оценок необходимо провести дальнейшие теоретические исследования с целью более строгого анализа зависимости числа итераций от m при применении описанного нами метода.

VI. Выводы и заключение

В представленной работе была рассмотрена оптимизационная задача (6)–(7). Оптимизационная задача формулировалась в рамках марковской модели угроз, исследованной в работе [2]. Произведён численный эксперимент для оценки эффективности метода последовательного анализа вариантов. Эффективность данного метода заключается в выигрыше количества итераций, относительно метода прямого перебора вариантов. Было вычислено средние значение количества итераций и дисперсия выборки. На основе дисперсии, можно предположить, что результаты выполнения программы сильно зависят от совокупности случайных переменных, поданных на вход.

Список литературы

1. Щеглов К. А., Щеглов А. Ю. Марковские модели угрозы безопасности информационной системы // Известия высших учебных заведений. Приборостроение. Автоматика. Вычислительная техника. 2015. № 12 (58). С. 957–965.

2. Magazev A., Tsyrulnik V. Optimizing the selection of information security remedies in terms of a Markov security model // IOP Conf. Series: Journal of Physics: Conf. 2019. Vol. 1096. 012160. DOI:10.1088/1742-6596/1096/1/012160.

3. Гаврилова Е. А. Исследование методов обнаружения сетевых атак // Научные записки молодых исследователей. Автоматика. Вычислительная техника. 2017. № 4 (56). С. 55–58.

4. Ковалёв М. М. Дискретная оптимизация (целочисленное программирование). Минск: Изд-во БГУ им. В.И. Ленина, 1977. 193 с.

УДК 004.056, 004.942

ОБ ОЦЕНКЕ СРЕДНЕГО ВРЕМЕНИ ЖИЗНИ ИНФОРМАЦИОННОЙ СИСТЕМЫ, ПОДВЕРГАЮЩЕЙСЯ УГРОЗАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

А. А. Магазев, А. А. Касенов
Омский государственный технический университет, г. Омск, Россия

Аннотация. **В работе изучается модель угроз, воздействующих на информационную систему. Модель представлена на языке случайных марковских процессов и описывает функционирование информационной системы как последовательность воздействий и отражений угроз. В результате исследования были получены явные аналитические формулы для среднего времени жизни информационной системы. Информационная система в свою очередь представлена структурной схемой с последовательным и параллельным соединением её элементов. Рассмотрим более подробно каждое соединение в частности. В первом случае, в случае последовательного соединения, при выводе из строя одного элемента - вся система выходит из строя. Во втором же случае для вывода из строя всей информационной системы необходимо чтобы все элементы такой системы вышли из строя. В дальнейшем такую систему можно сколько угодно усложнять.**

Ключевые слова: информационная система, угроза безопасности, марковский процесс.

DOI: 10.25206/2310-4597-2019-1-202-207

I. Введение

Моделирование в рамках информационной безопасности является одним из базовых методов в рамках информационной безопасности. Ключевым недостатком альтернативного метода – метода натурных испытаний – является его высокая стоимость, а также трудоемкость. Также метод натурных испытаний не даёт теоретического обоснования методов защиты информации.

В настоящей работе мы продолжаем исследование одной марковской модели угроз информационной безопасности, предложенной в статьях [1, 2], и частично проанализированной в работе [3].

II. Постановка задачи

Рассмотрим модель, в которой на информационную систему воздействует n независимых внешних угроз с вероятностями q_1, q_2, …, q_n. При этом $\sum_{i=1}^{n} q_i < 1$. Для упрощения расчетов примем во внимание следующие два допущения.

1. Ситуацию с одновременным воздействием нескольких угроз будем считать невозможным.
2. Очередная угроза может произойти только в случае успешного парирования предыдущей.

В соответствии с этим в каждый момент времени $t = 0, 1, 2, \ldots$ система находится в одном из $n + 1$ возможных состояний: $s_0, s_1, \ldots, s_n, s_{n+1}$. В состоянии s_0, называемом *безопасным*, ни одна из угроз не реализуется. Состояние s_i , где $i = 1, \ldots, n$, характеризуется воздействием i-й угрозы. При этом в последующий момент времени имеется две альтернативы: либо данная угроза будет успешно отражена с вероятностью r_i и система вернется в состояние s_0, либо с вероятностью $\bar{r}_i = 1 - r_i$ эта угроза приведет к выводу системы из строя. В последнем случае мы будем считать, что система переходит в состояние s_{n+1}. Граф состояний системы приведен на рис. 1.

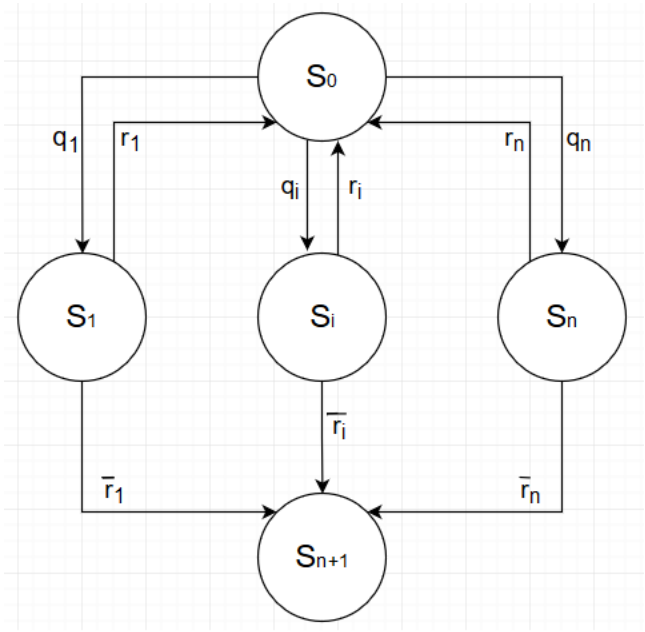

Рис. 1. Граф состояний модели.

Известно, что вероятности нахождения системы в i-ом состоянии вычисляется следующим образом:

$$p_i(t) = \sum_{j=0}^{n} \pi_{ij} p_j(t-1), \tag{1}$$

где π_{ij} – вероятность перехода системы из состояния s_j в состояние s_i. Матрица переходных состояний данной модели выглядит следующим образом:

$$\Pi = \begin{pmatrix} q_0 & q_1 & q_2 & \ldots & q_n & 0 \\ r_1 & 0 & 0 & \ldots. & 0 & \bar{r}_1 \\ r_2 & 0 & 0 & \ldots. & 0 & \bar{r}_2 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ r_n & 0 & 0 & \ldots. & 0 & \bar{r}_n \\ 0 & 0 & 0 & \ldots & 0 & 1 \end{pmatrix}.$$

Для краткости было введено обозначение $q_0 = 1 - \sum_{i=1}^{n} q_i$. Также является очевидным, что в начальный момент времени вероятности нахождения системы в каждом из состояний выглядят следующим образом:

$$p_0(t) = 1, \;\; p_1(t) = p_2(t) = \ldots = p_n(t) = 0, \;\; p_{n+1}(t) = 0 \tag{2}$$

В справедливости формулы (2) можно убедиться, воспользовавшись выражением (1). Выражение (1) представляет собой рекуррентную формулу, выражающую вероятность состояния s_i через вероятности состояний системы в предыдущий момент времени. Для практических целей более удобными являются явные выражения для вероятностей $p_i(t)$, рассматриваемые как функции времени t. Ниже приведен вид функции $p_0(t)$:

$$p_0(t) = \frac{1}{w}\left(\frac{q_0 + w}{2}\right)^{t+1} - \frac{1}{w}\left(\frac{q_0 - w}{2}\right)^{t+1} \tag{3}$$

.

В формуле (3) вводится параметр w для упрощения выражения. Параметр w является неотрицательным и вычисляется по следующей формуле:

$$w^2 = q_0^2 + 4\sum_{i=1}^{n} q_i r_i.$$

Используя выше описанную модель, можно собрать сложную систему, состоящую из двух таких элементов. Рассмотрим два примера такого сочетания моделей.

1. Две подсистемы объедены в общую систему с условием, что при переходе одной из подсистем в конечное состояние s_{n+1}, вся система выходит из строя. Такая система будет считаться системой с последовательным соединением. Схемотичное изображение данной модели приведено на рис. 2.

2. Две подсистемы объедены в общую систему, условием выхода из строя которой является переход в конечное состояние s_{n+1} каждой из составляющих подсистем. Такую систему назовём системой с параллельным соединением. Данная модель схемотично приведена на рис. 3.

Построим схематичные изображения для параллельного соединения на рис. 2, и последовательного соединения на рис. 3 соответственно.

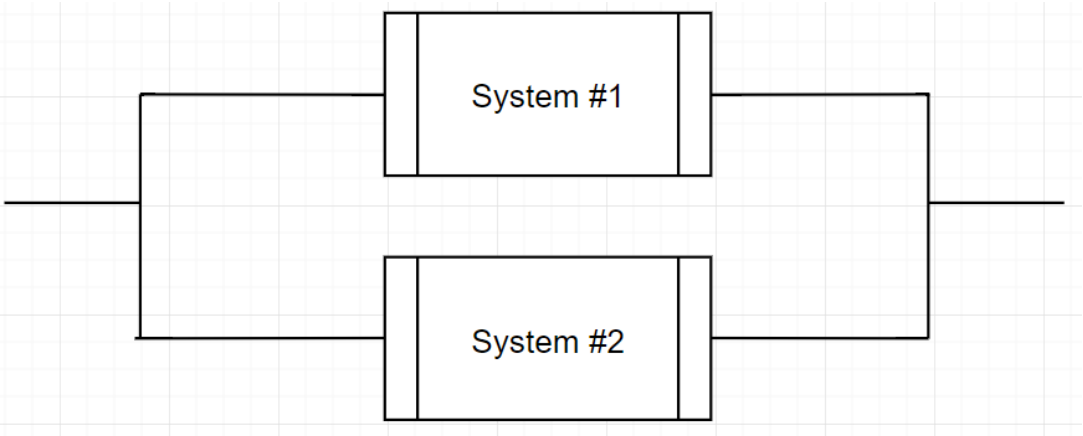

Рис. 2. Схематичное изображение системы с параллельным соединением

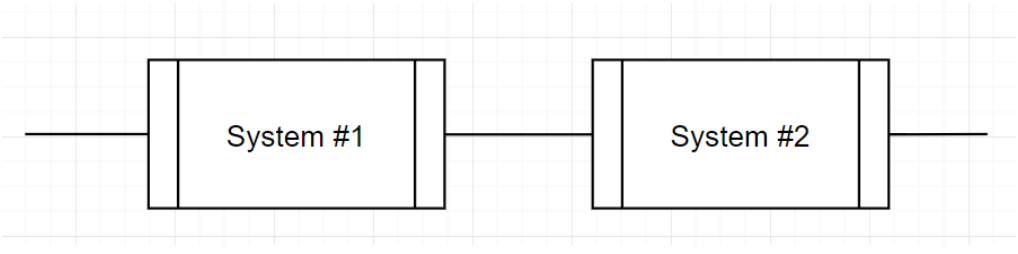

Рис. 3. Схематичное изображение системы с последовательным соединением

Для дальнейшего анализа необходимо построить графы и матрицы связности для систем с последовательным и параллельным соединениями.

Далее будем рассматривать систему с параллельным соединением. Построим граф состояний такой системы. Для построения такого графа необходимо понимать, что при противодействии одной угрозе, другая в этот же момент времени может подействовать на другую систему. Также введем новую переменную $\bar{q}_i = 1 - q_i$.

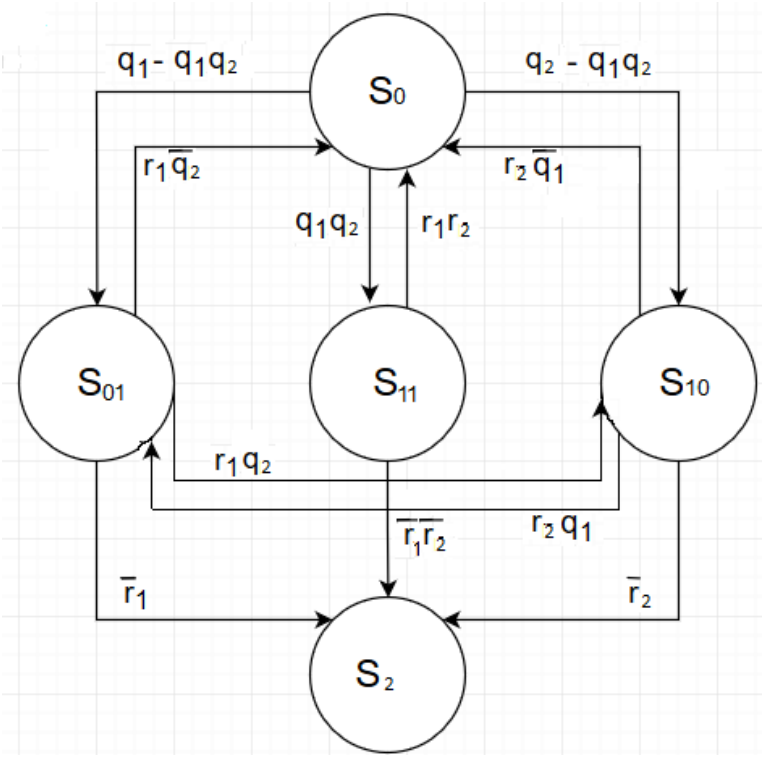

Рис. 4. Граф состояний модели с параллельным соединением

На основе имеющихся графов построим матрицы связности для обоих систем.

$$П_{пар} = \begin{pmatrix} q_0 & q_1 - q_1 q_2 & q_2 - q_1 q_2 & q_1 q_2 & 0 \\ r_1 \bar{q}_2 & 0 & r_1 q_2 & 0 & \bar{r}_1 \\ r_2 \bar{q}_1 & r_2 q_1 & 0 & 0 & \bar{r}_2 \\ r_1 r_2 & 0 & 0 & 0 & \bar{r}_1 \bar{r}_2 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}. \quad (4)$$

Глядя на матрицу переходных вероятностей, приведенную в формуле (4), очевидно, что вычисления путем перемножения матрицы на саму себя будет являться довольно трудоемким процессом. Необходимо попытаться найти более простые пути вычисления, например, используя вышеизложенные формулы для каждой из подсистем, таким образом найти прямую зависимость систем с параллельным и последовательным соединениями через их составляющие простые подсистемы.

III. Теория

Временем жизни T системы назовем время, за которое она перейдет в конечном состоянии s_{n+1}. Другими словами, время жизни – это число переходов системы между состояниями, до тех пор, пока она не окажется в состоянии s_{n+1}. Ясно, что T – это дискретная случайная величина, подчиненная некоторому закону распределения.

Закон распределения для времени жизни нетрудно выписать, используя формулу (3) для вероятности безопасного состояния $p_0(t)$. Обозначим $P(T)$ вероятность перехода системы в конечное состояние s_{n+1} ровно за T шагов. С помощью графа переходов, изображенного на рис. 1, видно, что система может оказаться в состоя-

нии s_{n+1} за T шагов только в том случае, если в момент времени $t = T - 2$ она находилась в безопасном состоянии s_0. Так как вероятность этого события равна $p_0(T - 2)$, для вероятности $P(T)$ получаем:

$$P(T) = p_0(T-2)\sum_{i=1}^{n} q_i(1-r_i)$$

С учетом (3) формулу для функции $P(T)$ можно записать следующим образом:

$$P(T) = \frac{\sum_{i=1}^{n} q_i(1-r_i)}{w}\left[\left(\frac{q_0+w}{2}\right)^{T-1} - \frac{1}{w}\left(\frac{q_0-w}{2}\right)^{T-1}\right].$$

Согласно данному нами определению время жизни есть величина равная:

$$\langle T \rangle = \sum_{T=2}^{\infty} P(T)T.$$

Аналогично напишем формулы для среднего времени жизни системы с параллельным и последовательным соединениями:

$$\langle T_{пар} \rangle = \sum_{T=2}^{\infty} P_{пар}(T)T, \tag{5}$$

$$\langle T_{посл} \rangle = \sum_{T=2}^{\infty} P_{посл}(T)T. \tag{6}$$

Через вероятности $P_1(T)$ обозначим вероятности перехода подсистемы 1 в конечное состояние s_{n+1} ровно за T шагов. Аналогично для $P_2(T)$. Остается необходимым выразить вероятности $P_{пар}(T)$ и $P_{посл}(T)$ через вероятности $P_1(T)$ и $P_2(T)$. Для этого рассмотрим функцию распределения $F(T) = \sum_{i=1}^{T} P(T)$. Воспользуемся определением функции распределения:

$$P_{пар}(T) = F_{пар}(T) - F_{пар}(T-1),$$

$$P_{посл}(T) = F_{посл}(T) - F_{посл}(T-1).$$

Используя известные функции закона распределения, приведенные в [4], получаем следующие формулы:

$$F_{пар}(T) = F_1(T)F_2(T) = \sum_{i=2}^{T} P_1(i)\sum_{i=2}^{T} P_2(i), \tag{7}$$

$$F_{посл}(T) = 1 - F_1(T)F_2(T) = 1 - \sum_{i=2}^{T} P_1(i)\sum_{i=2}^{T} P_2(i). \tag{8}$$

Подставляем (7) и (8) в (5) и (6) соответственно и получаем:

$$< T_{пар} >= \sum_{T=2}^{\infty} T\left[\sum_{i=2}^{T} P_1(i)\sum_{i=2}^{T} P_2(i) - \sum_{i=2}^{T-1} P_1(i)\sum_{i=2}^{T-1} P_2(i)\right] \tag{9}$$

$$< T_{посл} >= \sum_{T=2}^{\infty} T\left[(1 - \sum_{i=2}^{T} P_1(i)\sum_{i=2}^{T} P_2(i)) - (1 - \sum_{i=2}^{T-1} P_1(i)\sum_{i=2}^{T-1} P_2(i))\right] \tag{10}$$

Также из формул (9) и (10) очевидно следующее свойство:

$$< T_{посл} > + < T_{пар} >=< T_1 > + < T_2 > . \tag{11}$$

Для проверки подставим (5), (6) в формулу (11):

$$\sum_{T=2}^{\infty} P_{посл}(T)T + \sum_{T=2}^{\infty} P_{пар}(T)T = \sum_{T=2}^{\infty} P_1(T)T + \sum_{T=2}^{\infty} P_2(T)T.$$

Для справедливости равенства (19) достаточно понимать, что $P_{посл}(T)$ и $P_{пар}(T)$ есть минимумы и максимумы по выборке от $P_1(T)$ и $P_2(T)$.

IV. Результаты экспериментов

Дабы убедиться в справедливости формулы (10) был написан набор подпрограмм при помощи программы математического моделирования “MATLAB”. Набор программ включает в себя следующие функции: “GetNextState” – определяет следующие состояние системы, “LifeTime” – считает время жизни, “AverageLifeTime” – считает среднее время жизни. На вход программы необходимо подать только значения вероятностей внешних угроз q и вероятности их противодействия r, а также количество итераций, число которых чем больше, тем выше точность вычисляемых данных. На выходе нашего модуля мы имеем средние время жизни $\langle T_{посл} \rangle$ и $\langle T_{пар} \rangle$, полученные экспериментальным путем. Эти данные можно использовать для сравнения с данными, полученными в формулах (5) и (6).

ТАБЛИЦА 1
СРАВНЕНИЕ ТЕОРЕТИЧЕСКИХ И ПРАКТИЧЕСКИХ ЗНАЧЕНИЙ.

q_1	q_2	r_1	r_2	$\langle T_{посл} \rangle$ теор	$\langle T_{посл} \rangle$ практ	$\langle T_{пар} \rangle$ теор	$\langle T_{пар} \rangle$ практ	Кол-во итераций
0.2	0.6	0.8	0.3	3.6240	3.6237	30.1800	30.1700	40000
0.5	0.5	0.5	0.5	3.6800	3.6776	8.3200	8.2999	
0.7	0.3	0.3	0.7	3.1865	3.1900	14.7274	14.8211	
0.9	0.9	0.1	0.1	2.0489	2.0478	2.6424	2.6460	
0.9	0.9	0.9	0.9	11.0899	11.1645	31.1323	31.1485	

V. Обсуждение результатов

Полученные теоретические и практические значения, приведенные в табл. 1, являются очень близкими. Для более точного сравнения необходимо большее количество итераций, что является довольно трудозатратным, что снова говорит нам о сложности практических вычислений и необходимости получения явных выражений.

К сожалению, полученная итоговая формула есть бесконечная сумма, что несомненно в итоге облегчает нам вычисления по сравнению с практическими исчислениями, но всё же имеется надежда, что формулы (9) и (10) можно будет свернуть в более простое выражение.

VI. Выводы и заключение

Целью данной работы было получить явное выражение для составных систем, состоящих из простых подсистем. Было рассмотрено два основных варианта: с последовательным и параллельным соединениями. Имея полученные выше выражения, мы можем решать любые сложные системы, просто разбивая их на подсистемы, описанные в рамках данной работы. В дальнейшем хотелось бы усложнять нашу модель, убирая допущения в первой главе, чем мы сможем как можно сильнее приблизить нашу модель к действительности. Но и на данном этапе мы уже имеем модель, приближенно, но всё же дающую нам результаты, схожие с действительностью.

Список литературы

1. Клименко Е. С., Росенко А. П. Марковская модель оценки влияния внутренних угроз на безопасность конфиденциальной информации // Известия ЮФУ. Технические науки. 2007. Т. 76, № 4. С. 123–126.

2. Росенко А. П. Математическое моделирование влияния внутренних угроз на безопасность конфиденциальной информации, циркулирующей в автоматизированной информационной системе // Известия ЮФУ. Технические науки. 2008. Т. 85, № 8. С. 71–81.

3. Магазев А. А., Цырульник В. Ф. Исследование одной марковской модели угроз безопасности компьютерных систем // Модел. и анализ информ. систем. 2017. № 24:4. С. 445–458.

4. Положинцев Б. И. Теория вероятности и математическая статистика. Введение в математическую статистику: учеб. пособие. СПб.: Изд-во Политехнического университета, 2010. 95 с.