Моделирование и анализ информационных систем. Т. 24, № 4 (2017), с. 445–458
Modeling and Analysis of Information Systems. Vol. 24, No 4 (2017), pp. 445–458

©Магазев А. А., Цырульник В. Ф., 2017

DOI: 10.18255/1818-1015-2017-4-445-458

УДК 004.942, 004.056

Исследование одной марковской модели угроз безопасности компьютерных систем

Магазев А. А., Цырульник В. Ф.

получена 6 июля 2017

Аннотация. В настоящей работе исследуется модель угроз безопасности компьютерных систем, формулируемая на языке марковских процессов. В рамках данной модели функционирование компьютерной системы рассматривается как последовательность отказов и восстановлений, возникающих вследствие воздействия на систему угроз информационной безопасности. Приведено подробное описание модели: получены явные аналитические формулы для вероятностей состояний компьютерной системы в произвольный момент времени, обсуждаются некоторые предельные случаи и анализируется динамика системы на больших временах. Отдельно исследуется зависимость вероятности безопасного состояния (т.е. состояния, в котором угрозы отсутствуют) от вероятностей угроз. В частности, показано, что указанная зависимость качественно различается для четных и нечетных моментов времени. Например, в случае одной угрозы вероятность безопасного состояния в четные моменты времени зависит от вероятности угрозы не монотонно, имея, по крайней мере, один локальный минимум в своей области определения. Эта особенность представляется нам важной, так как ее учет позволяет выявить наиболее «опасные» области угроз, при которых вероятность обнаружения системы в безопасном состоянии может оказаться ниже допустимого уровня. В заключение вводится важная характеристика модели — время релаксации, и с ее помощью конструируется допустимая область значений параметров защиты системы.

Ключевые слова: компьютерная система, угроза безопасности, марковский процесс

Для цитирования: Магазев А. А., Цырульник В. Ф., "Исследование одной марковской модели угроз безопасности компьютерных систем", *Моделирование и анализ информационных систем*, **24**:4 (2017), 445–458.

Об авторах:
Магазев Алексей Анатольевич, orcid.org/0000-0002-8725-9183, канд. физ.-мат. наук, доцент,
Омский государственный технический университет,
пр. Мира, 11, г. Омск, 644050, Россия, e-mail: magazev@mail.ru

Цырульник Валерия Федоровна, orcid.org/0000-0002-6875-7216, студентка,
Омский государственный технический университет,
пр. Мира, 11, г. Омск, 644050, Россия, e-mail: lera.tsyrulnik@mail.ru

Введение

Роль моделирования в вопросах информационной безопасности и защиты информации трудно переоценить. После метода натурных испытаний, применение которого традиционно считается весьма дорогостоящим и трудоемким, метод моделирования остается практически единственной альтернативой существующим подходам к

исследованию современных защищенных компьютерных систем. Разработка и использование соответствующих моделей в этой области также необходимы для надлежащего теоретического обоснования механизмов и методов защиты, используемых при проектировании и эксплуатации реальных объектов.

Особое место среди существующих моделей информационной безопасности занимают модели, формулируемые на языке случайных марковских процессов. Спектр прикладных задач, решаемых с применением подобных моделей, необычайно широк: обнаружение кибер-атак в компьютерных сетях [1–3], моделирование процессов распространения компьютерных вирусов [4], обнаружение вторжений в компьютерных системах и вычислительных сетях [5,6], оптимизация и повышение надежности защищенных информационных систем [7, 8]. В последнее время также повысился интерес к скрытым марковским моделям, нашедшим свое применение в криптографии [9], а также в компьютерной вирусологии [10].

В работах [11–14] исследуется класс марковских моделей, в которых компьютерные системы, подвергающиеся угрозам информационной безопасности, рассматриваются как системы с отказами и восстановлениями. Подобный подход к исследованию безопасности компьютерных систем позволяет привлечь развитый математический аппарат теории надежности, хорошо зарекомендовавший себя при расчетах и проектировании сложных технических систем [15,16]. В частности, в статьях [11,12] была предложена марковская модель с конечным числом состояний, характеризующих степень влияния угроз информационной безопасности на компьютерную систему. Авторы процитированных работ провели предварительное исследование модели, обосновывали ее корректность, а также дали интерпретацию получаемых с ее помощью результатов.

В настоящей работе мы проводим более углубленный анализ марковской модели угроз информационной безопасности, предложенной в [11,12]. Помимо исследования некоторых нетривиальных особенностей моделей, не отмеченных ее авторами, мы также обсуждаем возможность приложения этой модели к задаче повышения надежности функционирования компьютерных систем, в частности, к задаче поиска оптимальных значений параметров защиты информации.

Структура настоящей статьи следующая.

В первом разделе дается подробное описание исследуемой марковской модели угроз информационной безопасности. Мы приводим явные аналитические выражения для вероятностей состояний компьютерной системы в произвольный момент времени и, в частности, показываем, что вероятность безопасного состояния (т.е. состояния, в котором отсутствуют угрозы) как функция времени представляется в виде аддитивной комбинации двух зависимостей — монотонно убывающей и осциллирующей. В этом же разделе показано, что на больших временах осциллирующей компонентой в динамике модели можно пренебречь.

Во втором разделе настоящей работы мы изучаем зависимость вероятности безопасного состояния от параметров, характеризующих вероятности угроз информационной безопасности. Показано, что эта зависимость качественно различается для четных и нечетных моментов времени; в частности, в случае одной угрозы вероятность безопасного состояния является монотонно убывающей функцией вероятности угрозы в нечетные моменты времени, тогда как в четные моменты времени она имеет, по крайней мере, один локальный минимум. Отмеченная особенность

представляется нам весьма важной, так как ее учет может позволить выявить наиболее «опасные» области угроз, при которых вероятность обнаружения системы в безопасном состоянии окажется ниже допустимого уровня.

Третий раздел посвящен применению рассматриваемой нами модели угроз информационной безопасности к задаче поиска допустимой области значений параметров защиты системы. В отличие от традиционного подхода, принятого в теории надежности и сводящегося к вычислению вероятности безотказной работы системы в течение заданного времени, мы предлагаем альтернативный подход, основанный на введении *времени релаксации* системы.

1. Описание модели

Рассмотрим компьютерную систему (в дальнейшем просто *систему*), на которую воздействует n независимых внешних угроз с вероятностями $q_1, q_2, \ldots, q_n$: $\sum_{i=1}^{n} q_i < 1$. Будем считать, что одновременное воздействие двух и более угроз невозможно и, кроме того, очередная угроза может проявиться только после 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.

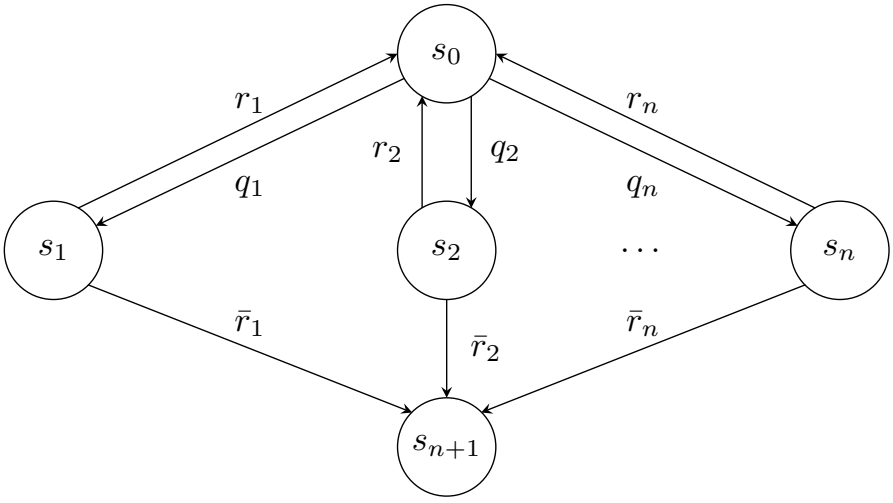

Рис. 1. Граф состояний модели

Fig. 1. The state graph of the model

Динамика рассматриваемой системы представляет собой простую марковскую цепь с матрицей переходных вероятностей

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

где $q_0 = 1 - \sum_{i=1}^{n} q_i$.

Обозначим через $p_i(t)$ вероятность того, что система находится в момент времени t в состоянии s_i. Эта вероятность определяется через вероятности состояний системы в момент времени $t-1$ согласно формуле

$$p_i(t) = \sum_{j=0}^{n+1} p_j(t-1)\,\Pi_{ji}, \tag{2}$$

или в матричной форме

$$\mathbf{p}(t) = \mathbf{p}(t-1) \cdot \Pi, \tag{3}$$

где $\mathbf{p}(t) = (p_0(t), p_1(t), \dots, p_{n+1}(t))$ — вектор вероятностей состояний системы в момент времени t. Используя (3) можно записать

$$\mathbf{p}(t) = \mathbf{p}(0) \cdot \Pi^t, \quad t = 0, 1, 2, \dots, \tag{4}$$

где через Π^t обозначена t-я степень матрицы Π.

Будем считать, что в начальный момент времени $t = 0$ система находилась в безопасном состоянии s_0, то есть $\mathbf{p}(0) = (1, 0, \dots, 0)$. Можно показать, что в этом случае вероятности состояний системы в произвольный момент времени t могут быть выражены следующими формулами:

$$p_0(t) = w^{-1}\left[\left(\frac{q_0 + w}{2}\right)^{t+1} - \left(\frac{q_0 - w}{2}\right)^{t+1}\right]; \tag{5}$$

$$p_i(t) = p_0(t-1)q_i, \quad i = 1, 2, \dots, n; \tag{6}$$

$$p_{n+1}(t) = 1 - p_0(t) - p_0(t-1)\sum_{i=1}^{n} q_i. \tag{7}$$

Здесь положительная величина w, которую мы далее будем называть *w-параметром* модели, определяется как

$$w^2 = q_0^2 + 4\sum_{i=1}^{n} r_i q_i > 0. \tag{8}$$

Докажем приведенные формулы индукцией по t. При $t = 1$ формулы (5) – (7) проверяются непосредственно. Допустим, что они верны для некоторого $t > 1$. Используя явный вид матрицы (1) для компонент вектора $\mathbf{p}(t+1) = \mathbf{p}(t) \cdot \Pi$ получаем:

$$p_0(t+1) = p_0(t)q_0 + \sum_{i=1}^{n} p_i(t) r_i; \tag{9}$$

$$p_i(t+1) = p_0(t)q_i, \quad i = 1, \ldots, n; \tag{10}$$

$$p_{n+1}(t+1) = \sum_{i=1}^{n} p_i(t)(1 - r_i) + p_{n+1}(t). \tag{11}$$

Равенство (9) с помощью формул (5), (6) и (8) может быть переписано как

$$p_0(t+1) = q_0 w^{-1} \left[\left(\frac{q_0 + w}{2} \right)^{t+1} - \left(\frac{q_0 - w}{2} \right)^{t+1} \right] +$$
$$+ w^{-1} \left[\left(\frac{q_0 + w}{2} \right)^{t} - \left(\frac{q_0 - w}{2} \right)^{t} \right] \sum_{i=1}^{n} q_i r_i = w^{-1} \left[\left(\frac{q_0 + w}{2} \right)^{t+2} - \left(\frac{q_0 - w}{2} \right)^{t+2} \right].$$

Далее, равенство (11) с учетом (9) принимает вид

$$p_{n+1}(t+1) = \sum_{i=1}^{n} p_i(t) - p_0(t+1) + p_0(t) \left(1 - \sum_{i=1}^{n} q_i \right) + p_{n+1}(t),$$

которое в силу формул (5) – (7) и тождества $\sum_{i=1}^{n} p_i(t) + p_0(t) + p_{n+1}(t) = 1$ может быть представлено в виде:

$$p_{n+1}(t+1) = 1 - p_0(t+1) - p_0(t) \sum_{i=1}^{n} q_i.$$

Таким образом, если равенства (5) – (7) верны для некоторого t, то они также будут верны и для $t+1$. Следовательно, по индукции эти равенства выполняются для любого t.

Отсутствие защиты в системе характеризуется условием $r_i = 0$, $i = 1, \ldots, n$. Тогда согласно (8) имеем $w = q_0$, то есть w-параметр в этом случае совпадает с вероятностью отсутствия реализации любой из угроз. Отсюда для вероятностей состояний системы будем иметь:

$$p_0(t) = q_0^t, \quad p_i(t) = q_0^{t-1} q_i, \quad i = 1, 2, \ldots, n; \quad p_{n+1}(t) = 1 - q_0^{t-1}. \tag{12}$$

Из этих равенств легко следуют предельные выражения для вероятностей состояний системы при $t \to \infty$:

$$\lim_{t\to\infty} p_0(t) = \cdots = \lim_{t\to\infty} p_n(t) = 0, \quad \lim_{t\to\infty} p_{n+1}(t) = 1. \tag{13}$$

Предельные соотношения (13) будут иметь место и в общем случае, когда не все параметры r_i равны нулю. Чтобы показать это, достаточно убедиться, что величины $(q_0 \pm w)/2$, стоящие в круглых скобках правой части равенства (5), по модулю всегда меньше единицы. Указанный факт, в свою очередь, является следствием того, что величины $(q_0 \pm w)/2$ представляют собой вещественные корни квадратного уравнения $f(x) = x^2 - q_0\, x - \sum_{i=1}^{n} q_i r_i = 0$, которые в силу неравенств $f(\pm 1) > 0$ и $f(0) < 0$ принадлежат интервалу $(-1, 1)$.

Из приведенных соображений видно, что по прошествии достаточно длительного времени система вероятнее всего будет обнаружена в состоянии s_{n+1}, в то время как

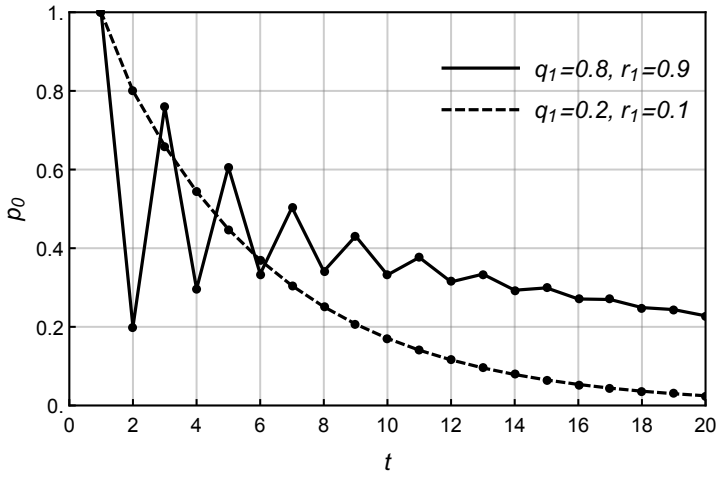

Рис. 2. Вероятность безопасного состояния как функция t при различных значениях параметров q_1 и r_1 в случае одной угрозы

Fig. 2. The security state probability as a function of t for different values of the parameters q_1 and r_1 in the case of one threat

вероятность ее обнаружения в остальных состояниях будет пренебрежимо мала. По этой причине состояние s_{n+1} будет являться *поглощающим состоянием* (что, впрочем, легко видно из графа состояний на рис. 1).

С практической точки зрения наибольший интерес представляет функция $p_0(t)$, являющаяся вероятностью обнаружения системы в безопасном состоянии в произвольный момент времени t. Из сказанного выше следует, что указанная вероятность будет уменьшаться с ростом t, однако в общем случае данная зависимость является не монотонной. Это легко видно из формулы (5): величина $p_0(t)$ представляется как разность двух стоящих в квадратных скобках слагаемых, первое из которых является монотонно убывающей функцией от t, а второе имеет осцилляционный характер (ввиду отрицательности величины $(q_0 - w)/2$). Скорость убывания функции $p_0(t)$ и выраженность ее осцилляций зависит, вообще говоря, от конкретных значений параметров модели q_i и r_i. На рис. 2 приведены графики зависимости $p_0(t)$ от t при двух различных значениях параметров q_1 и r_1 в случае $n = 1$.

В силу того, что

$$\lim_{t\to\infty} \left| \frac{q_0 - w}{q_0 + w} \right|^t = 0,$$

второе слагаемое, стоящее в квадратных скобках в выражении (5), является величиной бесконечно малой более высокого порядка, чем соответствующее первое слагаемое. Это означает, что «амплитуда» осцилляций функции $p_0(t)$ быстро убывает с ростом t, и на больших временах мы можем приближенно считать

$$p_0(t) \approx p_0^*(t) = w^{-1} \left(\frac{q_0 + w}{2} \right)^{t+1}. \tag{14}$$

Нетрудно оценить условие применимости приближения (14). Пусть $\varepsilon > 0$. Тогда

требование $|p_0(t) - p_0^*(t)| < \varepsilon$ эквивалентно неравенству

$$t > \log_{\frac{w-q_0}{2}} \varepsilon w - 1. \tag{15}$$

Таким образом, приближенное выражение (14) отличается от истинной вероятности $p_0(t)$ на величину, не большую ε, если система рассматривается на временах, удовлетворяющих условию (15).

2. Вероятность безопасного состояния как функция вероятности угроз

Изучим характер зависимости вероятности безопасного состояния $p_0(t)$ от вероятностей угроз $q_1, \ldots, q_n$. Для этого мы сначала разберем технически более простую ситуацию, когда на систему воздействует всего одна угроза: $n = 1$. Обозначим вероятность этой угрозы символом q, а соответствующий параметр отражения этой угрозы — r. Таким образом, матрица переходных вероятностей в этом случае имеет вид

$$\Pi = \begin{pmatrix} 1-q & q & 0 \\ r & 0 & 1-r \\ 0 & 0 & 1 \end{pmatrix}. \tag{16}$$

Всюду далее в этом параграфе мы предполагаем, что $0 \le q \le 1$ и $0 < r < 1$.

Из формул (4) и (16) следует, что зависимость $p_0(t)$ от q — полиномиальная, причем степень соответствующего полинома равна t:

$$p_0(t) = c_t q^t + c_{t-1} q^{t-1} + \cdots + c_1 q + c_0. \tag{17}$$

Используя для $p_0(t)$ равенство (5) нетрудно найти явный вид коэффициентов c_k:

$$c_k = (-1)^k \sum_{l=0}^{\min(t-k,k)} C_{t-l}^k C_k^l (-r)^l, \quad k = 0, 1, \ldots, t. \tag{18}$$

Здесь через C_n^k обозначен биномиальный коэффициент из n по k. В частности, для предельных значений параметра q с помощью (17) и (18) получаем:

$$p_0(t)|_{q=0} = 1, \quad p_0(t)|_{q=1} = \begin{cases} 0, & \text{если } t \text{ – нечетно,} \\ r^{t/2}, & \text{если } t \text{ – четно.} \end{cases} \tag{19}$$

Обратим внимание на различное поведение системы при $q = 1$ для четных и нечетных моментов времени: вероятность обнаружения системы в безопасном состоянии в нечетные моменты времени всегда равна нулю, в то время как аналогичная вероятность в четные моменты времени отлична от нуля и монотонно убывает с ростом t (напомним, что $0 < r < 1$). Отмеченная особенность связана с тем, что именно в нечетные моменты времени система «борется» с возникающей угрозой (т.е. находится в состоянии s_1), причем эффективность этой «борьбы» определяется значением параметра r.

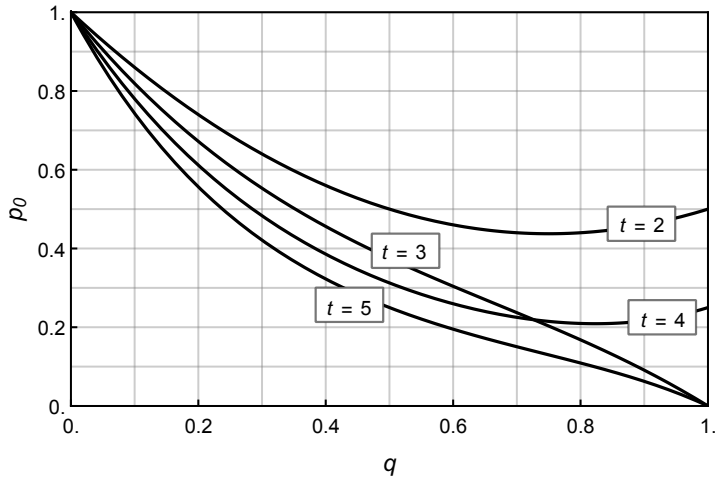

Рис. 3. Вероятность безопасного состояния как функция от q при $r = 0.5$ и $t = 2, 3, 4, 5$

Fig. 3. The security state probability as a function of q for $r = 0.5$ and $t = 2, 3, 4, 5$

Представление величины $p_0(t)$ в виде (17) позволяет предположить, что вероятность безопасного состояния системы не является, вообще говоря, *монотонной* функцией от вероятности угрозы q. В качестве примера на рис. 3 приведены графики зависимости $p_0(t)$ от q при $r = 0.5$ для четырех различных моментов времени t. Видно, что при четных значениях времени величина $p_0(t)$, рассматриваемая как функция от q, имеет выраженные минимумы, в то время как при нечетных значениях t эта функция является монотонно убывающей на всем промежутке $[0, 1]$. По-видимому, данная закономерность будет иметь место для любых значений t, хотя строгого доказательства этого нами пока не получено. Тем не менее, существование по крайней мере одного локального минимума для величины $p_0(t)$ (как функции q) при четных t можно легко доказать аналитически.

Вычисляя производную по q от выражения (17), получаем

$$\frac{dp_0(t)}{dq} = tc_t q^{t-1} + (t-1)c_{t-1}q^{t-2} + \cdots + 2c_2 q + c_1. \tag{20}$$

При *четных* значениях t данный полином будет иметь как минимум один вещественный корень $\bar{q}$ такой, что $0 < \bar{q} < 1$. Действительно, используя формулу (5), нетрудно найти, что

$$\frac{dp_0(t)}{dq}\Big|_{q=0} = t(r-1) - r < 0, \quad \frac{dp_0(t)}{dq}\Big|_{q=1} = \begin{cases} \frac{t}{2}\, r^{t/2} > 0, & \text{если } t \text{ – четное,} \\ -\frac{t+1}{2}\, r^{(t-1)/2} < 0, & \text{если } t \text{ – нечетное.} \end{cases}$$

Так как при четных t функция (20) имеет на концах отрезка $[0, 1]$ различные знаки, то в силу ее непрерывности заключаем, что по крайней мере в одной точке, принадлежащей интервалу $(0, 1)$, она равна нулю. При этом знаки производной $dp_0(t)/dq$ при $q = 0$ и $q = 1$ указывают на то, что хотя бы одна из указанных точек доставляет локальный минимум функции (17). Таким образом, *в четные моменты времени*

величина $p_0(t)$*, рассматриваемая как функция от вероятности угрозы* q*, имеет, по крайней мере, один локальный минимум на интервале* $(0, 1)$.

Возвращаясь к общему случаю произвольного числа угроз, отметим, что в определенном смысле он сводится к уже рассмотренному случаю одной угрозы. Действительно, согласно формулам (5) и (8) вероятность безопасного состояния системы, на которую воздействует n угроз с вероятностями $q_1, q_2, \ldots, q_n$, будет такой же, как и в случае системы с одной угрозой с вероятностью q и параметром защиты r, если положить, что

$$q = \sum_{i=1}^{n} q_i, \quad r = \frac{\sum\limits_{i=1}^{n} q_i r_i}{\sum\limits_{i=1}^{n} q_i}.$$

В частности, используя (17) и (18), нетрудно получить для вероятности $p_0(t)$ выражение, полиномиальное по переменным q_i и r_i:

$$p_0(t) = \sum_{k=1}^{t} \sum_{l=1}^{\min(k,t-k)} (-1)^{k+l} C_{t-l}^{k} C_{k}^{l} \left(\sum_{i=1}^{n} q_i r_i \right)^{l} \left(\sum_{j=1}^{n} q_j \right)^{k-l}.$$

Как функцию от вероятностей угроз $q_1, q_2, \ldots, q_n$ величину $p_0(t)$ следует рассматривать на выпуклой области $Q = \{(q_1, \ldots, q_n) \in \mathbb{R}_+^n \colon \sum_{i=1}^{n} q_i \le 1\}$. С помощью формул (19) нетрудно видеть, что имеют место следующие «граничные условия»:

$$p_0(t)|_{q_i=0} = 1, \quad p_0(t)|_{\sum q_i=1} = \begin{cases} 0, & \text{если } t \text{ – нечетно,} \\ \left(\sum\limits_{i=1}^{n} q_i r_i \right)^{t/2}, & \text{если } t \text{ – четно.} \end{cases}$$

Отметим также, что в отличие от случая одной угрозы, функция $p_0(t)$ при произвольном n в общем случае не имеет локальных минимумов внутри области Q. Тем не менее, она может иметь в этой области условные экстремумы. Их исследование — важная, хотя и технически сложная задача, решению которой будут посвящены наши последующие работы.

3. Время релаксации и построение допустимой области параметров защиты

Как было отмечено в первом разделе, по истечении длительного времени вероятность обнаружить систему в безопасном состоянии будет близкой к нулю. Принимая во внимание неизбежность подобного итога, мы, тем не менее, можем исследовать условия, при которых система будет находиться в безопасном состоянии как можно дольше. Естественно ожидать, что подобные условия будут сводиться к некоторым ограничениям, накладываемым на внутренние параметры системы $r_1, r_2, \ldots, r_n$.

Перейдем к строгим формулировкам. Будем рассматривать динамику системы на временах, удовлетворяющих неравенству (15); в этом случае с точностью до величин порядка ε мы можем приближенно считать

$$p_0(t) \approx w^{-1} \left(\frac{q_0 + w}{2} \right)^{t+1}. \tag{21}$$

В дальнейшем для нас будет важным то, что в рамках рассматриваемого приближения величина $p_0(t)$ является монотонно убывающей функцией t.

Временем релаксации τ назовем время, за которое вероятность безопасного состояния системы уменьшается в *два раза* (по сравнению с моментом времени $t = 0$). С помощью (21) из равенства $p_0(0)/p_0(\tau) = 2$ немедленно получаем

$$\tau = \log_{\frac{q_0+w}{2}} \frac{w}{2} - 1. \tag{22}$$

Пусть t_0 — фиксированный момент времени. Наша ближайшая задача будет заключаться в нахождении значений параметров защиты $r_1, \ldots, r_n$, при которых $\tau \geq t_0$. Другими словами, нас будут интересовать условия, при которых вероятность обнаружения системы в безопасном состоянии на временах, меньших или равных t_0, будет относительно большой.

Используя формулу (22), перепишем неравенство $\tau \geq t_0$ в виде

$$\frac{w}{2} \leq \left(\frac{q_0 + w}{2}\right)^{t_0+1}. \tag{23}$$

Будем рассматривать данное неравенство как ограничение на параметры защиты системы $r_1, \ldots, r_n$; так как последние входят только в выражение для w-параметра, нам необходимо решать неравенство (23) относительно переменной w. Нетрудно видеть, что соответствующее решение имеет вид

$$w \geq 2x^* - q_0, \tag{24}$$

где x^* — вещественный корень уравнения

$$x^{t_0+1} - x + \frac{q_0}{2} = 0, \tag{25}$$

принадлежащий отрезку $[q_0, 1]$.

Подставляя в (24) выражение для w-параметра (8), получаем ограничение на значения параметров защиты r_i:

$$\sum_{i=1}^{n} q_i r_i \geq x^*(x^* - q_0). \tag{26}$$

Вместе с неравенствами

$$r_i \leq 1, \quad i = 1, \ldots, n; \tag{27}$$

требование (26) определяет в пространстве значений параметров защиты выпуклую область $R_{t_0}(q_1, \ldots, q_n) \subset \mathbb{R}^n_+$, которую мы будем называть *допустимой*. Таким образом, только для значений параметров $r_1, \ldots, r_n$ из допустимой области $R_{t_0}(q_1, \ldots, q_n)$ время релаксации τ системы будет не меньшим, чем фиксированное значение t_0.

Приведем примеры построения допустимой области параметров защиты для случаев одной и двух угроз.

ПРИМЕР 1. В случае одной угрозы система характеризуется двумя параметрами: q и r. Как следует из неравенств (26) и (27), допустимая область $R_{t_0}(q)$ параметра защиты r представляет собой отрезок $[r^*, 1]$, где

$$r^* = \frac{x^*(x^* + q - 1)}{q}.$$

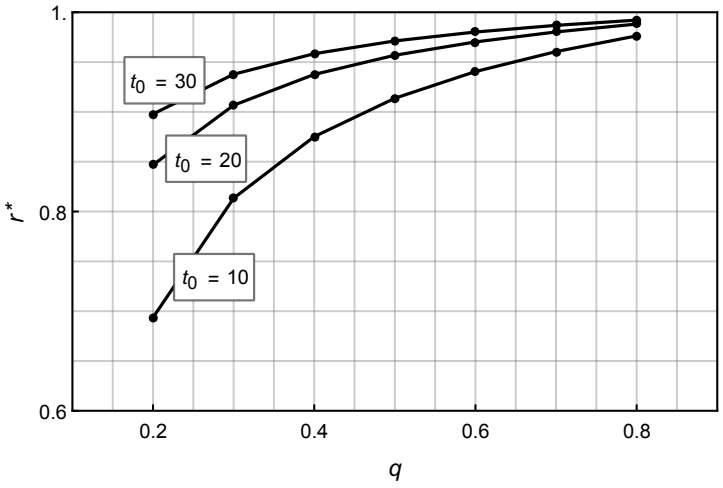

Рис. 4. Величина r^* как функция q при $t_0 = 10, 20, 30$

Fig. 4. The value r^* as a function of q for $t_0 = 10, 20, 30$

Здесь x^* — корень уравнения (25), принадлежащий отрезку $[1 - q, 1]$. На рис. 4 приведены результаты численного моделирования величины r^* как функции q для трех различных значений t_0. Видно, что с ростом q эта величина асимптотически стремится к единице, сужая, тем самым, допустимую область параметра защиты r.

ПРИМЕР 2. Рассмотрим систему с двумя угрозами, вероятности которых равны q_1 и q_2. Согласно (26) и (27) допустимая область параметров защиты — это выпуклая область

$$R_{t_0}(q_1, q_2) = \{(r_1, r_2) \in \mathbb{R}^2_+ \colon r_1 \le 1,\ r_2 \le 1,\ q_1 r_1 + q_2 r_2 \le x^*(x^* - 1 + q_1 + q_2)\},$$

где x^* — корень уравнения (25), принадлежащий отрезку $[q_1 + q_2, 1]$. В качестве примера на рис. 5 графически изображены допустимые области при $q_1 = 0.25$ и $q_2 = 0.45$ для моментов времени $t_0 = 10, 20, 30$.

В заключение обсудим возможное приложение полученных результатов к задаче выбора оптимального набора значений параметров защиты. Данная задача имеет важное прикладное значение, например, при проектировании и разработке систем защиты информации [17, 18].

С помощью описанного выше алгоритма мы можем сузить множество возможных значений параметров защиты до множества $R_{t_0}(q_1, \ldots, q_n)$, однако в пределах этой области выбор их более ничем не ограничен. Для дальнейшей конкретизации значений $r_1, \ldots, r_n$ нам необходимы дополнительные условия, сужающие область параметров защиты, например, до одной конкретной точки. Естественной постановкой задачи, гарантирующей единственность соответствующего решения, является задача поиска минимума (или максимума) некоторой целевой функции $I(r_1, \ldots, r_n)$, рассматриваемой на области $R_{t_0}(q_1, q_2, \ldots, q_n)$. В простейшем варианте целевая функция может быть выбрана линейной по переменным $r_1, \ldots, r_n$

$$I(r_1, \ldots, r_n) = \sum_{i=1}^{n} c_i r_i, \tag{28}$$

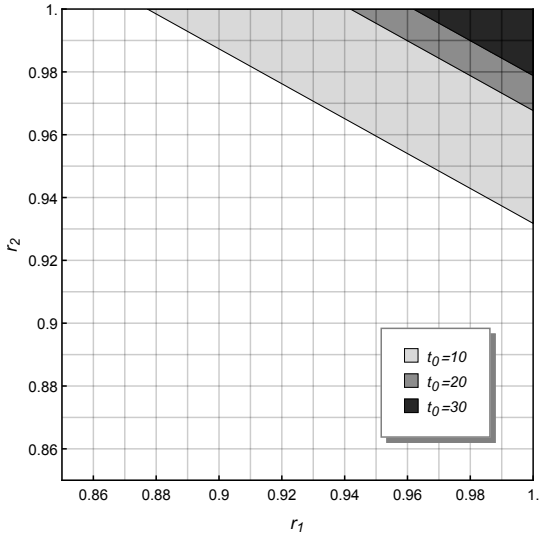

Рис. 5. Допустимая область $R_{t_0}(0.25, 0.45)$ при $t_0 = 10, 20, 30$

Fig. 5. The permitting domain $R_{t_0}(0.25, 0.45)$ for $t_0 = 10, 20, 30$

где c_i — некоторые заданные коэффициенты, интерпретация которых (как и целевой функции I) зависит от решаемой оптимизационной задачи. В такой постановке задача поиска минимума (или максимума) целевой функции (28) на выпуклой области $R_{t_0}(q_1, \ldots, q_n)$ представляет собой стандартную задачу линейного программирования, решению которой посвящена обширная литература (см., например, [19]).

Заключение

Рассмотрена модель угроз информационной безопасности, описываемая в терминах марковских процессов. Динамика модели представляется последовательностью сбоев и восстановлений компьютерной системы, происходящих в результате воздействия случайных внешних угроз. Получены явные аналитические формулы для вероятностей состояний системы, обсуждаются их некоторые предельные случаи и анализируется поведение системы на больших временах. Исследована зависимость вероятности безопасного состояния системы от вероятностей угроз; в частности, показано, что эта зависимость качественно различается для четных и нечетных моментов времени. Также введена важная характеристика модели — время релаксации, с помощью которой определяется допустимая область значений параметров защиты системы и приводится алгоритм ее построения.

Список литературы / References

[1] Ye N. et al., “Robustness of the Markov-Chain Model for Cyber-Attack Detection”, *IEEE Transactions on Reliability*, **53**:1 (2004), 116–123.

[2] Fava D. et al., "Projecting Cyberattacks through Variable-Length Markov Models", *IEEE Transactions on Information Forensics and Security*, **3**:3 (2008), 359–369.

[3] Piétre-Cambacédès L., Bouissou M., "Beyond Attack Trees: Dynamic Security Modeling with Boolean Logic Driven Markov Processes (BDMP)", *Proceedings of the 2010 European Dependable Computing Conference*, IEEE Computer Society, 2010, 199–208.

[4] Далингер Я. М. и др., "Математические модели распространения вирусов в компьютерных сетях различной структуры", *Информатика и системы управления*, 2011, № 4, 3–11; [Dalinger Ya. M. et al., "The mathematical models of the spreading of viruses in computer networks with the diferent structures", *Information Science and Control Systems*, 2011, № 4, 3–11, (in Russian).]

[5] Ye N., "A Markov Chain Model of Temporal Behavior for Anomaly Detection", *Proceeding on the 2000 IEEE Systems, Man, and Cybern. Information Assurance and Security Workshop*, IEEE Computer Society, 2000, 171–174.

[6] Kovalev S. M., Sukhanov A. V., "Anomaly detection based on Markov chain model with production rules", *Software and Systems*, **107**:3 (2014), 40–43.

[7] Богатырев В. А. и др., "Оптимизация интервалов проверки информационной безопасности систем", *Научно-технический вестник информационных технологий, механики и оптики*, 2014, № 5 (93), 119–125; [Bogatyrev V. A. et al., "Intervals optimization of systems information security inspection", *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2014, № 5 (93), 119–125, (in Russian).]

[8] Щеглов К. А. и др., "Математические модели эксплуатационной информационной безопасности", *Вопросы защиты информации*, 2014, № 3, 52–65; [Shcheglov K. A. et al., "Mathematical models of operational information security", *Information security questions*, 2014, № 3, 52–65, (in Russian).]

[9] Vobbilisetty R. et al., "Classic Cryptanalysis Using Hidden Markov Models", *Cryptologia*, **41**:1, 1–28.

[10] Austin T. H. et al., "Exploring Hidden Markov Models for Virus Analysis: a Semantic Approach", *Proceedings of the 2013 46th Hawaii International Conference on System Sciences*, IEEE Computer Society, 2013, 5039–5048.

[11] Клименко Е. С., Росенко А. П., "Марковская модель оценки влияния внутренних угроз на безопасность конфиденциальной информации", *Известия ЮФУ. Технические науки*, 2007, № 4(76), 123–126; [Klimenko E. S., Rosenko A. P., "Markovskaya model otsenki vliyaniya vnutrennikh ugroz na bezopasnost konfidentsialnoy informatsii", *Izvestiya SFedU. Engineering Sciences*, 2007, № 4(76), 123–126, (in Russian).]

[12] Росенко А. П., "Математическое моделирование влияния внутренних угроз на безопасность конфиденциальной информации, циркулирующей в автоматизированной информационной системе", *Известия ЮФУ. Технические науки*, 2008, № 8(85), 71–81; [Rosenko A. P., "Mathematical Modelling of Internal Threats on Safety of the Confidential Information Circulating in Automated Information System Availability", *Izvestiya SFedU. Engineering Sciences*, 2008, № 8(85), 71–81, (in Russian).]

[13] Щеглов К. А., Щеглов А. Ю., "Марковские модели угрозы безопасности информационной системы", *Известия высших учебных заведений. Приборостроение*, **58**:12 (2015), 957–965; [Shcheglov K. A., Shcheglov A. Yu., "Markov models for informational system security threat", *Izvestiya Vysshikh Uchebnykh Zavedeniy. Priborostroenie*, **58**:12 (2015), 957–965, (in Russian).]

[14] Щеглов К. А., Щеглов А. Ю., "Моделирование угрозы безопасности информационной системы с использованием аппроксимирующих функций", *Известия высших учебных заведений. Приборостроение*, **59**:1 (2016), 50–59; [Shcheglov K. A., Shcheglov A. Yu., "Modeling of information system security threat using approximating functions", *Izvestiya Vysshikh Uchebnykh Zavedeniy. Priborostroenie*, **59**:1 (2016), 50–59, (in Russian).]

[15] Беляев Ю. К. и др., *Математические методы в теории надежности*, Наука, 1963, 524 с.; English transl.: Gnedenko B. V. et al., *Mathematical Methods of Reliability Theory*, Academic Press, 1969, 503 pp.

[16] Rausand M, Hoyland A., *System Reliability Theory: Models, Statistical Methods, and Applications*, John Wiley & Sons, 2004, 664 pp.

[17] Овчинников А. И. и др., "Математическая модель оптимального выбора средств защиты от угроз безопасности вычислительной сети предприятия", *Вестник Московского государственного технического университета им. Н.Э. Баумана. Серия «Приборостроение»*, 2007, № 3, 115–121; [Ovchinnikov A. I. et al., "Mathematical Model of Optimal Selection of Aids of Protection Against Threats for Safety of Enterprise Computer Network", *Herald of the Bauman Moscow State Technical University. Series Instrument Engineering*, 2007, № 3, 115–121, (in Russian).]

[18] Завгородний В. И., "Системное управление информационными рисками. Выбор механизмов защиты", *Проблемы управления*, 2009, № 1, 53–58; [Zavgorodniy V. I., "System management of information risks: choice of mechanisms for protection against information risks", *Problemy Upravleniya*, 2009, № 1, 53–58, (in Russian).]

[19] Юдин Д. Б., Гольштейн Е. Г., *Линейное программирование. Теория, методы и приложения*, Наука, 1969, 424 с.; [Yudin D. B., Gol'shteyn E. G., *Lineynoe programmirovanie. Teoriya, metody i prilozheniya*, Nauka, 1969, 424 pp., (in Russian).]

Magazev A. A., Tsyrulnik V. F., "Investigation of a Markov Model for Computer System Security Threats", *Modeling and Analysis of Information Systems*, **24**:4 (2017), 445–458.

DOI: 10.18255/1818-1015-2017-4-445-458

Abstract. In this work, a model for computer system security threats formulated in terms of Markov processes is investigated. In the framework of this model the functioning of the computer system is considered as a sequence of failures and recovery actions which appear as results of information security threats acting on the system. We provide a detailed description of the model: the explicit analytical formulas for the probabilities of computer system states at any arbitrary moment of time are derived, some limiting cases are discussed, and the long-run dynamics of the system is analysed. The dependence of the security state probability (i.e. the state for which threats are absent) on the probabilities of threats is separately investigated. In particular, it is shown that this dependence is qualitatively different for odd and even moments of time. For instance, in the case of one threat the security state probability demonstrates non-monotonic dependence on the probability of threat at even moments of time; this function admits at least one local minimum in its domain of definition. It is believed that the mentioned feature is important because it allows to locate the most dangerous areas of threats where the security state probability can be lower then the permissible level. Finally, we introduce an important characteristic of the model, called the relaxation time, by means of which we construct the permitting domain of the security parameters. Also the prospects of the received results application to the problem of finding the optimal values of the security parameters is discussed.

Keywords: computer system, security threat, Markov process

On the authors:
Alexey A. Magazev, orcid.org/0000-0002-8725-9183, PhD,
Omsk State Technical University, 11 Mira pr., Omsk, 644050, Russia,
e-mail: magazev@mail.ru

Valeria F. Tsyrulnik, orcid.org/0000-0002-6875-7216, student,
Omsk State Technical University, 11 Mira pr., Omsk, 644050, Russia,
e-mail: lera.tsyrulnik@mail.ru