Математические структуры и моделирование 2020. № 4(56). С. 112–125

УДК 004.056
DOI 10.24147/2222-8772.2020.4.112-125

ОЦЕНКА СРЕДНЕГО ВРЕМЕНИ ДО ОТКАЗА БЕЗОПАСНОСТИ НА ОСНОВЕ МАРКОВСКИХ ЦЕПЕЙ С НЕПРЕРЫВНЫМ ВРЕМЕНЕМ

А. А. Магазев
д.ф.-м.н., профессор, кафедра «Комплексная защита информации»,
e-mail: magazev@omgtu.ru
А. С. Мельникова
магистрант, кафедра «Комплексная защита информации»,
e-mail: anastasiya_m.96@mail.ru
В. Ф. Цырульник
аспирант, кафедра «Комплексная защита информации», e-mail: lera.tsyrulnik@mail.ru

Омский государственный технический университет, Омск, Россия

Аннотация. В статье рассматривается марковская модель компьютерных атак, в рамках которой атаки и ответные действия со стороны системы моделируются простейшими пуассоновскими потоками событий. Описан метод решения соответствующей системы уравнений Колмогорова с помощью вычисления собственных векторов и собственных чисел некоторой матрицы. Детально исследована важная случайная величина, ассоциированная с соответствующим марковским случайным процессом и называемая временем до отказа безопасности. Представлены результаты сравнения полученных результатов с результатами имитационного моделирования.

Ключевые слова: марковская цепь с непрерывным временем, уравнения Колмогорова, среднее время до отказа безопасности.

Введение

Оценка эффективности систем защиты информации представляет собой важную задачу информационной безопасности. Стоит, однако, отметить, что данная проблема всё ещё плохо поддаётся формализации, во многом из-за большого разнообразия актуальных угроз кибербезопасности и структурной сложности информационных систем, на которые эти угрозы направлены. Существующие нормативно-правовые механизмы подобной оценки (например, требования регуляторов сферы ИБ) носят, в основном, качественный характер и не учитывают множество тонких аспектов развития современных информационных технологий. В то же время подобные аспекты являются довольно актуальными, например, в коммерческом секторе, где владельцы защищаемой информации заинтересованы в более гибких и своевременных способах управления инвестициями в кибербезопасность.

Одним из современных направлений решения проблемы оценки защищённости информации является стохастическое моделирование и основанное на нём использование так называемых *метрик безопасности* (см. [1–3]). Последние представляют собой наборы количественных характеристик, правильная агрегация которых может служить оценкой уровня защищённости моделируемой компьютерной системы. Одной из наиболее часто применяемых метрик безопасности является *время до отказа безопасности*, то есть время, прошедшее до момента совершения события, ассоциируемого с нарушением режима безопасности. В качестве примера приведём работу [3], в которой авторы вычисляют эту метрику, основываясь на результатах моделирования компьютерных систем с помощью полумарковских цепей.

В статье [4] была предложена марковская модель с непрерывным временем, в которой кибератаки (или киберугрозы) моделируются простейшими пуассоновскими потоками событий. В настоящей статье мы более подробно исследуем эту марковскую модель; в частности, описываем алгебраический метод решения соответствующей системы уравнений Колмогорова, основанный на вычислении собственных чисел и собственных векторов некоторой матрицы. Далее мы определяем время до отказа безопасности как время, прошедшее с момента $t = 0$ до момента попадания системы в так называемое состояние *отказа безопасности*. После этого мы детально описываем эту случайную величину, вычислив её функцию плотности вероятности и получив формулы для её моментов произвольного порядка. В конце нашей статьи мы приводим результаты сравнения полученных нами теоретических результатов с результатами имитационного моделирования.

1. Моделирование кибератак с помощью марковских цепей с непрерывным временем

Рассмотрим некоторую компьютерную систему (далее просто *систему*), потенциально уязвимую для n различных кибератак. Под *кибератакой* мы понимаем любую попытку воздействия на систему, целью которой является несанкционированный доступ, уничтожение, модификация или кража информационных активов.

Опишем математическую модель, в рамках которой возможно количественное описание как самих кибератак, так и ответных действий со стороны системы [4]. Во-первых, мы будем предполагать, что последовательность появлений любой i-ой кибератаки представляет собой простейший пуассоновский поток событий с интенсивностью λ_i. Наше второе предположение состоит в том, что последовательность встречных действий (защитных реакций) со стороны системы также распределена в соответствии с пуассоновским распределением; интенсивность соответствующего потока мы обозначим μ_i, а вероятность успешного отражения i-ой кибератаки — r_i. Таким образом, наша модель описывается с помощью $3n$ входных параметров:

- $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_n)$ — интенсивности потоков кибератак;
- $\mu = (\mu_1, \mu_2, \ldots, \mu_n)$ — интенсивности потоков отражений кибератак;

• $r = (r_1, r_2, \ldots, r_n)$ — вероятности отражения кибератак.

По своему смыслу эти параметры подчиняются следующим требованиям:

$$\lambda_i \geqslant 0, \quad \mu_i \geqslant 0, \quad 0 \leqslant r_i \leqslant 1, \quad i = 1, 2, \ldots, n.$$

В соответствии со сделанными предположениями, наша система может быть описана в терминах некоторой модели конечных состояний. Состояние s_0, в котором система не подвергается никаким кибератакам, мы будем называть *безопасным состоянием*. Состояние, ассоциированное с появлением i-ой кибератаки, мы обозначаем s_i и называем *состоянием i-ой кибератаки*. В этом состоянии система находится некоторое время, имеющее пуассоновское распределение с параметром μ_i. По истечении этого времени данная кибератака будет либо отражена с вероятностью r_i, либо не отражена с вероятностью $\bar{r}_i \equiv 1 - r_i$. В первом случае система возвращается в безопасное состояние s_0, во втором — переходит в состояние *отказа безопасности* s_{n+1}.

Состояние отказа безопасности s_{n+1} мы будем считать финальным, то есть система, однажды оказавшись в этом состоянии, останется в нём навсегда. Это состояние означает успешную реализацию атаки, что влечёт за собой определённые негативные последствия для системы (кража информации, финансовые потери и т. д.). Очевидно, на практике это состояние не является конечным; после осуществления различных восстановительных мероприятий система может быть возвращена в безопасное состояние s_0. Подобные действия, однако, выходят за рамки рассматриваемой модели, и мы их учитывать не будем.

На основе изложенных выше положений мы можем сделать вывод о том, что вероятность состояний системы в будущем зависит только от того, в каком состоянии система находится в настоящем, и не зависит от её поведения в прошлом. Это позволяет нам трактовать последовательность состояний системы как *марковский процесс* с непрерывным временем и конечным числом состояний. Общее представление о данном случайном процессе даёт размеченный граф состояний системы, показанный на рис. 1.

Обозначим $p_i(t)$ вероятность того, что система в момент времени t находится в состоянии s_i, $i = 0, 1, \ldots, n+1$. Как известно, эти вероятности могут быть найдены путём решения системы обыкновенных дифференциальных уравнений первого порядка, называемых *уравнениями Колмогорова*. В нашем случае эти уравнения легко могут быть выписаны с использованием размеченного графа состояний, изображённого на рис. 1:

$$\frac{dp_0(t)}{dt} = -\lambda_0 p_0(t) + \sum_{k=1}^{n} \mu_k r_k p_k(t); \tag{1}$$

$$\frac{dp_i(t)}{dt} = \lambda_i p_0(t) - \mu_i p_i(t), \quad i = 1, \ldots, n; \tag{2}$$

$$\frac{dp_{n+1}(t)}{dt} = \sum_{k=1}^{n} \mu_k \bar{r}_k p_k(t). \tag{3}$$

Здесь мы ввели дополнительное обозначение $\lambda_0 \equiv \sum_{i=1}^{n} \lambda_i$. Для однозначного определения вероятностей $p_i(t)$ требуется задать их значения в начальный

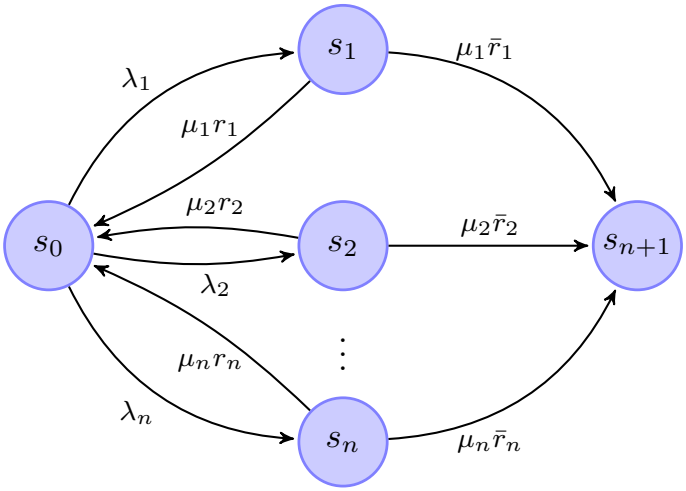

Рис. 1. Размеченный граф состояний системы

момент времени $t = 0$; мы сделаем это, наложив условие

$$p_0(0) = 1, \quad p_1(0) = p_2(0) = \cdots = p_{n+1}(0) = 0, \tag{4}$$

означающее, что в момент времени $t = 0$ система находится в безопасном состоянии s_0. Решение задачи Коши (1)–(4) полностью определяет динамику системы.

В практических вычислениях удобнее всего представлять систему уравнений (1)–(3) в матричной форме

$$\frac{d\mathbf{p}(t)}{dt} = \mathbf{p}(t) \cdot \Pi. \tag{5}$$

Здесь $\mathbf{p}(t) = (p_0(t), p_1(t), \ldots, p_{n+1}(t))$ — вектор вероятностей состояний системы в момент t, а квадратная матрица Π порядка $n + 2$ имеет вид

$$\Pi = \begin{pmatrix} -\lambda_0 & \lambda_1 & \lambda_2 & \ldots & \lambda_n & 0 \\ \mu_1 r_1 & -\mu_1 & 0 & \ldots & 0 & \mu_1\bar{r}_1 \\ \mu_2 r_2 & 0 & -\mu_2 & \ldots & 0 & \mu_2\bar{r}_2 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ \mu_n r_n & 0 & 0 & \ldots & -\mu_n & \mu_n\bar{r}_n \\ 0 & 0 & 0 & \ldots & \ldots & 0 \end{pmatrix}. \tag{6}$$

Матрица Π обладает следующим важным свойством: сумма элементов каждой её строки равна нулю.

2. Алгебраический метод решения уравнений Колмогорова

Перед тем как заняться решением задачи (1)–(4) в общем случае, рассмотрим две частные ситуации, в которых эту задачу можно сравнительно легко

решить в аналитическом виде.

ПРИМЕР 1 (случай отсутствия кибератак). Пусть $\lambda_i = 0$ для всех i. В этой ситуации решение задачи Коши (1)–(4) имеет простой вид:

$$p_0(t) = 1, \quad p_1(t) = p_2(t) = \cdots = p_{n+1}(t) = 0.$$

Данное решение иллюстрирует тривиальный факт: в отсутствие кибератак система всегда будет находиться в безопасном состоянии.

ПРИМЕР 2 (случай отсутствия защиты). Предположим, что $r_i = 0$ для всех i. Если ни один параметр μ_i не совпадает с λ_0, решение задачи (1)–(4) также находится элементарно

$$p_0(t) = e^{-\lambda_0 t};$$

$$p_i(t) = \frac{\lambda_i}{\lambda_0 - \mu_i}\left(e^{-\mu_i t} - e^{-\lambda_0 t}\right), \quad i = 1, \ldots, n;$$

$$p_{n+1}(t) = 1 - e^{-\lambda_0 t} - \sum_{j=1}^{n} \frac{\lambda_j}{\lambda_0 - \mu_j}\left(e^{-\mu_j t} - e^{-\lambda_0 t}\right).$$

Отсюда видно, что с ростом t вероятность обнаружения системы в безопасном состоянии s_0 экспоненциально уменьшается, а в состоянии s_{n+1}, напротив, увеличивается и стремится к единице. Отметим, что хотя случаи, когда некоторые из μ_i совпадают с λ_0, необходимо рассматривать отдельно, получить аналитическое решение не составляет труда и в таких ситуациях.

Вернёмся к общему случаю. Обычно для построения общего решения системы уравнений Колмогорова с постоянными коэффициентами широко применяется преобразование Лапласа. В нашем случае, однако, более удобным будет метод, использующий собственные числа и собственные векторы матрицы (6). Предварительно отметим некоторую полезную информацию о собственных числах матрицы П.

Предложение 1. *Все собственные числа матрицы* (6) *вещественны и принадлежат отрезку* $[-2\gamma, 0]$*, где* $\gamma = \max\{\lambda_0, \mu_1, \ldots, \mu_n\}$.

Доказательство. Вещественность собственных чисел матрицы (6) следует из результата Дрейзина и Хейнсворса, приведённого в работе [5]. Доказательство второй части утверждения базируется на теореме Гершгорина (см., например, монографию [6]), согласно которой все собственные значения матрицы (6) заключены в объединении $n + 1$ отрезков

$$[-2\lambda_0, 0] \cup [-2\mu_1, 0] \cup [-2\mu_2, 0] \cup \cdots \cup [-2\mu_n, 0].$$

Отсюда следует, что всякое собственное число будет принадлежать отрезку $[-2\gamma, 0]$, где γ — максимум из чисел $\lambda_0, \mu_1, \ldots, \mu_n$. ■

Отметим, что в силу наличия в матрице (6) нулевой строки, матрица П всегда имеет одно нулевое собственное число $\sigma_0 = 0$. Таким образом, спектр матрицы (6) имеет следующую структуру

$$\mathrm{Spec}(\Pi) = \{\sigma_0 = 0, -|\sigma_1|, -|\sigma_2|, \ldots, -|\sigma_{n+1}|\},$$

где $\sigma_1, \ldots, \sigma_{n+1}$ — отрицательные вещественные числа (для упрощения дальнейших рассуждений мы будем считать, что спектр матрицы (6) является простым).

Из общей теории систем линейных однородных дифференциальных уравнений с постоянными коэффициентами известно, что система (5) имеет $n+2$ линейно независимых решения вида

$$\mathbf{p}_0(t) = \mathbf{c}_0, \quad \mathbf{p}_1(t) = \mathbf{c}_1 e^{\sigma_1 t}, \quad \mathbf{p}_2(t) = \mathbf{c}_2 e^{\sigma_2 t}, \quad \ldots, \quad \mathbf{p}_{n+1}(t) = \mathbf{c}_{n+1} e^{\sigma_{n+1} t},$$

где $\mathbf{c}_\nu$ — левый собственный вектор матрицы Π, отвечающий собственному значению σ_ν, $\nu = 0, 1, \ldots, n+1$.

Выберем собственные векторы $\mathbf{c}_\nu$ так, чтобы выполнялось условие $\sum_{\nu=0}^{n+1} \mathbf{c}_\nu = \mathbf{e}_0$, где $\mathbf{e}_0 = (1, 0, \ldots, 0)$ — вектор с единицей в первой позиции и с нулями в остальных. Тогда решение системы уравнений Колмогорова (1)–(3), удовлетворяющее начальному условию (4), будет иметь вид

$$\mathbf{p}(t) = \sum_{\nu=0}^{n+1} \mathbf{c}_\nu e^{\sigma_\nu t} = \mathbf{c}_0 + \mathbf{c}_1 e^{\sigma_1 t} + \cdots + \mathbf{c}_{n+1} e^{\sigma_{n+1} t}. \tag{7}$$

Последняя формула в покомпонентной записи может быть переписана как

$$p_i(t) = \delta_{i,n+1} + \sum_{\nu=1}^{n+1} c_{\nu,i} e^{\sigma_\nu t}, \quad i = 0, \ldots, n+1, \tag{8}$$

где через $c_{\nu,i}$ обозначена i-ая компонента собственного вектора $\mathbf{c}_\nu$, δ_{ij} — символ Кронеккера и, кроме того, мы учли тот факт, что собственный вектор, отвечающий собственному числу $\sigma_0 = 0$, имеет вид $\mathbf{c}_0 = (0, \ldots, 0, 1)$. Начальное условие (4) также может быть выражено в терминах собственных векторов $\mathbf{c}_\nu = (c_{\nu,i})$:

$$\sum_{\nu=1}^{n+1} c_{\nu,i} = \delta_{0,i} - \delta_{n+1,i}, \quad i = 0, 1, \ldots, n+1. \tag{9}$$

Резюмируя полученные результаты, приведем пошаговый алгоритм решения задачи Коши (1)–(4), который может быть легко реализован в помощью современных математических пакетов.

Шаг 1. По заданным входным параметрам модели λ, μ и r формируем матрицу Π в соответствии с формулой (6).

Шаг 2. Находим собственные числа σ_ν и собственные векторы $\mathbf{c}_\nu = (c_{\nu,i})$ матрицы Π.

Шаг 3. Решаем систему линейных однородных уравнений $\sum_{\nu=0}^{n+1} a_\nu c_{\nu,i} = \delta_{0,i}$ относительно неизвестных a_ν и делаем замену $\mathbf{c}_\nu \to a_\nu \mathbf{c}_\nu$ для всех $\nu = 0, 1, \ldots, n+1$.

Шаг 4. Выписываем решение задачи Коши (1)–(4) в соответствии с формулой (7).

ПРИМЕР 3. Приведём численный пример. Рассмотрим модель со следующими значениями входных параметров:

$$n = 3, \quad \lambda = (4.28, 3.97, 1.13), \quad \mu = (0.92, 0.42, 0.95), \quad r = (0.10, 0.40, 0.38). \tag{10}$$

В этом случае матрица (6) записывается как

$$\Pi = \begin{pmatrix} -9.38 & 4.28 & 3.97 & 1.13 & 0. \\ 0.092 & -0.92 & 0. & 0. & 0.828 \\ 0.168 & 0. & -0.42 & 0. & 0.252 \\ 0.361 & 0. & 0. & -0.95 & 0.589 \\ 0. & 0. & 0. & 0. & 0. \end{pmatrix}.$$

Спектр этой матрицы имеет вид

$$\mathrm{Spec}(\Pi) = \{0., -9.5462, -0.9374, -0.8529, -0.3335\}.$$

Соответствующие собственные векторы $\mathbf{c}_\nu$, нормированные условием $\sum_{\nu=0}^{4} \mathbf{c}_\nu = (1, 0, 0, 0, 0)$, равны

$$\begin{aligned} \mathbf{c}_0 &= (0, 0, 0, 0, 1); \\ \mathbf{c}_1 &= (0.9815, -0.4870, -0.4270, -0.1290, 0.0615); \\ \mathbf{c}_2 &= (0.0003, -0.0635, -0.0020, 0.0232, 0.0421); \\ \mathbf{c}_3 &= (0.0074, 0.4716, -0.0678, 0.0860, -0.4972); \\ \mathbf{c}_4 &= (0.0108, 0.07896, 0.4968, 0.0198, -0.6064). \end{aligned}$$

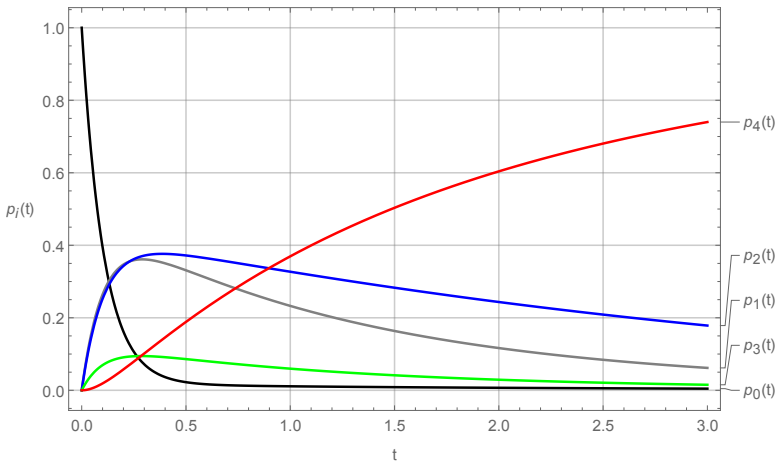

Рис. 2. Графики функций $p_i(t)$ при $\lambda = (4.28, 3.97, 1.13)$, $\mu = (0.92, 0.42, 0.95)$ и $r = (0.10, 0.40, 0.38)$.

Отсюда в соответствии с формулой (7) получаем следующее решение задачи Коши (1)–(4):

$$p_0(t) = +0.9815e^{-9.5462t} + 0.0003e^{-0.9374t} + 0.0074e^{-0.8529t} + 0.0108e^{-0.3335t},$$
$$p_1(t) = -0.4870e^{-9.5462t} - 0.0635e^{-0.9374t} + 0.4716e^{-0.8529t} + 0.0790e^{-0.3335t},$$
$$p_2(t) = -0.4270e^{-9.5462t} - 0.0020e^{-0.9374t} - 0.0678e^{-0.8529t} + 0.4968e^{-0.3335t},$$
$$p_3(t) = -0.1290e^{-9.5462t} + 0.0232e^{-0.9374t} + 0.0860e^{-0.8529t} + 0.0198e^{-0.3335t},$$
$$p_4(t) = 1 + 0.0615e^{-9.5462t} + 0.0421e^{-0.9374t} - 0.4972e^{-0.8529t} - 0.6064e^{-0.3335t}.$$

На рис. 2 приведены зависимости полученных вероятностей $p_i(t)$ от времени на отрезке $[0, 3]$.

3. Время до отказа безопасности

Стохастическое моделирование кибератак часто используется как вспомогательный инструмент для строгой теоретической оценки различных количественных характеристик систем защиты информации, отражающих их эффективность. Одной из таких характеристик является время до отказа безопасности, определяемое как время, прошедшее с момента $t = 0$ до момента попадания системы в конечное состояние, ассоциированное с успешной реализацией какой-либо из кибератак [3, 7, 8]. Приведём определение этой величины в рамках рассматриваемой марковской модели.

Определение 1. Время $T \in [0, +\infty)$, прошедшее с момента $t = 0$, когда система находилась в состоянии безопасности s_0, до момента $t = T$ попадания системы в финальное состояние s_{n+1}, называется *временем до отказа безопасности*.

Ясно, что T — непрерывная случайная величина. Исследуем подробнее её вероятностное распределение.

Пусть $F_T(t)$ — функция распределения непрерывной случайной величины T, а $f_T(t)$ — её плотность распределения. Считая, что $F_T(t)$ — дифференцируемая функция, имеем $f_T(t) = F'_T(t)$. По своему смыслу значение функции распределения в момент t даёт вероятность того, что величина T будет меньше либо равна t, то есть $F_T(t) = P\{T \leqslant t\}$. Указанная вероятность, в свою очередь, совпадает с вероятностью того, что в момент t система находится в состоянии s_{n+1}: $F_T(t) = p_{n+1}(t)$. Отсюда мы имеем $f_T(t) = p'_{n+1}(t)$ или в силу равенства (8):

$$f_T(t) = \sum_{\nu=1}^{n+1} c_{\nu,n+1}\sigma_\nu e^{\sigma_\nu t}. \tag{11}$$

Нетрудно убедиться, что полученная функция действительно удовлетворяет условию нормировки, так как

$$\int_0^{+\infty} f_T(t)dt = \sum_{\nu=1}^{n+1} c_{\nu,n+1}\sigma_\nu \int_0^{+\infty} e^{\sigma_\nu t}dt = \sum_{\nu=1}^{n+1} c_{\nu,n+1}\sigma_\nu \cdot \frac{1}{\sigma_\nu} = \sum_{\nu=1}^{n+1} c_{\nu,n+1} = 1,$$

где мы учли условие (9).

Получим теперь формулы, в соответствии с которыми мы сможем вычислять числовые характеристики времени до отказа безопасности в терминах собственных значений и собственных векторов матрицы Π.

Предложение 2. *k-ые начальные моменты случайной величины T даются формулой*

$$\mu_k[T] = -\sum_{\nu=1}^{n+1} \frac{c_{\nu,n+1}}{|\sigma_\nu|^k}, \tag{12}$$

где $c_{\nu,n+1}$ — $(n+1)$-ая компонента собственного вектора $\mathbf{c}_\nu$ матрицы (6)*, отвечающего собственному числу σ_ν. В частности, математическое ожидание $\tau \equiv \mu_1[T]$ случайной величины T вычисляется как*

$$\tau = \sum_{\nu=1}^{n+1} \frac{c_{\nu,n+1}}{\sigma_\nu}. \tag{13}$$

Доказательство. Используя формулы (8) и (11), в соответствии с определением k-го начального момента, имеем

$$\mu_k[T] = \int_0^{+\infty} t^k f_T(t)dt = \sum_{\nu=1}^{n+1} c_{\nu,n+1}\sigma_\nu \int_0^{+\infty} t^k e^{\sigma_\nu t}dt. \tag{14}$$

Так как $\sigma_\nu < 0$ для всех $\nu = 1, \ldots, n+1$, интегралы в правой части полученного равенства сходятся и равны:

$$\int_0^{+\infty} t^k e^{\sigma_\nu t}dt = \frac{k!}{|\sigma_\nu|^{k+1}}. \tag{15}$$

Подставляя (15) в (14), получаем формулу (12). В частности, при $k = 1$ мы приходим к формуле (13). ■

Определение 2. Математическое ожидание τ случайной величины T будем называть *средним временем до отказа безопасности*.

Очевидно, что среднее время до отказа безопасности является одним из показателей эффективности имеющихся средств защиты от кибератак. В частности, на основе данной числовой характеристики мы можем сделать вывод о достаточности применяемых механизмов защиты или, напротив, о необходимости добавочных инвестиций в кибербезопасность.

Приведём несколько примеров вычисления среднего времени до отказа безопасности.

ПРИМЕР 4 (случай отсутствия защиты). Если $r_i = 0$ для всех i, тогда собственные числа матрицы Π равны $\sigma_0 = 0$, $\sigma_1 = -\mu_1$, $\ldots$, $\sigma_n = -\mu_n$, $\sigma_{n+1} =$

$-\lambda_0$. Соответствующие собственные векторы $\mathbf{c}_\nu$, удовлетворяющие требованию $\sum_{\nu=0}^{n+1} \mathbf{c}_\nu = \mathbf{e}_0$, имеют вид

$$\begin{aligned}
&\mathbf{c}_0 = (0, 0, 0, \ldots, 0, 1)\,,\\
&\mathbf{c}_1 = \left(0, \frac{\lambda_1}{\lambda_0 - \mu_1}, 0, \ldots, 0, -\frac{\lambda_1}{\lambda_0 - \mu_1}\right),\\
&\mathbf{c}_2 = \left(0, 0, \frac{\lambda_2}{\lambda_0 - \mu_2}, \ldots, 0, -\frac{\lambda_2}{\lambda_0 - \mu_2}\right),\\
&\ldots\\
&\mathbf{c}_n = \left(0, 0, 0, \ldots, \frac{\lambda_n}{\lambda_0 - \mu_n}, -\frac{\lambda_n}{\lambda_0 - \mu_n}\right),\\
&\mathbf{c}_{n+1} = \left(1, -\frac{\lambda_1}{\lambda_0 - \mu_1}, -\frac{\lambda_2}{\lambda_0 - \mu_2}, \ldots, -\frac{\lambda_n}{\lambda_0 - \mu_n}, \sum_{j=1}^{n} \frac{\lambda_j}{\lambda_0 - \mu_j} - 1\right).
\end{aligned}$$

Отсюда согласно формуле (13) для величины τ получаем следующее выражение

$$\tau = \frac{1}{\lambda_0}\left(1 + \sum_{i=1}^{n} \frac{\lambda_i}{\mu_i}\right). \tag{16}$$

В частности, при $n = 1$ имеем $\tau = 1/\lambda_1 + 1/\mu_1$. Данный результат имеет простое толкование: время τ есть сумма среднего времени до кибератаки $1/\lambda_1$ и среднего времени продолжительности атаки $1/\mu_1$.

Таким образом, при отсутствии защиты среднее время до отказа безопасности может быть найдено в аналитическом виде.

ПРИМЕР 5. В общем случае получение аналитических выражений для τ громоздко, поэтому предпочтительнее вычислять эту метрику безопасности численно. Рассмотрим, например, систему с входными параметрами, указанными в примере 3 из предыдущего раздела. Так как собственные значения и собственные векторы матрицы П для этого примера выше уже найдены, сразу же воспользуемся формулой (13):

$$\tau = \frac{0.0615}{-9.5462} + \frac{0.0421}{-0.9374} + \frac{-0.4972}{-0.8529} + \frac{-0.6064}{-0.3335} = 2.34967.$$

Отметим, что если допустить, что в этом примере все $r_i = 0$, а λ_i и μ_i остаются неизменными, по формуле (16) мы бы получили оценку

$$\tau_{\min} \equiv \tau|_{r=0} = 1.7371,$$

то есть, как и ожидается, $\tau_{\min} < \tau$ в силу того, что присутствие защитных механизмов увеличивает среднее время до отказа безопасности.

В заключение этого раздела сформулируем алгоритм нахождения среднего времени до отказа безопасности.

Шаг 1. По заданным входным параметрам модели λ, μ и r, формируем матрицу П в соответствии с формулой (6).

`Шаг 2`. Находим собственные числа σ_ν и собственные векторы $\mathbf{c}_\nu = (c_{\nu,i})$ матрицы Π.

`Шаг 3`. Решаем систему линейных однородных уравнений $\sum_{\nu=0}^{n+1} a_\nu c_{\nu,i} = \delta_{0,i}$ на неизвестные a_ν и делаем замену $\mathbf{c}_\nu \to a_\nu \mathbf{c}_\nu$ для всех $\nu = 0, 1, \ldots, n+1$.

`Шаг 4`. В соответствии с формулой (13) вычисляем среднее время до отказа безопасности τ.

4. Сравнение с результатами имитационного моделирования

Для оценки адекватности приведённых выше аналитических результатов проведём их сравнение с результатами, полученными в ходе имитационного моделирования.

Имитационное моделирование марковской цепи с непрерывным временем, описанной в разделе 1, осуществлялось нами с помощью пакета прикладных программ MatLAB. Для этих целей мы реализовали следующий набор функций:

- `GetErlang`(λ, k) — моделирование случайной величины, имеющей распределение Эрланга k-го порядка с параметром $\lambda > 0$;
- `GetState`(X, λ, μ, r, k) — разыгрывание нового случайного состояния марковской цепи при условии, что в настоящий момент система находится в состоянии X; λ, μ и r — векторные параметры модели, k — порядок потока Эрланга;
- `LifeTime`(λ, μ, r, k) — разыгрывание частной реализации марковской цепи и вычисление соответствующего этой реализации времени до отказа безопасности.

В частности, опишем подробнее алгоритм работы функции `GetState`.

Состояние X марковской цепи представляется парой (t, m), где t — момент времени, в который система перешла в это состояние, m — номер состояния, $m = 0, 1, \ldots, n+1$. Функция `GetState` осуществляет переход $X \to X'$, где $X = (t, m)$ — текущее состояние цепи, $X' = (t', m')$ — новое состояние, в которое переходит марковская цепь. При этом в зависимости от значения m мы имеем следующие варианты данного перехода.

1. Пусть $m = 0$ (система находится в безопасном состоянии). Тогда с помощью функции `GetState` мы генерируем n случайных чисел $\tau_1, \ldots, \tau_n$, распределённых по пуассоновскому закону с параметрами $\lambda_1, \ldots, \lambda_n$ соответственно. Пусть $\tau_i = \min\{\tau_1, \ldots, \tau_n\}$ для некоторого $i \in \{1, \ldots, n\}$. Полагаем $t' = t + \tau_i$ и $m' = m + i$, то есть $X' = (t + \tau_i, i)$.

2. Пусть $1 \leqslant m \leqslant n$ (осуществляется m-ая кибератака). С помощью функции `GetState` генерируем случайное число τ, распределённое по пуассоновскому закону с параметром μ_m, после чего полагаем $t' = t + \tau$. Далее с помощью штатной функции `rand`, входящей в состав ядра MATLab, разыгрываем случайное число x, равномерно распределённое на отрезке $[0, 1]$. Если $x < r_m$, полагаем $m' = 0$; в обратном случае имеем $m' = n + 1$.

3. Пусть $m = n + 1$ (состояние «отказ безопасности»). Тогда полагаем $t' = t$ и $m' = m$, то есть $X' = X$.

Используя функцию `GetState`, мы можем разыгрывать различные реализации марковской цепи, то есть последовательности состояний вида

$$X_0 = (t_0, m_0) \to X_1 = (t_1, m_1) \to \cdots \to X_N = (t_N, m_N) \to \ldots.$$

Реализации, начинающиеся с состояния $X_0 = (0, 0)$, генерируются функцией `LifeTime`. При этом переходы $X \to X'$ осуществляются до тех пор, пока мы не получим $X' = (t_M, n + 1)$ для некоторого $M \in \mathbb{N}$. Выходное значение функции `LifeTime` — это число t_M, которое и представляет собой время до отказа безопасности, отвечающее данной реализации.

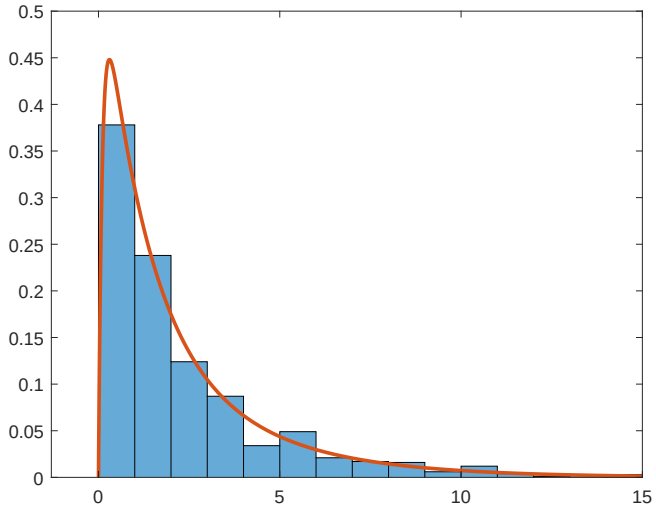

Рис. 3. Сравнение теоретической плотности распределения времени до отказа безопасности (сплошная кривая) с гистограммой, полученной по результатам имитационного моделирования

ПРИМЕР 6. В качестве конкретного примера проведём сравнение результатов, полученных в примерах 3 и 5, с результатами имитационного моделирования. Для этого $N = 1000$ раз мы запустим функцию `LifeTime`, выбрав в качестве значений параметров n, λ, μ и r величины (10). В результате получим 1000 возможных значений времени до отказа безопасности. На рис. 3 приведена гистограмма, построенная по полученным данным, а также теоретическая кривая плотности вероятности $f_T(t)$, полученная в результате дифференцирования функции $p_4(t)$, найденной в примере 3:

$$f_T(t) = -0.5869e^{-9.5462t} - 0.0395e^{-0.9374t} + 0.4240e^{-0.8529t} + 0.2022e^{-0.3335t}.$$

Из рисунка видно, что теоретическая и эмпирическая зависимости хорошо соответствуют друг другу.

Приведём также оценки для среднего времени до отказа безопасности, полученные в результате усреднения статистических испытаний, сводящихся к N запускам функции `LifeTime`. В таблице 1 указаны подобные оценки для $N = 10^3$, 10^4, 10^5 и 10^6. В последнем столбце приведена точная оценка, полученная в теоретических расчётах.

Таблица 1. Оценки среднего времени до отказа безопасности в имитационной модели при различном числе испытаний N

Число испытаний N	10^3	10^4	10^5	10^6	∞
Среднее время до отказа безопасности τ	2.3755	2.3576	2.3550	2.3471	**2.3497**

Литература

1. Wang A.J.A. Information security models and metrics // Proceedings of the 43rd annual Southeast regional conference. 2005. V. 2. P. 178–184.
2. Purboyo T.W., Rahardjo B., Kuspriyanto. Security metrics: a brief survey // 2011 2nd International Conference on Instrumentation, Communications, Information Technology, and Biomedical Engineering. IEEE. 2011. P. 79–82.
3. Almasizadeh J., Azgomi M.A. A stochastic model of attack process for the evaluation of security metrics // Computer Networks. 2013. V. 57, No. 10. P. 2159–2180.
4. Росенко А.П., Бордак И.В. Математическая модель определения вероятности последствий от реализации злоумышленником угроз безопасности информации ограниченного распространения // Известия Южного федерального университета. Технические науки. 2015. № 7(168). С. 6–19.
5. Drazin M.P., Haynsworth E.V. Criteria for the reality of matrix eigenvalues // Mathematische Zeitschrift. 1962. V. 78, No. 1. P. 449–452.
6. Хорн Р., Джонсон Ч. Матричный анализ. М. : Мир, 1989.
7. Le N.T. et al. A threat computation model using a Markov Chain and common vulnerability scoring system and its application to cloud security // Australian Journal of Telecommunications and the Digital Economy. 2019. V. 7, No. 1. P. 37.
8. Jouini M., Rabai L.B.A. Mean Failure Cost Extension Model towards Security Threats Assessment: A Cloud Computing Case Study // Journal of Computers. 2015. V. 10, No. 3. P. 184–194.

EVALUATING MEAN TIME TO SECURITY FAILURE BASED ON CONTINUOUS-TIME MARKOV CHAINS

A. A. Magazev
Dr.Sc.(Phys.-Math.), Professor, Department of Complex Information Security,
e-mail: magazev@omgtu.ru
A. S. Melnikova
Undergraduate, Department of Complex Information Security,
e-mail: anastasiya_m.96@mail.ru
V. F. Tsyrulnik
Postgraduate, Department of Complex Information Security,
e-mail: lera.tsyrulnik@mail.ru

Omsk State Technical University, Omsk, Russia

Abstract. In the article, we consider a Markov model of computer attacks, in the framework of which attacks and the system responses are modelled by homogeneous Poisson point processes. We describe a method of solving the corresponding Kolmogorov system of equations by calculating eigenvalues and eigenvectors of some matrix. An important random variable associated with the corresponding Markov chain and called the time to security failure is explored in detail. The comparison of the results obtained and the results of simulation modelling are presented.

Keywords: continuous-time Markov chain, Kolmogorov's equations, mean time to security failure.

References

1. Wang A.J.A. Information security models and metrics. Proceedings of the 43rd annual Southeast regional conference, 2005, vol. 2, pp. 178–184.
2. Purboyo T.W. and Rahardjo B., Kuspriyanto. Security metrics: a brief survey. 2011 2nd International Conference on Instrumentation, Communications, Information Technology, and Biomedical Engineering, IEEE, 2011, pp. 79–82.
3. Almasizadeh J. and Azgomi M.A. A stochastic model of attack process for the evaluation of security metrics. Computer Networks, 2013, vol. 57, no. 10, pp. 2159–2180.
4. Rosenko A.P. and Bordak I.V. Matematicheskaya model' opredeleniya veroyatnosti posledstvii ot realizatsii zloumyshlennikom ugroz bezopasnosti informatsii ogranichennogo rasprostraneniya. Izvestiya Yuzhnogo federal'nogo universiteta, Tekhnicheskie nauki, 2015, no. 7(168), pp. 6–19. (in Russian)
5. Drazin M.P. and Haynsworth E.V. Criteria for the reality of matrix eigenvalues. Mathematische Zeitschrift, 1962, vol. 78, no. 1, pp. 449–452.
6. Khorn R., Dzhonson Ch. Matrichnyi analiz. Moscow, Mir Publ., 1989. (in Russian)
7. Le N.T. et al. A threat computation model using a Markov Chain and common vulnerability scoring system and its application to cloud security. Australian Journal of Telecommunications and the Digital Economy, 2019, vol. 7, no. 1, pp. 37.
8. Jouini M. and Rabai L.B.A. Mean Failure Cost Extension Model towards Security Threats Assessment: A Cloud Computing Case Study. Journal of Computers, 2015, vol. 10, no. 3, pp. 184–194.

Дата поступления в редакцию: 26.11.2020