КРАВЧЕНКО Ксения Владимировна, старший преподаватель кафедры «Математические методы и информационные технологии в экономике».
SPIN-код: 1851-6858
AuthorID (РИНЦ): 243244
Адрес для переписки: trr474747@mail.ru
ШЕВЕЛЕВА Ольга Геннадьевна, старший преподаватель кафедры «Математические методы и информационные технологии в экономике».
SPIN-код: 8060-6060
Адрес для переписки: osh_a@mail.ru

Для цитирования

Бояркин Г. Н., Кравченко К. В., Шевелева О. Г. Системный подход в планировании и управлении бизнес-процессами подготовки кадров высшей квалификации // Омский научный вестник. 2018. № 6 (162). С. 211—216. DOI: 10.25206/1813-8225-2018-162-211-216.

Статья поступила в редакцию 27.10.2018 г.

УДК 004.942
DOI: 10.25206/1813-8225-2018-162-216-219

А. А. МАГАЗЕВ
А. С. МЕЛЬНИКОВА

Омский государственный технический университет, г. Омск

ПОСТРОЕНИЕ ОБЛАСТИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ МЕТОДОМ ДИНАМИКИ СРЕДНИХ

В работе рассматривается модель информационной системы, каждый элемент которой подвергается пуассоновским потокам угроз безопасности. С помощью теории марковских процессов описывается усредненная динамика системы. Конструируется область значений внутренних параметров модели, при которых число вышедших из строя элементов не превысит заданный порог за определенное время.

Ключевые слова: марковский процесс, пуассоновский поток, метод динамики средних, область безопасности.

Введение. С активным развитием IT-индустрии связано появление новых типов информационных угроз и уязвимостей компьютерных систем, поэтому информационная безопасность является бурно развивающейся областью информационных технологий. Одна из проблем, с которой часто сталкиваются при построении надежных систем защиты информации, — это повышенные материальные и временные затраты, связанные с проведением натурных испытаний. Приемлемой альтернативой является математическое моделирование, так как затраты на исследование здесь сравнительно невелики, существует возможность изучения долговременного поведения модели, а также отсутствует риск навредить реальной системе.

Так как информационные угрозы носят преимущественно вероятностный характер, при моделировании целесообразно применение теории случайных процессов. Особо плодотворным в решении задач информационной безопасности является применение *марковских процессов.* Действительно, моделирование процессов распространения компьютерных вирусов [1], оптимизация и повышение надежности защищенных информационных систем [2, 3], обнаружение вторжений в компьютерных системах и вычислительных сетях [4, 5], обнаружение кибер-атак в компьютерных сетях [6] — вот далеко не полный перечень задач, которые решаются с помощью подобных моделей. В последнее время в компьютерной вирусологии и криптографии также нашли применение так называемые *скрытые марковские модели* [7—9].

В настоящей работе представлен способ моделирования информационной системы (ИС), состоящей из большого числа однородных элементов, методом динамики средних. В рамках моделируемой ИС состояние каждого элемента описывается марковской моделью, предложенной в работах А. П. Росенко [10, 11].

В статье [12] данная модель была исследована более углубленно. В частности, на ее основе была сформулирована оптимизационная задача о выборе комплекса средств защиты информации [13]. В настоящей работе мы используем данную модель для описания усредненной динамики ИС, состоящей из большого числа однородных элементов и подвергающейся пуассоновским потокам угроз. С помощью системы дифференциальных уравнений, являющихся результатом усреднения уравнений Колмогорова, мы конструируем и исследуем так называемую *область безопасности системы*, определяемую как область значений внутренних параметров модели, при которых система функционирует заданное время.

Описание модели. Рассмотрим ИС, состоящую из большого числа N *однородных* элементов (ресурсов). Будем считать, что на каждый элемент ИС воздействует n *простейших пуассоновских потоков угроз* с интенсивностями $\lambda_1, ..., \lambda_n$. В соответствии с этим каждый элемент системы может находиться в одном из следующих состояний: $S_0, ..., S_n, S_f$. Здесь S_0 — состояние, в котором угрозы отсутствуют, S_i — состояние, в которое переходит элемент в случае воздействия на него i-ой угрозы, $i = 1, ..., n$. Состояние S_f, называемое *финальным*, отражает факт неудачной попытки восстановления элемента от последствий какой-либо из угроз.

Обозначим через μ_i интенсивность потока восстановления от последствий реализации i-ой угрозы, а через R_i — вероятность этого восстановления. Если в данный момент времени элемент находится в состоянии S_i, где $i \neq 0$, то имеется два пути развития ситуации:

1. Угроза будет устранена с вероятностью $\mu_i R_i$, и ресурс вернется в исходное состояние S_0;

2. Угроза приведет к выходу ресурса из строя с вероятностью $\mu_i(1-R_i)$, и система перейдет в *финальное состояние* S_f.

Из приведенного описания следует, что последовательность переходов между состояниями элемента представляет собой марковский процесс с конечным числом состояний и непрерывным временем (рис. 1).

Вероятности состояний элемента $p_0(t)$, $p_1(t)$, ..., $p_n(t)$, $p_f(t)$ как функции времени могут быть найдены с помощью системы дифференциальных уравнений Колмогорова, которая в нашем случае имеет следующий вид:

$$p_0'(t) = -p_0(t)\sum_{i=1}^{n}\lambda_i + \sum_{i=1}^{n}\mu_i R_i p_i(t),$$

$$p_k'(t) = \lambda_k p_0(t) - p_k(t)\mu_k, \quad k = 1,..., n, \qquad (1)$$

$$p_f'(t) = \sum_{i=1}^{n}\mu_i(1-R_i)p_i(t).$$

Считая, что в начальный момент времени угрозы отсутствовали, дополним систему (1) следующими начальными условиями:

$$p_0(0) = 1,\ p_1(0) = ... = p_n(0) = p_f(0) = 0.$$

Известно, что общий аналитический метод решения систем вида (1) основан на преобразовании Лапласа и сводит исходную задачу к алгебраической. Поэтому само по себе интегрирование системы (1) не представляет особых трудностей. Тем не менее, если учесть, что в типовых ИС количество элементов N может достигать нескольких тысяч, приходится решать систему $N(n+2)$ дифференциальных уравнений, что уже может вызвать определенные затруднения даже при использовании численных методов.

Часто, однако, столь детальная информация о системе не требуется; во многих ситуациях достаточно лишь знание ее динамики в *среднем*. В таких случаях целесообразно использование *метода динамики средних*, определяющего математическое ожидание $m_i(t)$ числа элементов ИС, находящихся в одинаковых состояниях S_i в данный момент времени t. Данный метод дает приближенные результаты, но имеет существенное преимущество: чем

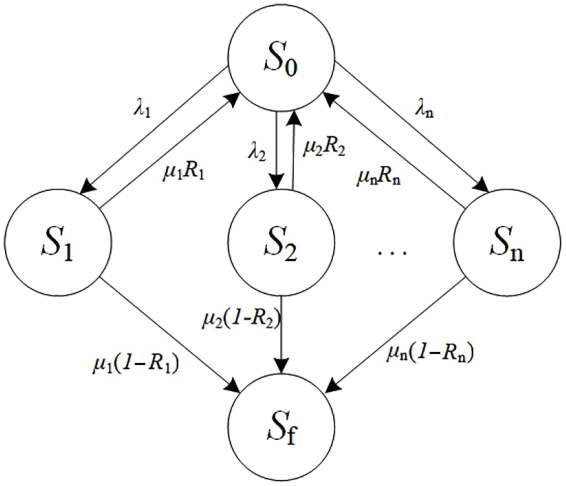

Рис. 1. Граф состояний элемента системы

больше элементов и состояний имеется в системе, тем точнее результат математического моделирования.

Следуя методу динамики средних, усредним каждое уравнение системы (1) по всем элементам ИС. В результате мы получаем систему дифференциальных уравнений, определяющих динамику математических ожиданий числа элементов ИС в каждом из состояний:

$$m_0'(t) = -m_0(t)\sum_{i=1}^{n}\lambda_i + \sum_{i=1}^{n}\mu_i R_i m_i(t),$$

$$m_k'(t) = \lambda_k m_0(t) - m_k(t)\mu_k, \quad k = 1,..., n, \qquad (2)$$

$$m_f'(t) = \sum_{i=1}^{n}\mu_i(1-R_i)m_i(t).$$

Нетрудно видеть, что начальные условия для данной системы уравнений имеют вид

$$m_0(0) = N,\ m_1(0) = ... = m_n(0) = m_f(0) = 0. \qquad (3)$$

Конструкция области безопасности. По своему смыслу интенсивности потоков угроз λ_i представляют собой внешние параметры модели, влиять на которые на практике мы не можем. В свою очередь, параметры защиты R_i и μ_i — это *внутренние* параметры модели, которые мы можем регулировать. В связи с этим возникает естественный вопрос: какими должны быть эти параметры, чтобы ИС приемлемо функционировала заданное время?

Сформулируем задачу более строго. Пусть T_{cr} — некоторый фиксированный промежуток времени, N_{cr} — заданный порог числа ресурсов, при превышении которого мы будем считать, что ИС функционирует в опасном (аварийном) режиме. Задача состоит в поиске тех значений параметров μ_i и R_i, при которых среднее число ресурсов в безопасном состоянии в момент времени T_{cr} не превышает порогового значения N_{cr} при заданных значениях внешних параметров λ_i. Множество значений параметров μ_i и R_i, удовлетворяющих указанным условиям, будем называть *областью безопасности* модели.

Нетрудно видеть, что задача построения области безопасности сводится к решению неравенства

$$m_0(T_{cr}) \geq N_{cr}, \qquad (4)$$

рассматриваемого относительно неизвестных μ_i и R_i (эти неизвестные входят в выражение для $m_0(T_{cr})$ как параметры). Формально задача может быть решена, если нам известно решение системы (2) с начальным условием (3). На практике, однако, чаще всего неравенство (4) не может быть решено аналитически в силу трансцендентного характера $m_0(T_{cr})$ как функции μ_i и R_i.

Для численного решения задачи (4) нами была разработана программа в рамках системы компьютерной алгебры Maple 2016, работающая по следующему алгоритму. В $2n$-мерном евклидовом пространстве выбираем прямоугольную область и разбиваем ее на *элементарные ячейки* — $2n$-мерные малые прямоугольники. Каждая вершина элементарной ячейки представляет собой точку с координатами (μ_1, ..., μ_n, R_1, ..., R_n). Далее, в зависимости от выполнения или невыполнения неравенства (4), все вершины из рассматриваемой области делим на два класса — принадлежащие или не принадлежащие области безопасности модели. В результате мы получаем дискретное разбиение исходной области на две подобласти — безопасную и опасную.

Проиллюстрируем решение задачи на частном случае одной угрозы: $n=1$. На рис. 2 приведен результат численного разбиения прямоугольной области $[0,1]\times[0,1]$ на безопасную (белый цвет) и опасную (серый цвет) подобласти. При этом мы брали следующие входные данные задачи: $N=1000$; $\lambda=1{,}1$; $N_{cr}=150$; $T_{cr}=30$.

Из рис. 2 видно, что граница, разделяющая безопасную и опасную зоны, — это некоторая гладкая кривая $R=R(\mu)$. В результате численного анализа модели было показано, что данная кривая может быть эффективно аппроксимирована функцией вида:

$$R(\mu) \approx R_\infty + e^{-\alpha(\mu-\mu_{cr})}(1-R_\infty), \qquad (5)$$

где R_∞ — критический порог вероятности восстановления ресурса, μ_{cr} — критическое значение интенсивности потока восстановления, α — крутизна кривой. Ясно, что R_∞, μ_{cr}, α представляют собой функции входных параметров задачи λ, T, N_{cr} и в каждой конкретной ситуации могут быть найдены численно, например, методом наименьших квадратов.

Таким образом, для того, чтобы ИС функционировала в безопасном режиме, необходимо, чтобы параметры μ_i и R_i выбирались из области безопасности, определяемой неравенством (4). В случае одной угрозы — это плоская область, лежащая выше кривой $R=R(\mu)$. Отметим, что аппроксимационная зависимость (5) позволяет сформулировать следующий грубый критерий «попадания» в безопасную область: значения μ и R должны удовлетворять неравенствам:

$$R > R_\infty,\ \mu > \mu_{cr}.$$

Заключение. В статье рассмотрена марковская модель функционирования однородной ИС, на каждый элемент которой действуют пуассоновские потоки угроз. Предложен подход описания динамики ИС методом усреднения исходных уравнений Колмогорова по всем элементам. Предложен и реализован алгоритм построения области безопасности модели, то есть области значений ее внутренних параметров, при которых среднее число нормально функционирующих ресурсов (элементов) ИС

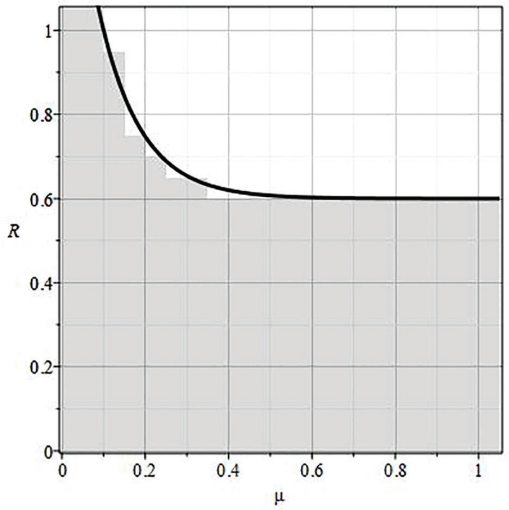

Рис. 2. Область безопасности системы в случае одной угрозы

не ниже определенного критического значения. Подробно рассмотрен случай одной угрозы.

В заключение также отметим, что с помощью представленного в статье подхода можно моделировать информационные системы банкоматов современных банков. Банкоматы выполняют идентичные функции и подвергаются однородным угрозам (целостности, конфиденциальности и доступности). Если банкомат был подвержен той или иной угрозе, его отправляют в сервисный центр для восстановления.

Ремонту банкомат подлежит с определенной долей вероятности R, интенсивность восстановления μ также зависит от некоторых параметров, например, от степени загруженности ремонтной бригады. Метод моделирования, описанный в данной работе, позволяет оценить необходимые интенсивности и вероятности восстановлений банкоматов.

Библиографический список

1. Бойко А. А. Способ аналитического моделирования процесса распространения вирусов в компьютерных сетях различной структуры // Труды СПИИРАН. 2015. Т. 5, № 42. С. 196–211.

2. Богатырев В. А., Богатырев А. В., Богатырев С. В. Оптимизация интервалов проверки информационной безопасности систем // Научно-технический вестник информационных технологий, механики и оптики. 2014. № 5. С. 119–125.

3. Щеглов К. А., Щеглов А. Ю. Математические модели эксплуатационной информационной безопасности // Вопросы защиты информации. 2014. № 3. С. 52–65.

4. Sha W., Zhu Y., Chen M., Huang T. Statistical learning for anomaly detection in cloud server systems: a multi-order Markov chain framework // IEEE Transactions on Cloud Computing. 2015. Vol. 6. P. 401–413. DOI: 10.1109/TCC.2015.2415813.

5. Mirsky Y., Cohen A., Stern R. [et al.]. Search problems in the domain of multiplication: Case study on anomaly detection using markov chains // Eighth Annual Symposium on Combinatorial Search. 2015. P. 70–77.

6. Bourget E., Cuppens F., Cuppens-Boulahia N. [et al.]. Probabilistic Event Graph to Model Safety and Security for Diagnosis Purposes // IFIP Annual Conference on Data and Applications Security and Privacy. 2018. P. 38–47.

7. Austin T. H., Filiol E., Josse S. [et al.]. Exploring hidden Markov models for virus analysis: a semantic approach // 2013 46th Hawaii International Conference on System Sciences

(HICSS), Wailea, Maui, HI USA. 2013. P. 5039—5048. DOI: 10.1109/HICSS.2013.217.

8. Vobbilisetty R., Di Troia F., Low R. M. [et al.]. Classic cryptanalysis using hidden Markov models // Cryptologia. 2017. Vol. 41, no. 1. P. 1—28. DOI: 10.1080/01611194.2015.1126660.

9. Stamp M., Di Troia, F., Stamp M. Hidden Markov Models for Vigenure Cryptanalysis // Proceedings of the 1st International Conference on Historical Cryptology HistoCrypt. 2018. No. 149. P. 39—46.

10. 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.

11. Росенко А. П., Бордак И. В. Математическая модель определения вероятности последствий от реализации злоумышленником угроз безопасности информации ограниченного распространения // Известия ЮФУ. Технические науки. 2015. № 7. С. 6—19.

12. Магазев А. А., Цырульник В. Ф. Исследование одной марковской модели угроз безопасности компьютерных систем // Моделирование и анализ информационных систем. 2017. № 4. С. 445—458. DOI: 10.18255/1818-1015-2017-4-445-458.

13. Магазев А. А., Цырульник В. Ф., Оптимизация выбора средств защиты информации в рамках одной марковской модели безопасности // Информационные технологии и нанотехнологии: IV Междунар. конф. и молодеж. школа ИТНТ, 24—27 апреля 2018 г. Самара, 2018. С. 2050—2058.

МАГАЗЕВ Алексей Анатольевич, доктор физико-математических наук, доцент кафедры «Комплексная защита информации».
SPIN-код: 2833-0366
ORCID: orci-dorg-0000-0002
Author ID (SCOPUS): 6507004666
ResearcherID: H-9479-2013
Адрес для переписки: magazev@omgtu.ru
МЕЛЬНИКОВА Анастасия Сергеевна, магистрант гр. ИВТм-183 факультета элитного образования и магистратуры.
Адрес для переписки: anastasiya170696@gmail.com

Для цитирования

Магазев А. А., Мельникова А. С. Построение области безопасности информационной системы методом динамики средних // Омский научный вестник. 2018. № 6 (162). С. 216—219. DOI: 10.25206/1813-8225-2018-162-216-219.

Статья поступила в редакцию 22.10.2018 г.