MODELING AND ANALYSIS OF INFORMATION SYSTEMS, VOL. 27, NO. 1, 2020
journal homepage: www.mais-journal.ru

DISCRETE MATHEMATICS IN RELATION TO COMPUTER SCIENCE

A Markov Model of Non-Mutually Exclusive Cyber Threats and its Applications for Selecting an Optimal Set of Information Security Remedies

A. A. Kassenov[1], A. A. Magazev[1], V. F. Tsyrulnik[1]

DOI: 10.18255/1818-1015-2020-1-108-123

[1]Omsk State Technical University, 11 Mira pr., Omsk, 644050 Russia.

MSC2020: 68M25
Research article
Full text in Russian

Received October 27, 2019
After revision February 20, 2020
Accepted February 28, 2020

In this work, we study a Markov model of cyber threats that act on a computer system. Within the framework of the model the computer system is considered as a system with failures and recoveries by analogy with models of reliability theory. To estimate functionally-temporal properties of the system we introduce a parameter called the lifetime of the system and defined as the number of transitions of the corresponding Markov chain until the first hit to the final state. Since this random variable plays an important role at evaluating a security level of the computer system, we investigate in detail its random distribution for the case of mutually exclusive cyber threats; in particular, we derive explicit analytical formulae for numerical characteristics of its distribution: expected value and dispersion. Then we generalize substantially the Markov model dropping the assumption that cyber threats acting on the system are mutually exclusive. This modification leads to an extended Markov chain that has (at least qualitatively) the same structure as the original chain. This fact allowed to generalize the above analytical results for the expected value and dispersion of the lifetime to the case of non-mutually exclusive cyber threats. At the end of the work the Markov model for non-mutually exclusive cyber threats is used to state a problem of finding an optimal configuration of security remedies in a given cyber threat space. It is essential that the formulated optimization problems belong to the class of non-linear discrete (Boolean) programming problems. Finally, we consider an example that illustrate the solution of the problem on selecting the optimal set of security remedies for a computer system.

Keywords: cyber threat; Markov chain; security remedy; optimization

INFORMATION ABOUT THE AUTHORS

Adil A. Kassenov	orcid.org/0000-0002-2770-1144. E-mail: kassenov_adil@mail.ru graduate student.
Alexey A. Magazev correspondence author	orcid.org/0000-0002-8725-9183. E-mail: magazev@omgtu.ru doctor of sc., professor.
Valeriya F. Tsyrulnik	orcid.org/0000-0002-6875-7216. E-mail: lera.tsyrulnik@mail.ru postgraduate student.

Funding: The reported study was funded by RFBR, project number 19-37-90122.

For citation: A. A. Kassenov, A. A. Magazev, and V. F. Tsyrulnik, “A Markov Model of Non-Mutually Exclusive Cyber Threats and its Applications for Selecting an Optimal Set of Information Security Remedies”, *Modeling and analysis of information systems*, vol. 27, no. 1, pp. 108-123, 2020.

МОДЕЛИРОВАНИЕ И АНАЛИЗ ИНФОРМАЦИОННЫХ СИСТЕМ, ТОМ 27, № 1, 2020
сайт журнала: www.mais-journal.ru

DISCRETE MATHEMATICS IN RELATION TO COMPUTER SCIENCE

Марковская модель совместных киберугроз и ее применение для выбора оптимального набора средств защиты информации

А. А. Касенов[1], А. А. Магазев[1], В. Ф. Цырульник[1]

DOI: 10.18255/1818-1015-2020-1-108-123

[1]Омский государственный технический университет, пр. Мира, 11, Омск, 644050 Россия.

УДК 51-74, 004.942
Научная статья
Полный текст на русском языке

Получена 27 октября 2019 г.
После доработки 20 февраля 2020 г.
Принята к публикации 28 февраля 2020 г.

В данной работе исследуется марковская модель киберугроз, действующих на компьютерную систему. В рамках данной модели компьютерная система рассматривается как система с отказами и восстановлениями по аналогии с моделями теории надежности. Для оценки функционально-временных свойств системы мы вводим ее параметр, называемый временем жизни и определяемый как число переходов в соответствующей марковской цепи до первого попадания в финальное состояние. В силу того, что данная случайная величина играет важную роль при оценке уровня защищенности компьютерной системы, мы подробно исследуем ее распределение вероятностей в случае несовместных киберугроз; в частности, мы получаем явные аналитические формулы для ее числовых характеристик: математического ожидания и дисперсии. Затем мы существенно обобщаем рассматриваемую марковскую модель, исключив допущение о несовместности действующих на систему киберугроз. Соответствующая марковская цепь при такой модификации расширяется за счет дополнительных состояний, не меняя своей качественной структуры. Указанный факт позволил обобщить полученные ранее аналитические результаты для математического ожидания и дисперсии времени жизни на случай совместных киберугроз. В заключении работы марковская модель совместных кибеугроз используется для постановки задачи о поиске оптимальной конфигурации средств защиты информации в заданном пространстве киберугроз. Существенно, что сформулированные оптимизационные задачи принадлежат к классу задач нелинейного дискретного (булева) программирования. В заключении работы рассматривается пример, иллюстрирующий решение задачи о выборе оптимального набора средств защиты для компьютерной системы.

Ключевые слова: киберугроза; марковская цепь; средство защиты информации; оптимизация.

ИНФОРМАЦИЯ ОБ АВТОРАХ

Адиль Аскарович Касенов	orcid.org/0000-0002-2770-1144. E-mail: kassenov_adil@mail.ru магистрант.
Алексей Анатольевич Магазев автор для корреспонденции	orcid.org/0000-0002-8725-9183. E-mail: magazev@omgtu.ru доктор физ.-мат. наук, профессор.
Валерия Федоровна Цырульник	orcid.org/0000-0002-6875-7216. E-mail: lera.tsyrulnik@mail.ru аспирантка.

Финансирование: Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 19-37-90122.

Для цитирования: A. A. Kassenov, A. A. Magazev, and V. F. Tsyrulnik, “A Markov Model of Non-Mutually Exclusive Cyber Threats and its Applications for Selecting an Optimal Set of Information Security Remedies”, *Modeling and analysis of information systems*, vol. 27, no. 1, pp. 108-123, 2020.

Введение

В связи с высокой стоимостью проведения натурных экспериментов, математическое моделирование является едва ли не единственной альтернативой в исследовании проблем информационной безопасности современных компьютерных систем. Как следствие, разработка и анализ моделей компьютерной безопасности — это бурно развивающаяся область знаний, в которой число научных публикаций продолжает расти из года в год.

Из всего многообразия существующих моделей безопасности следует выделить группу *теоретико-вероятностных моделей*, основанных на различных концепциях теории вероятности и теории случайных процессов. Среди них особую роль играют модели, основанные на теории марковских случайных процессов, так как хорошо разработанный соответствующий математический аппарат во многих ситуациях позволяет получить исчерпывающее численное или даже аналитическое решение сформулированных с их помощью задач. Для иллюстрации этого тезиса достаточно отметить чрезвычайно широкой спектр приложений марковских моделей к проблемам кибербезопасности: обнаружение вторжений и аномалий в компьютерных системах [1—4], моделирование процессов распространения компьютерных вирусов [5—8], управление рисками информационной безопасности [9, 10], моделирование процессов возникновения киберугроз и эксплуатации уязвимостей в информационных и кибер-физических системах [11—13].

В работе [14] был предложен класс моделей киберугроз, формулируемых в терминах марковских цепей с дискретным временем. В рамках данных моделей компьютерная система, подвергающаяся воздействию киберугроз, описывается как система с отказами и восстановлениями (по аналогии с моделями технических систем в теории надежности). Высказав возможность использования подобных моделей для получения оценок защищенности информации, автор цитируемой работы провел лишь их поверхностный анализ и ограничился, в основном, рассмотрением простейших примеров. Частично данный недостаток был устранен в статьях [15, 16], в которых было проведено более углубленное и детальное исследование указанного класса моделей. Помимо явных аналитических формул для вероятностей состояний системы, в этих работах также был предложен оригинальный метод оценки защищенности компьютерной системы, основанный на вычислении так называемого *времени релаксации* соответствующей марковской цепи. Кроме того, с помощью исследуемой марковской модели киберугроз в работе [16] была сформулирована задача о поиске *оптимального* набора средств защиты информации, то есть набора, имеющего минимальную стоимость, но обеспечивающего необходимый уровень защиты от заданных киберугроз.

Отметим, что рассмотренные в работах [14—16] модели киберугроз сформулированы с использованием ряда упрощающих допущений, которые далеко не всегда имеют место на практике. Одним из таких допущений является предположение о том, что одновременное появление двух и более киберугроз невозможно, то есть угрозы являются *несовместными* случайными событиями. Кроме того, время релаксации марковской цепи, введенное в [15] для оценки времени достижения поглощающего состояния, представляет из себя довольно искусственную характеристику, вычисление которой осуществляется не аналитически, а численно. Цель настоящей статьи состоит в устранении этих двух недостатков. В частности, вместо времени релаксации марковской цепи мы предлагаем использовать ее более естественный параметр — *время жизни* системы, то есть число переходов в марковской цепи до достижения ее финального состояния. В настоящей работе мы подробно исследуем распределение этой случайной величины и получаем явные формулы для вычисления ее основных характеристик — математического ожидания и дисперсии. Также мы существенно обобщаем класс рассмотренных в [14, 15] марковских моделей, допустив, что все киберугрозы являются совместными случайными событиями. При этом все аналитические результаты, полученные при предположении о несовместности угроз, легко обобщаются на совместный случай с помощью расширения множества состояний марковской цепи.

В заключении настоящей статьи мы обсуждаем применение марковской модели совместных киберугроз к формулировке задачи поиска оптимальной конфигурации средств защиты информации. Данная задача имеет важное прикладное значение в управлении информационной безопасностью, в частности, в вопросах оптимизации инвестиций в кибербезопасность (см. обзорную статью [17] и приведенные в ней ссылки). В частности, мы формулируем две задачи условной оптимизации, в которых целевой функцией является либо стоимость набора средств защиты, либо среднее время жизни системы. Существенно, что обе эти задачи относятся к классу оптимизационных задач нелинейного дискретного программирования, в связи с чем актуальной становится задача поиска подходов к их эффективному решению. Разработка соответствующих методов, однако, будет представлять для нас дальнейший исследовательский интерес; здесь мы лишь ограничились рассмотрением одного простого примера, иллюстрирующего применение предложенного нами подхода к задаче выбора оптимальной конфигурации средств защиты в компьютерных системах.

1. Описание исходной модели

В настоящем разделе мы напомним основные положения модели киберугроз, предложенной в [14], а также приведем соответствующие аналитические результаты, полученные в наших предыдущих работах [15, 16].

Рассмотрим компьютерную систему (далее просто *систему*), которая подвергается воздействию n угроз с вероятностями $q_1, q_2, \dots, q_n$ соответственно. Примем следующие допущения:

- угрозы действуют на систему только в дискретные моменты времени $t = 1, 2, 3, \dots$;
- в каждый момент времени на систему может действовать только одна угроза;
- если в момент времени t на систему подействовала одна из угроз, в следующий момент $t + 1$ происходит попытка ее отражения (воздействие еще каких-либо угроз в этот момент считается невозможным).

Согласно сделанным предположениям мы можем считать, что в каждый момент времени система находится в одном из состояний $s_0, s_1, \dots, s_{n+1}$. Состояние s_0, которое мы далее будем называть *безопасным*, характеризуется отсутствием действия любой из угроз. В случае действия i-ой угрозы система переходит в состояние s_i, где $i = 1, 2, \dots, n$. Наконец, состояние s_{n+1} отвечает факту неудачного отражения любой из угроз. Данное состояние мы будем называть *финальным*.

Обозначим через r_i вероятность успешного отражения i-ой угрозы, а через $\bar{r}_i = 1 - r_i$ — вероятность соответствующей безуспешной попытки. Нетрудно видеть, что состояние системы в каждый момент времени определяется только ее состоянием в предыдущий момент времени. Это означает, что последовательность состояний системы представляет собой простую марковскую цепь, граф переходов которой изображен на рис. 1.

Задача описания динамики рассматриваемой системы сводится к вычислению величин $p_i(t)$ — вероятностей состояний s_i системы в произвольный момент времени t. Как хорошо известно из общей теории марковских цепей, эти вероятности могут быть вычислены согласно формуле

$$p_i(t) = \sum_{j=0}^{n+1} \pi_{ji}\, p_j(t-1), \qquad i = 0, 1, \dots, n+1, \tag{1}$$

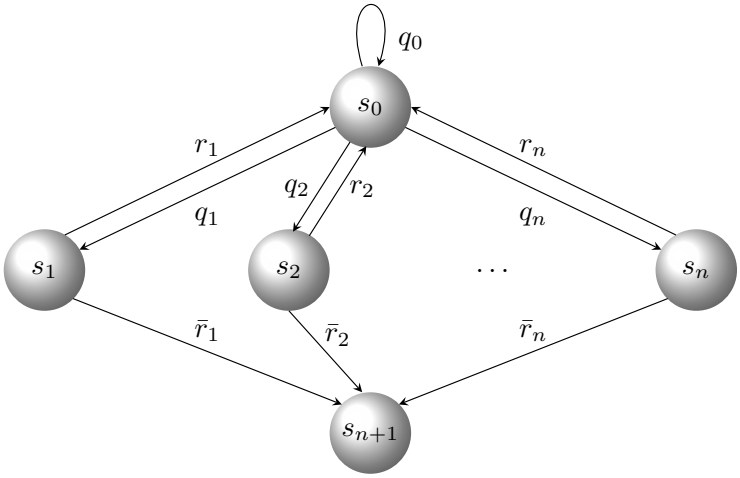

Fig. 1. System transitions graph

Рис. 1. Граф переходов системы

где π_{ji} — вероятность перехода системы из состояния s_j в состояние s_i. Совокупность величин π_{ji} образует *матрицу переходных вероятностей* Π, которая в нашем случае имеет вид:

$$\Pi = \begin{pmatrix} q_0 & q_1 & q_2 & \dots & q_n & 0 \\ r_1 & 0 & 0 & \dots & 0 & \bar{r}_1 \\ r_2 & 0 & 0 & \dots & 0 & \bar{r}_2 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ r_n & 0 & 0 & \dots & 0 & \bar{r}_n \\ 0 & 0 & 0 & \dots & 0 & 1 \end{pmatrix}. \tag{2}$$

Здесь введено обозначение $q_0 = 1 - \sum_{i=1}^{n} q_i$. Естественно также предположить, что в начальный момент времени $t = 0$ система находится в безопасном состоянии:

$$p_0(0) = 1, \quad p_1(0) = p_2(0) = \dots = p_{n+1}(0) = 0. \tag{3}$$

Формула (1) и начальные условия (3) позволяют однозначно определить вероятности $p_i(t)$ состояний системы в произвольный момент времени.

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. Такие выражения были получены в нашей предыдущей работе [15]. Мы приведем здесь только вид функции $p_0(t)$, так как для дальнейших рассуждений ее будет достаточно:

$$p_0(t) = \frac{1}{w}\left(\frac{q_0 + w}{2}\right)^{t+1} - \frac{1}{w}\left(\frac{q_0 - w}{2}\right)^{t+1}. \tag{4}$$

Здесь неотрицательный параметр w определяется как

$$w^2 = q_0^2 + 4\sum_{i=1}^{n} q_i r_i. \tag{5}$$

Рассмотрим три частных случая.

1. Случай отсутствия угроз: $q_i = 0$ для всех i. Согласно (5) в этом случае $q_0 = w = 1$, поэтому в соответствии с (4) имеем

$$p_0(t) = 1.$$

Полученный результат иллюстрирует следующий тривиальный факт: при отсутствии угроз система всегда будет находиться в безопасном состоянии.

2. Случай отсутствия защиты: $r_i = 0$ для всех i. Из (5) следует, что $w = q_0$, так что формула (4) дает

$$p_0(t) = q_0^t.$$

Таким образом, вероятность безопасного состояния монотонно убывает с течением времени (здесь предполагается, что $0 < q_0 < 1$).

3. Случай частых угроз $q_0 \approx 0$. В этом случае мы приближенно можем считать $w^2 \approx 4\sum_{i=1}^{n} q_i r_i$, откуда

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

Видно, что в рамках данного приближения система в нечетные моменты времени практически никогда не обнаруживается в безопасном состоянии, так как в эти моменты времени на систему с большой вероятностью воздействует какая-либо из угроз.

2. Время жизни системы: случай несовместных киберугроз

Временем жизни T системы назовем время, за которое она перейдет в финальное состояние s_{n+1}. Другими словами, время жизни — это число переходов между состояниями системы до тех пор, пока она в первый раз не окажется в состоянии s_{n+1}. Ясно, что T — это дискретная случайная величина, принимающая целые значения $T = 2, 3, 4, \ldots$. Задачей настоящего раздела является нахождение явного вида этого распределения и вычисление его основных числовых характеристик.

Закон распределения для времени жизни можно найти, используя формулу (4) 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. 2, видно, что система может оказаться в состоянии 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 $P(T)$ при $T \geq 2$ имеем:

$$P(T) = p_0(T-2) \sum_{i=1}^{n} q_i \bar{r}_i.$$

Здесь выражение $\sum_{i=1}^{n} q_i \bar{r}_i$ определяет вероятность перехода из состояния s_0 в состояние s_{n+1}. С учетом (4) получаем, что распределение вероятностей случайной величины T имеет вид:

$$P(T) = \begin{cases} w^{-1} \sum\limits_{i=1}^{n} q_i \bar{r}_i \left[\left(\frac{q_0+w}{2} \right)^{T-1} - \left(\frac{q_0-w}{2} \right)^{T-1} \right], & T \geq 2, \\ 0, & T < 2. \end{cases} \tag{6}$$

Напомним, что $\bar{r}_i = 1 - r_i$, $q_0 = 1 - \sum_{i=1}^{n} q_i$, а параметр w определяется формулой (5). В качестве иллюстрации на рис. 2 приведен вид этого распределения для случая трех киберугроз.

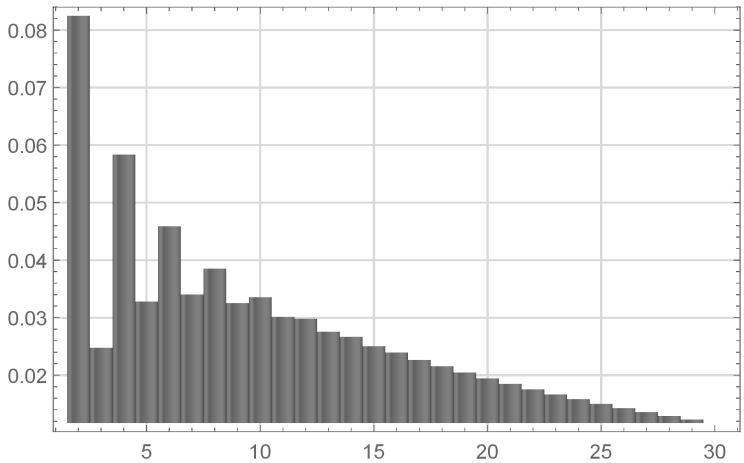

Fig. 2. Probability distribution of T for $q_1 = 0{,}35$, $q_2 = 0{,}25$, $q_3 = 0{,}1$ and $r_1 = 0{,}85$, $r_2 = 0{,}9$, $r_3 = 0{,}95$

Рис. 2. Распределение вероятностей величины T при $q_1 = 0{,}35$, $q_2 = 0{,}25$, $q_3 = 0{,}1$ и $r_1 = 0{,}85$, $r_2 = 0{,}9$, $r_3 = 0{,}95$

Напомним, что *моментом* k-го порядка случайной величины T называется математическое ожидание величины T^k:

$$\mu_k[T] = \sum_{T=0}^{\infty} T^k P(T), \quad k = 1, 2, \ldots.$$

Подставляя сюда формулу (6), получаем

$$\mu_k[T] = w^{-1} \sum_{i=1}^{n} q_i \bar{r}_i \left[\sum_{T=2}^{\infty} T^k \left(\frac{q_0 + w}{2} \right)^{T-1} - \sum_{T=2}^{\infty} T^k \left(\frac{q_0 - w}{2} \right)^{T-1} \right] =$$

$$= \frac{\sum_{i=1}^{n} q_i \bar{r}_i}{w} \left[\frac{2}{q_0 + w} \sum_{T=0}^{\infty} T^k \left(\frac{q_0 + w}{2} \right)^{T} - \frac{2}{q_0 - w} \sum_{T=0}^{\infty} T^k \left(\frac{q_0 - w}{2} \right)^{T} \right]. \quad (7)$$

В силу того, что $|q_0 \pm w| < 2$, ряды в квадратных скобках в правой части формулы (7) сходятся. Применяя известный результат (см. [18], стр. 555)

$$\sum_{n=0}^{\infty} n^k x^n = S_k(x) \equiv \left(x \frac{d}{dx} \right)^k \frac{1}{1 - x}, \quad (8)$$

мы можем записать

$$\mu_k[T] = \frac{\sum_{i=1}^{n} q_i \bar{r}_i}{w} \left[\frac{2}{q_0 + w} S_k\left(\frac{q_0 + w}{2} \right) - \frac{2}{q_0 - w} S_k\left(\frac{q_0 - w}{2} \right) \right]. \quad (9)$$

Формулы (8) и (9) позволяют выписать моменты случайной величины T для любого порядка k. В частности, момент 1-го порядка — это *математическое ожидание* $\mathbb{M}[T]$ случайной величины T. Так как $S_1(x) = x/(1 - x)^2$, из (9) получаем

$$\mathbb{M}[T] = \frac{1 + \sum_{i=1}^{n} q_i}{\sum_{i=1}^{n} q_i (1 - r_i)}. \quad (10)$$

Легко заметить, что полученная нами формула для $\mathbb{M}[T]$ вполне согласуется с ожидаемыми результатами в простейших частных случаях. Например, если $q_i = 0$ для всех i или $r_i = 1$ для всех i,

среднее время жизни становится бесконечным. Эти предельные ситуации отвечают случаю полного отсутствия угроз или случаю абсолютной защиты соответственно.

Аналогично, *дисперсия* $\mathbb{D}[T]$ случайной величины T определяется с помощью ее момента 2-го порядка следующим образом: $\mathbb{D}[T] = \mu_2[T] - \mathbb{M}[T]^2$. В силу того, что $S_2(x) = x(1+x)/(1-x)^3$, из (9) и (10) получаем:

$$\mathbb{D}[T] = \frac{1 - \sum_{i=1}^n q_i + \sum_{i=1}^n q_i r_i \left(3 + \sum_{j=1}^n q_j\right)}{\left[\sum_{i=1}^n q_i(1-r_i)\right]^2}. \tag{11}$$

Видно, что, если все q_i равны нулю или все r_i равны единице, дисперсия также как и математическое ожидание становится бесконечной.

В отсутствие защиты, то есть когда $r_i = 0$ для всех i, мы имеем

$$\mathbb{M}[T] = \frac{1}{\sum_{i=1}^n q_i} + 1, \quad \mathbb{D}[T] = \frac{1}{\sum_{i=1}^n q_i}\left(\frac{1}{\sum_{i=1}^n q_i} - 1\right).$$

Удобно выразить эти формулы через параметр $q_0 = 1 - \sum_{i=1}^n q_i$, представляющий собой вероятность отсутствия киберугроз:

$$\mathbb{M}[T] = \frac{2 - q_0}{1 - q_0}, \quad \mathbb{D}[T] = \frac{q_0}{(1-q_0)^2}.$$

Еще одна крайняя ситуация — случай частых угроз: $\sum_{i=1}^n q_i \approx 1$. Нетрудно видеть, что в этом случае

$$\mathbb{M}[T] \approx \frac{2}{1 - \sum_{i=1}^n q_i r_i}, \quad \mathbb{D}[T] \approx \frac{4\sum_{i=1}^n q_i r_i}{\left(1 - \sum_{i=1}^n q_i r_i\right)^2}.$$

3. Время жизни системы: случай совместных угроз

Ситуации, в которых на систему единовременно может воздействовать *только одна* угроза из некоторого списка возможных, представляются, на самом деле, весьма искусственными. На практике зачастую имеет место более общая картина, когда не исключаются случаи *одновременного* появления двух и более угроз, направленных на компьютерную систему. Описанная выше марковская модель киберугроз допускает естественное обобщение на указанные ситуации, приводя при этом к чисто техническим модификациям полученных в предыдущем разделе формул.

Итак, допустим теперь, что если система находится в безопасном состоянии s_0, на нее *единовременно* может воздействовать произвольный поднабор из набора n независимых киберугроз с вероятностями $q_1, q_2, \ldots, q_n$. Для описания возможных исходов удобно ввести следующую нотацию. Обозначим через x_i булеву переменную, равную 1, если в данный момент времени подействовала i-ая угроза, и равную 0 в обратном случае. Итоговый результат мы можем изобразить n-мерным булевым вектором $\mathbf{x} = (x_1, x_2, \ldots, x_n)$, у которого единицы стоят в позициях, отвечающих номерам появившихся в данный момент времени угроз. Таким образом, система, находящаяся в момент t в состоянии s_0, в момент $t+1$ оказывается в состоянии $s_{\sigma(\mathbf{x})}$, где $\sigma(\mathbf{x}) = \sum_{i=1}^n 2^{n-i} x_i$ — десятичная форма записи булева вектора $\mathbf{x} \in \{0,1\}^n$. Считая угрозы не влияющими друг на друга, нетрудно оценить вероятность перехода из состояния s_0 в состояние $s_{\sigma(\mathbf{x})}$:

$$Q_{\sigma(\mathbf{x})} = \prod_{i=1}^n \left[x_i q_i + (1 - x_i)(1 - q_i)\right]. \tag{12}$$

Здесь i-ый сомножитель в произведении в правой части данной формулы равен q_i, если i-ая угроза подействовала в момент t, и $1 - q_i$ — в обратном случае.

Далее, если в некоторый момент t система находится в состоянии $s_{\sigma(\mathbf{x})}$, где $\mathbf{x} \neq 0$, в момент $t+1$ мы имеем два возможных исхода:

– все угрозы ликвидированы и система возвращается в безопасное состояние s_0;

– *какая-либо* из угроз успешно реализовалась и система переходит в финальное состояние s_{2^n}.

Нетрудно видеть, что вероятности $R_{\sigma(\mathbf{x})}$ и $\bar{R}_{\sigma(\mathbf{x})}$ этих двух исходов равны

$$R_{\sigma(\mathbf{x})} = \prod_{i=1}^{n} \left[x_i(r_i - 1) + 1\right], \quad \bar{R}_{\sigma(\mathbf{x})} = 1 - R_{\sigma(\mathbf{x})}, \tag{13}$$

где параметр r_i означает вероятность успешного отражения i-ой угрозы.

С учетом вышесказанного, последовательность переходов между состояниями рассматриваемой нами системы представляет собой простую марковскую цепь с матрицей переходных вероятностей вида:

$$\Pi = \begin{pmatrix} Q_0 & Q_1 & Q_2 & \dots & Q_{2^n} & 0 \\ R_1 & 0 & 0 & \dots & 0 & \bar{R}_1 \\ R_2 & 0 & 0 & \dots & 0 & \bar{R}_2 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ R_{2^n} & 0 & 0 & \dots & 0 & \bar{R}_{2^n} \\ 0 & 0 & 0 & \dots & 0 & 1 \end{pmatrix}. \tag{14}$$

Сравнение с матрицей (2) показывает, что данная марковская цепь получается из описанной нами в предыдущем разделе марковской цепи формальной заменой:

$$n \longrightarrow 2^n, \quad q_i \longrightarrow Q_i, \quad r_i \longrightarrow R_i. \tag{15}$$

В частности, распределение случайной величины T и ее числовые характеристики могут быть получены из приведенных выше результатов подстановкой (15). В качестве примера выпишем явные аналитические выражения для среднего времени жизни $\mathbb{M}[T]$ и дисперсии $\mathbb{D}[T]$, получаемые из формул (10) и (11) с помощью замены (15):

$$\mathbb{M}[T] = \frac{1 + \sum\limits_{\mathbf{x}\neq 0} Q_{\sigma(\mathbf{x})}}{\sum\limits_{\mathbf{x}\neq 0} Q_{\sigma(\mathbf{x})}\left(1 - R_{\sigma(\mathbf{x})}\right)}, \tag{16}$$

$$\mathbb{D}[T] = \frac{1 - \sum\limits_{\mathbf{x}\neq 0} Q_{\sigma(\mathbf{x})} + \sum\limits_{\mathbf{x}\neq 0} Q_{\sigma(\mathbf{x})} R_{\sigma(\mathbf{x})} \left(3 + \sum\limits_{\mathbf{x}'\neq 0} Q_{\sigma(\mathbf{x}')}\right)}{\left[\sum\limits_{\mathbf{x}\neq 0} Q_{\sigma(\mathbf{x})}(1 - R_{\sigma(\mathbf{x})})\right]^2}. \tag{17}$$

Здесь $Q_{\sigma(\mathbf{x})}$ и $R_{\sigma(\mathbf{x})}$ определяются формулами (12) и (13) соответственно, а суммирования осуществляются по всевозможным ненулевым векторам $\mathbf{x}$ и $\mathbf{x}'$ из $\{0,1\}^n$.

Полученные в настоящем разделе результаты были проверены с помощью численных экспериментов. Для этого с помощью пакета математических программ MatLAB была разработана имитационная модель, позволяющая получать различные реализации марковской цепи с матрицей переходных вероятностей (14). На основе статистической обработки N реализаций марковской цепи ($N \approx 100000$) мы получили численные оценки для величин $\mathbb{M}[T]$ и $\mathbb{D}[T]$ в случаях одной и двух угроз, которые затем сравнивались с теоретическими оценками, предсказываемыми формулами (16) и (17). Результаты этого сравнения для некоторых значений параметров модели приведены в таблицах 1 и 2. Из таблиц видно, что теоретические и экспериментальные результаты хорошо согласуются друг с другом.

Table 1. Expected value and variance of lifetime T for one cyber threat

Таблица 1. Математическое ожидание и дисперсия времени жизни T в случае одной киберугрозы

Параметры модели		**Математическое ожидание** $\mathbb{M}[T]$		**Дисперсия** $\mathbb{D}[T]$	
q	r	**Теория**	**Эксперимент**	**Теория**	**Эксперимент**
0,2000	0,8000	30,0000	30,0235	820,0000	819,7795
0,4000	0,5000	7,0000	7,0005	32,0000	31,6664
0,7000	0,3000	3,4693	3,4710	4,48563	4,6000

Table 2. Expected value and variance of lifetime T for two cyber threats

Таблица 2. Математическое ожидание и дисперсия времени жизни T в случае двух киберугроз

Параметры модели				**Математическое ожидание** $\mathbb{M}[T]$		**Дисперсия** $\mathbb{D}[T]$	
q_1	q_2	r_1	r_2	**Теория**	**Эксперимент**	**Теория**	**Эксперимент**
0,2000	0,5000	0,8000	0,7000	8,6956	8,7331	56,0491	55,9479
0,4000	0,2000	0,5000	0,5000	5,4285	5,4352	16,8980	16,8045
0,7000	0,2000	0,3000	0,7000	3,3807	3,3765	4,2068	4,1692

4. Оптимизация выбора средств защиты информации

В работе [15] была высказана идея об использовании описанной в разделе 1 марковской модели киберугроз в задаче о выборе оптимального набора средств защиты информации. Более подробно эта идея обсуждается в [16]. В данной главе мы напомним основную постановку соответствующей оптимизационной задачи применительно к модифицированной версии модели с совместными киберугрозами.

Допустим, что для отражения существующих киберугроз имеется набор m различных средств защиты. Обозначим через z_a булеву переменную, ассоциированную с a-ым средством защиты: $z_a = 1$, если a-ое средство используется, и $z_a = 0$ — в обратном случае. Таким образом, мы имеем множество из 2^m возможных конфигураций системы защиты информации; каждая конфигурация будет описываться булевым вектором $\mathbf{z} = (z_1, z_2, \dots, z_m) \in \{0,1\}^m$. В частности, нулевому $\mathbf{z}$ будет отвечать конфигурация, в которой никакие средства не задействованы, а случай $\mathbf{z} = (1,1,\dots,1)$ отвечает использованию всех имеющихся средств защиты информации.

Обозначим через $r_{i,a}$ вероятность отражения i-ой угрозы a-ым средством защиты. В общем случае одну и ту же угрозу могут отражать сразу несколько средств защиты, поэтому вероятность отражения i-ой угрозы *хотя бы одним* средством защиты определяется в соответствии с формулой (см. [19], стр. 99):

$$r_i(\mathbf{z}) = \sum_{k=1}^{m} (-1)^k \sum_{a_1<a_2<\dots<a_k} (r_{i,a_1} z_{a_1})(r_{i,a_2} z_{a_2}) \dots \left(r_{i,a_k} z_{a_k}\right). \tag{18}$$

Подстановка этих выражений в формулу (13) позволяет получить вероятности отражения действующих поднаборов киберугроз, изображаемых, следуя нотации предыдущего раздела, n-мерными булевыми векторами $\mathbf{x} = (x_1, x_2, \dots, x_n)$:

$$R_{\sigma(\mathbf{x})}(\mathbf{z}) = \prod_{i=1}^{n} \left[(1 - x_i) r_i(\mathbf{z}) + 1\right]. \tag{19}$$

Напомним, что здесь $x_i = 1$, если в данный момент времени подействовала i-ая угроза, и $x_i = 0$ — в обратном случае. Отсюда для среднего времени жизни системы мы получаем выражение, зависящее от $\mathbf{z}$:

$$\mathbb{M}[T](\mathbf{z}) = \frac{1 + \sum\limits_{\mathbf{x}\neq 0} Q_{\sigma(\mathbf{x})}}{\sum\limits_{\mathbf{x}\neq 0} Q_{\sigma(\mathbf{x})} \left(1 - R_{\sigma(\mathbf{x})}(\mathbf{z})\right)}. \tag{20}$$

На практике довольно часто ставится задача определения *оптимального поднабора* из некоторого заранее заданного набора средств защиты информации. В зависимости от конкретных целей соответствующая задача оптимизации может быть сформулирована по-разному (см., например, [20]). Оказывается, что с использованием рассматриваемой модели мы можем сформулировать несколько задач оптимизации, сводящихся к нахождению определенного баланса между экономической стоимостью защитных мер и их функциональной эффективностью.

Обозначим через c_a стоимость a-го средства защиты (в условных денежных единицах). Тогда функция стоимости данной конфигурации системы защиты информации имеет следующий вид:

$$C(\mathbf{z}) = \sum_{a=1}^{m} c_a z_a.$$

Первая из оптимизационных задач, которую мы можем сформулировать с использованием имеющихся конструкций, звучит так: при существующих ограничениях на используещиеся при построении системы защиты ресурсы требуется максимизировать среднее время жизни компьютерной системы. Формальная запись данной оптимизационной задачи имеет следующий вид:

$$\mathbb{M}[T](\mathbf{z}) \longrightarrow \max, \quad C(\mathbf{z}) \leq C_0. \tag{21}$$

Здесь C_0 — положительная постоянная, означающая максимальную величину затрат на защиту от угроз. Вторая оптимизационная задача заключается в поиске такой конфигурации системы защиты, при которой вложения в защиту будут минимальны при имеющемся ограничении на продолжительность функционирования компьютерной системы:

$$\mathbb{M}[T](\mathbf{z}) \geq T_0, \quad C(\mathbf{z}) \longrightarrow \min. \tag{22}$$

Отметим, что обе эти задачи представляют интерес и часто встречаются при решении реальных задач при проектировании и разработке систем обеспечения информационной безопасности.

Как следует из формул (18)–(20), величина $\mathbb{M}[T](\mathbf{z})$ имеет вид $1/P(\mathbf{z})$, где $P(\mathbf{z})$ представляет собой полином степени m от булевых переменных $z_1, \dots, z_m$. Следовательно, оптимизационные задачи (21) и (22) принадлежат к классу задач нелинейного целочисленного программирования. Как известно, универсальных и эффективных алгоритмов решения подобных задач на сегодняшний день не существует. С другой стороны, как показали численные эксперименты, при небольших значениях m ($m \lesssim 15$) задачи (21) и (22) могут быть решены методом прямого перебора. При больших m определенную эффективность демонстрирует метод последовательного анализа вариантов [21], учитывающий имеющуюся специфику функций $C(\mathbf{z})$ и $\mathbb{M}[T](\mathbf{z})$. Строгая оценка вычислительной

сложности этого подхода будет представлять для нас дальнейший исследовательский интерес, а в настоящей статье мы ограничимся сделанными замечаниями и просто продемонстрируем применение изложенных нами идей на гипотетическом примере.

Пример. Рассмотрим абстрактную компьютерную систему (это может быть, например, отдельный компьютер с установленным системным и прикладным ПО или совокупность подобных компьютеров, объединенных в локальную сеть) и продемонстрируем как на основе рассмотренной выше марковской модели безопасности может быть определен оптимальный набор средств ее защиты.

При выборе наиболее актуальных угроз для данной системы мы можем воспользоваться банком данных угроз безопасности информации ФСТЭК России[1]. Ограничиваясь только угрозами, устраняемыми программными средствами защиты и характерными только для нарушителей с низким потенциалом, мы примем в качестве наиболее актуальных восемь угроз, перечисленных в таблице 3 (конечно, в реальных ситуациях их больше). В этой же таблице приведены вероятности возникновения этих угроз за единичный интервал времени $\Delta t = 1$. Отметим, что значения q_i в рассматриваемом примере носят достаточно декларативный характер; для конкретных объектов эти величины на практике получаются экспертным методом с учетом применяемых на объекте информационных технологий и программно-аппаратных средств.

Table 3. Actual threats for the described computer system and probability of their appearances for a single time interval

Таблица 3. Актуальные угрозы для рассматриваемой компьютерной системы и вероятности их появления за единичный интервал времени

№	ID	Описание угрозы	Вероятность
1	УБИ.006	Угроза внедрения кода или данных	0,02
2	УБИ.018	Угроза загрузки нештатной операционной системы	0,01
3	УБИ.031	Угроза использования механизмов авторизации для повышения привилегий	0,03
4	УБИ.034	Угроза использования слабостей протоколов сетевого/локального обмена данными	0, 03
5	УБИ.116	Угроза перехвата данных, передаваемых по вычислительной сети	0,02
6	УБИ.130	Угроза подмены содержимого сетевых ресурсов	0,04
7	УБИ.167	Угроза заражения компьютеров при посещении неблагонадежных сайтов	0,05
8	УБИ.170	Угроза неправомерного шифрования информации	0,02

В таблице 4 приведен перечень представителей классов типовых средств защиты информации, наиболее часто используемых для отражения киберугроз из таблицы 3, а также ориентировочные затраты, связанные с их приобретением и эксплуатацией[2].

В соответствии с таблицей 4 функция стоимости $C(\mathbf{z})$, определенная на множестве конфигураций системы защиты, для нашего примера имеет вид:

$$C(\mathbf{z}) = 20000z_1 + 10000z_2 + 8000z_3 + 15000z_4 + 10000z_5 + 5000z_6.$$

[1] https://bdu.fstec.ru/threat

[2] Стоимости приведены достаточно условно ввиду большого разнообразия имеющихся на современном рынке конкретных представителей различных классов средств защиты. Кроме того, в реальных системах стоимости очень сильно зависят от масштабов самой системы (числа рабочих станций, числа пользователей и т.д.), а также от срока их эксплуатации и пр.

Вероятности $r_{i,a}$ отражения угроз средствами защиты на практике обычно определяются с помощью экспертных оценок [22]. В нашем случае мы введем эти вероятности также довольно декларативно, так как в реальных ситуациях необходимо учитывать множество особенностей конкретной компьютерной системы и конкретных используемых средств защиты информации:

$$\|r_{i,a}\| = \begin{pmatrix} 0{,}8 & 0{,}5 & 0{,}25 & 0{,}5 & 0 & 0 \\ 0 & 0 & 0,5 & 0 & 0{,}9 & 0 \\ 0 & 0 & 0 & 0,8 & 0{,}2 & 0 \\ 0 & 0{,}7 & 0 & 0 & 0 & 0{,}5 \\ 0 & 0{,}8 & 0 & 0 & 0 & 0{,}5 \\ 0 & 0{,}8 & 0 & 0 & 0 & 0{,}5 \\ 0{,}9 & 0{,}5 & 0 & 0 & 0 & 0 \\ 0{,}2 & 0 & 0{,}2 & 0{,}5 & 0{,}1 & 0 \end{pmatrix}. \tag{23}$$

Отметим, что в нашем примере каждая из угроз может быть отражена несколькими средствами защиты с различной степенью эффективности. Согласно данной матрице, например, угроза УБИ.167 (угроза заражения компьютеров при посещении неблагонадежных сайтов) с вероятностью 0,9 отражается имеющимся антивирусным ПО и с вероятностью 0,5 отражается межсетевым экраном с помощью различных механизмов фильтрации и анализа сетевого трафика.

Ограничимся решением оптимизационной задачи (22). Подставляя элементы матрицы (23) в формулу (18), получаем набор из $n = 8$ полиномов $r_i(\mathbf{z})$ от 6 булевых переменных $z_1, \ldots, z_6$, ассоциированных с соответствующими средствами защиты из таблицы 3:

$$\begin{aligned}
r_1(\mathbf{z}) &= 0{,}8z_1 + 0{,}5z_2 + 0{,}25z_3 + 0{,}5z_4 - 0{,}4z_1z_2 - 0{,}2z_1z_3 - 0{,}4z_1z_4 - 0{,}125z_2z_3 - \\
&\quad - 0{,}25z_2z_4 - 0{,}125z_3z_4 + 0{,}1z_1z_2z_3 + 0{,}2z_1z_2z_4 + 0{,}1z_1z_3z_4 + 0{,}0625z_2z_3z_4 - \\
&\quad - 0{,}05z_1z_2z_3z_4, \\
r_2(\mathbf{z}) &= 0{,}5z_3 + 0{,}9z_5 - 0{,}45z_3z_5, \\
r_3(\mathbf{z}) &= 0{,}8z_4 + 0{,}2z_5 - 0{,}16z_4z_5, \\
r_4(\mathbf{z}) &= 0{,}7z_2 + 0{,}5z_6 - 0{,}35z_2z_6, \\
r_5(\mathbf{z}) &= 0{,}8z_2 + 0{,}5z_6 - 0{,}4z_2z_6, \\
r_6(\mathbf{z}) &= 0{,}8z_2 + 0{,}5z_6 - 0{,}4z_2z_6, \\
r_7(\mathbf{z}) &= 0{,}9z_1 + 0{,}5z_2 - 0{,}45z_1z_2, \\
r_8(\mathbf{z}) &= 0{,}2z_1 + 0{,}2z_3 + 0{,}5z_4 + 0{,}1z_5 - 0{,}04z_1z_3 - 0{,}1z_1z_4 - 0{,}02z_1z_5 - 0{,}02z_3z_5 - \\
&\quad - 0{,}1z_3z_4 - 0{,}05z_4z_5 + 0{,}02z_1z_3z_4 + 0{,}004z_1z_3z_5 + 0{,}01z_1z_4z_5 + 0{,}01z_3z_4z_5 - \\
&\quad - 0{,}002z_1z_3z_4z_5.
\end{aligned}$$

После подстановки полиномов $r_i(\mathbf{z})$ в формулу (19), находим 2^n полиномов $R_{\sigma(\mathbf{x})}(\mathbf{z})$[3], определяющих вероятности отражения поднаборов $\mathbf{x}$ киберугроз данной конфигурацией средств защиты $\mathbf{z}$. Далее, используя вероятности возникновения угроз q_i, приведенные в таблице 3, получаем в соответствии с формулой (12):

$$Q_{\sigma(\mathbf{x})} = (x_1 - 0{,}98)(x_2 - 0{,}99)(x_3 - 0{,}97)(x_4 - 0{,}97)(x_5 - 0{,}98) \times (x_6 - 0{,}96)(x_7 - 0{,}95)(x_8 - 0{,}98).$$

[3]Напомним, что $\sigma(\mathbf{x}) = \sum_{i=1}^{n} 2^{n-i}x_i$.

Table 4. Security remedies against current cyber threats and their costs

Таблица 4. Средства защиты от актуальных киберугроз и их стоимости

№	Средство защиты	Стоимость c_a в усл. ед.
1	Средство антивирусной защиты	20 000
2	Программный межсетевой экран	10 000
3	Средство защиты от НСД	8 000
4	Система разграничения доступа	15 000
5	Средство доверенной загрузки	10 000
6	Средство криптографической защиты информации	5 000

Подставляя полученные выражения для $R_{\sigma(\mathbf{x})}(\mathbf{z})$ и $Q_{\sigma(\mathbf{x})}$ в формулу (16), после суммирования по всевозможным $\mathbf{x} \in \{0,1\}^n$ находим среднее время жизни нашей системы в виде $\mathbb{M}[T](\mathbf{z}) = P^{-1}(\mathbf{z})$, где $P(\mathbf{z})$ — полином шестой степени от булевых переменных $z_1, \ldots, z_6$ (мы не выписываем его здесь в виду громоздкости). На рис. 3 приведена графическая зависимость среднего времени жизни системы от номера конфигурации $\sigma(\mathbf{z})$. Из рисунка видно, что минимальное среднее время жизни системы соответствует нулевой конфигурации $\sigma(\mathbf{z}) = 0$ ($\mathbb{M}[T]_{\min} = 5{,}9891$), а максимальное — конфигурации $\sigma(\mathbf{z}) = 2^m - 1 = 64$ ($\mathbb{M}[T]_{\max} = 48{,}8869$).

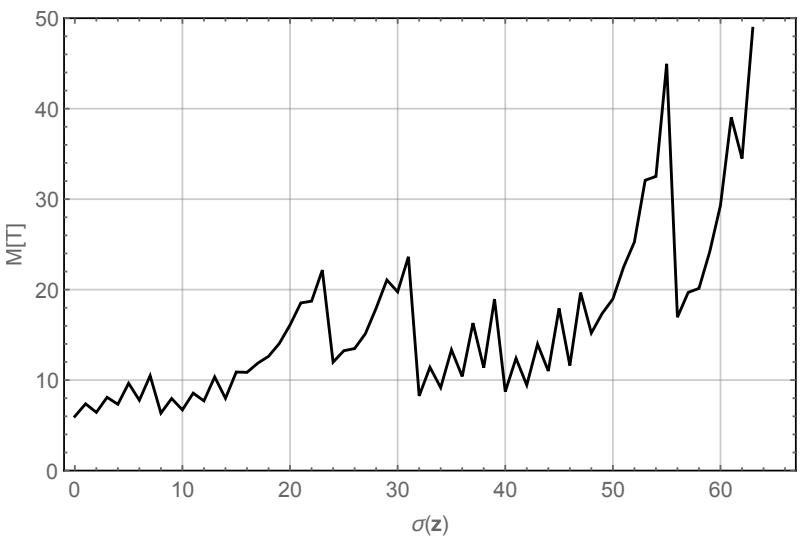

Fig. 3. Dependence of $\mathbb{M}[T]$ on $\sigma(\mathbf{z})$ for the considered example

Рис. 3. Зависимость $\mathbb{M}[T]$ от $\sigma(\mathbf{z})$ для рассматриваемого примера

Перейдем к решению оптимизационной задачи (22). Так как число возможных вариантов здесь невелико и равно $2^m = 64$, мы решали эту задачу методом прямого перебора. В таблице 5 для каждого рассматриваемого значения T_0 приводится найденное оптимальное решение $\mathbf{z}$ и соответствующая стоимость $C(\mathbf{z})$. Как видно из таблицы, стоимость оптимальной конфигурации средств защиты увеличивается с ростом T_0, что, очевидно, согласуется с реальным положением вещей, так как более длительное безотказное функционирование системы требует больших затрат.

В заключение отметим, что цель данного примера — демонстрация использования рассмотренной выше марковской модели киберугроз для формулировки задачи о выборе оптимального поднабора средств защиты информации. Данный пример никоим образом не исчерпывает всего

Table 5. Solutions of the optimization task (22) for the different values of T_0

Таблица 5. Решения оптимизационной задачи (22) для различных значений T_0

T_0	**Оптимальная конфигурация**	**Стоимость**, руб.
10	$\mathbf{z} = (0, 1, 0, 0, 0, 0)$	10 000
15	$\mathbf{z} = (0, 1, 0, 1, 0, 0)$	25 000
20	$\mathbf{z} = (0, 1, 1, 1, 0, 1)$	38 000
25	$\mathbf{z} = (1, 1, 0, 1, 0, 0)$	45 000
30	$\mathbf{z} = (1, 1, 0, 1, 0, 1)$	50 000
35	$\mathbf{z} = (1, 1, 1, 1, 0, 1)$	58 000
40	$\mathbf{z} = (1, 1, 0, 1, 1, 1)$	60 000

многообразия возникающих на практике ситуаций с системами защиты информации и служит скорее иллюстрацией одного из возможных подходов к оценке уровня защищенности информации в современных информационных системах.

Заключение

В настоящей статье мы продолжили исследование класса марковских моделей киберугроз, начатое в предыдущих работах [14—16]. В рамках этих моделей компьютерная система, подвергающаяся действию киберугроз, рассматривается как система с отказами и восстановлениями, функционируя до момента своего полного (фатального) отказа. В настоящей работе мы ввели понятие времени жизни системы, определяя его как число переходов в соответствующей марковской цепи до первого попадания в финальное состояние. Получив явную формулу для распределения данной случайной величины, мы также вычислили ее явные числовые характеристики — математическое ожидание и дисперсию. Далее мы существенно обобщили рассматриваемый класс марковских моделей, отказавшись от допущения о несовместности киберугроз. В заключение с помощью марковской модели совместных киберугроз мы сформулировали две задачи нелинейного дискретного программирования о нахождении оптимального набора средств защиты. В качестве примера рассмотрена задача о выборе оптимальной конфигурации средств защиты для простейшей компьютерной системы с восемью актуальными кибеугрозами.

Наши дальнейшие исследовательские перспективы будут связаны с ослаблением допущения о независимости киберугроз, а также с разработкой эффективных подходов к решению сформулированных в разделе 4 оптимизационных задач. Отметим также, что полученные нами результаты могут быть использованы в различных методиках и стандартах, посвященных оценке и анализу защищенности современных компьютерных систем и вычислительных сетей.

References

[1] N. Ye, Y. Zhang, and B. C.M., “Robustness of the Markov-chain model for cyber-attack detection”, *IEEE Transactions on Reliability*, vol. 53, no. 1, pp. 116–123, 2004.

[2] S. Jha, K. Tan, and R. Maxion, “Markov Chains, Classifiers, and Intrusion Detection.”, in *Proc. IEEE Computer Security Foundations Workshops*, vol. 1, 2001, pp. 206–219.

[3] A. Ahmadian Ramaki, A. Rasoolzadegan, and A. Javan Jafari, “A systematic review on intrusion detection based on the Hidden Markov Model”, *Statistical Analysis and Data Mining: The ASA Data Science Journal*, vol. 11, no. 3, pp. 111–134, 2018.

[4] P. Garcia-Teodoro, J. Diaz-Verdejo, G. Maciá-Fernández, and E. Vázquez, “Anomaly-based network intrusion detection: Techniques, systems and challenges”, *Computers and Security*, vol. 28, no. 1-2, pp. 18–28, 2009.

[5] L. Billings, W. Spears, and I. Schwartz, "A unified prediction of computer virus spread in connected networks", *Physics Letters A*, vol. 297, no. 3-4, pp. 261–266, 2002.

[6] A. Boyko, "Sposob analiticheskogo modelirovaniya protsessa rasprostraneniya virusov v komp'yuternykh setyakh razlichnoy struktury", *Trudy SPIIRAN*, vol. 5, no. 42, pp. 196–211, 2015.

[7] Y. Dalinger, D. Babanin, and B. S.M., "Matematicheskie modeli rasprostraneniya virusov v komp'yuternykh setyakh razlichnoy struktury", *Informatika i sistemy upravleniya*, no. 4, pp. 25–33, 2012.

[8] A. Del Rey, "Mathematical modeling of the propagation of malware: a review", *Security and Communication Networks*, vol. 8, no. 15, pp. 2561–2579, 2015.

[9] M. Yang, R. Jiang, T. Gao, W. Xie, and J. Wang, "Research on Cloud Computing Security Risk Assessment Based on Information Entropy and Markov Chain.", *I. J. Network Security*, vol. 20, no. 4, pp. 664–673, 2018.

[10] C. Xiaolin, T. Xiaobin, Z. Yong, and X. Hongsheng, "A Markov game theory-based risk assessment model for network information system", in *International Conference on Computer Science and Software Engineering, China*, IEEE, vol. 3, 2008, pp. 1057–1061.

[11] H. Orojloo and M. Azgomi, "A method for modeling and evaluation of the security of cyber-physical systems", in *11th International ISC Conference on Information Security and Cryptology, Iran*, IEEE, 2014, pp. 131–136.

[12] J. Almasizadeh and M. Azgomi, "A stochastic model of attack process for the evaluation of security metrics", *Computer Networks*, vol. 57, no. 10, pp. 2159–2180, 2013.

[13] K. Shcheglov and A. Shcheglov, "Markovskie modeli ugrozy bezopasnosti informatsionnoy sistemy", *Izvestiya vysshikh uchebnykh zavedeniy. Priborostroenie*, vol. 58, no. 12, pp. 957–965, 2015.

[14] A. Rosenko, "Matematicheskoe modelirovanie vliyaniya vnutrennikh ugroz na bezopasnost' konfidentsial'noy informatsii, tsirkuliruyushchey v avtomatizirovannoy informatsionnoy sisteme", *Izvestiya Yuzhnogo federal'nogo universiteta. Tekhnicheskie nauki*, vol. 85, no. 8, pp. 71–81, 2008.

[15] A. Magazev and V. Tsyrulnik, "Investigation of a Markov Model for Computer System Security Threats", *Automatic Control and Computer Sciences*, vol. 52, no. 7, pp. 615–624, 2018.

[16] A. Magazev and V. Tsyrulnik, "Optimizing the selection of information security remedies in terms of a Markov security model", in *Journal of Physics: Conference Series*, vol. 1096, 2018, p. 012 160.

[17] D. Shirtz and Y. Elovici, "Optimizing investment decisions in selecting information security remedies", *Information Management and Computer Security*, vol. 19, no. 2, pp. 95–112, 2011.

[18] P. A.P., Y. Brychkov, and M. O.I., *Integrals and series: Elementary functions*. Gordon&Breach Sci. Publ., New York, 1986, vol. 1.

[19] W. Feller, *An introduction to probability theory and its applications*. John Wiley & Sons Inc, 1968, vol. 1, 528 pp.

[20] A. e. a. Ovchinnikov, "Matematicheskaya model' optimal'nogo vybora sredstv zashchity ot ugroz bezopasnosti vychislitel'noy seti predpriyatiya", *Vestnik Moskovskogo gosudarstvennogo tekhnicheskogo universiteta im. N. E. Baumana. Ser. "Priborostroenie"*, no. 3, pp. 115–121, 2007.

[21] M. Kovalev, *Diskretnaya optimizatsiya (tselochislennoe programmirovanie)*, 2-e izd., stereotipnoe. Editorial URSS, 2003, 192 pp.

[22] Beshelev, S.D., and F. Gurvich, *Matematiko-statisticheskie metody ekspertnykh otsenok*. 1980, 263 pp.