Стохастические матрицы и анализ защищённости автоматизированных систем

А. С. ВЫДРИН, А. В. МИХАЛЁВ
Московский государственный университет им. М. В. Ломоносова

УДК 512.64+519.2

Ключевые слова: стохастические матрицы, автоматизированные системы.

Аннотация

Цель данной работы — рассмотреть теоретические основы процесса сканирования (анализа) защищённости автоматизированных систем и доказать возможность определения распределения внутренних состояний системы на основе проведения процесса сканирования, называемого в соответствии с международными стандартами процессом анализа защищённости. Проведение данного процесса и наличие средств для его проведения является необходимым условием для построения эффективных систем информационной безопасности.

Abstract

A. S. Vydrin, A. V. Mikhalev, Stochastic matrices and the assessment of the vulnerability of automated systems, Fundamentalnaya i prikladnaya matematika, vol. 13 (2007), no. 1, pp. 61—99.

The aim of this article is to consider the theoretical basis of automated system vulnerability scanning (assessment) process and to prove the possibility of determining the internal state distribution based on conducting the scanning process. According to international information security standards, the scanning process is called the vulnerability assessment process. Conducting this process and the existence of the required technical resources is a necessary condition for creating effective information security systems.

1. Вероятностные автоматы

Вероятностные автоматы возможно использовать для описания переходов системы, имеющей уязвимости программной реализации, а также для описания сложных систем. В данной работе вероятностные автоматы используются для моделирования исходной автоматизированной системы. Вероятностные автоматы, так же как детерминированные автоматы (или просто автоматы), принимают входные воздействия и реагируют на них путём выдачи выходного сигнала, а также перехода из текущего внутреннего состояния в следующее. В отличие от детерминированных автоматов, природа смены состояний и выходной реакции вероятностного автомата носит вероятностный характер. Введение в теорию абстрактных вероятностных автоматов можно найти в [1].

Фундаментальная и прикладная математика, 2007, том 13, № 1, с. 61—99.

В данной работе вероятностные автоматы используются как инструмент для построения моделей процесса анализа защищённости.

Определение 1.1. Пусть имеется множество входных сигналов X, множество выходных сигналов Y и множество Q, называемое множеством состояний. Вероятностный автомат $\mathcal{A}$ есть четвёрка $\mathcal{A} = (X, Y, Q, p)$, где p — функция вероятностного перехода, $p\colon X \times Q \times Y \times Q \mapsto \mathbb{R}^+$, такая что для любой четвёрки (x, q, y, q') выполняются свойства

$$p(x, q, y, q') \geqslant 0,$$
$$\sum_{(y,q')\in Y\times Q} p(x, q, y, q') = 1.$$

В дальнейшем в данной работе рассматриваются только конечные вероятностные автоматы, т. е. вероятностные автоматы, для которых $|X| < \infty$, $|Y| < \infty$, $|Q| < \infty$.

Пример 1.2 (детерминированный автомат). Пусть $\mathcal{A}$ — конечный детерминированный автомат с функцией перехода α и функцией выхода β, которые определяются следующим образом: если автомат $\mathcal{A}$ находится в состоянии $q \in Q$ и на его вход поступает сигнал $x \in X$, то он переходит в состояние $\alpha(x, q)$ и выдаёт сигнал $\beta(x, q) \in Y$. Тогда его можно представить как вероятностный автомат со следующей функцией перехода:

$$p(x, q, y, q') = \begin{cases} 1, & \text{если } q' = \alpha(x, q),\ y = \beta(x, q), \\ 0 & \text{иначе.} \end{cases}$$

Пример 1.3 (автомат Бернулли, простейший вероятностный автомат). Автомат Бернулли определяется следующим образом: $|X| = |Q| = 1$, т. е. фактически это автомат без состояний и без реакции на входные последовательности, $p(x, q, y, q') = p(y)$ — вероятность выдачи выходного сигнала, равного y. Данный автомат имеет ещё одно название: неуправляемый датчик случайных чисел, или просто датчик случайных чисел.

Определение 1.4. Пусть имеется вероятностный автомат $\mathcal{A} = (X, Y, Q, p)$. Через $p(x, q, q')$ обозначим вероятность перехода из состояния q в состояние q' при поступлении входного сигнала x.

Предложение 1.5. $p(x, q, q') = \sum\limits_{y\in Y} p(x, q, y, q')$.

Доказательство. Рассмотрим события

$\omega = \{$вероятностный автомат, находясь в состоянии q при поступлении x, переходит в состояние $q'\}$,

$\omega_y = \{$вероятностный автомат, находясь в состоянии q при поступлении x, переходит в состояние q' и выдаёт на выходе сигнал $y\}$.

Тогда ясно, что для любых $y_1 \neq y_2$ справедливо $\omega_{y_1} \cap \omega_{y_2} = \varnothing$ (поскольку одновременно невозможно выдать два различных сигнала). Также ясно, что $\omega = \bigcup\limits_{y \in Y} \omega_y$, поскольку хотя бы какой-то сигнал автомат выдаёт всегда. Используя аддитивность вероятностной меры, получаем утверждение предложения. □

Определение 1.6. Пусть имеется вероятностный автомат $\mathcal{A} = (X, Y, Q, p)$. Через $p(x, q, y)$ обозначим вероятность выдачи выходного сигнала, равного y, при условии, что автомат при поступлении входного сигнала x находился в состоянии q.

Предложение 1.7. $p(x, q, y) = \sum\limits_{q' \in Q} p(x, q, y, q')$.

Доказательство данного предложения аналогично доказательству предложения 1.5.

Под процессом сканирования автоматизированной системы (или вероятностного автомата $\mathcal{A}$) понимается процесс передачи на вход системы заранее заданной последовательности входных сигналов $\{x_1, \ldots, x_m\}$ и получения последовательности выходных сигналов $\{y_1, \ldots, y_m\}$. При этом в том случае, когда больше про вероятностный автомат ничего не известно, данный процесс называется *внешним сканированием*. Также при решении задач анализа защищённости автоматизированной системы рассматривается процесс *внутреннего сканирования*, при котором считается известным распределение вероятностей перехода $p(x, q, y, q')$.

Определение 1.8. Пусть $v \in \mathbb{C}^n$, $A \in \mathrm{M}_n(\mathbb{C})$. Положим

$$\|v\| = \sum_{i=1}^{n} |v_i|, \quad \|A\| = \sup_{v \neq 0} \frac{\|Av\|}{\|v\|}$$

(соответственно норма линейного пространства и кольца матриц).

Замечание 1.9. Для введённых норм линейного пространства $\mathbb{C}^n$ и кольца матриц $\mathrm{M}_n(\mathbb{C})$ верны следующие утверждения:

1) для любого $v \in \mathbb{C}^n$ справедливо $\|v\| \geqslant 0$; $\|v\| = 0$ тогда и только тогда, когда $v = 0$;
2) для любой матрицы $A \in \mathrm{M}_n(\mathbb{C})$ справедливо $\|A\| \geqslant 0$; $\|A\| = 0$ тогда и только тогда, когда $A = 0$;
3) для любых $v \in \mathbb{C}^n$, $\lambda \in \mathbb{C}$ справедливо $\|\lambda v\| = |\lambda| \, \|v\|$;
4) для любых $A \in \mathrm{M}_n(\mathbb{C})$, $\lambda \in \mathbb{C}$ справедливо $\|\lambda A\| = |\lambda| \, \|A\|$;
5) для любых $u, v \in \mathbb{C}^n$ выполнено $\|u + v\| \leqslant \|u\| + \|v\|$;
6) для любых $A, B \in \mathrm{M}_n(\mathbb{C})$ выполнено $\|A + B\| \leqslant \|A\| + \|B\|$;
7) для любых $A, B \in \mathrm{M}_n(\mathbb{C})$ выполнено $\|AB\| \leqslant \|A\| \, \|B\|$.

2. Распределения состояний и выходных сигналов при сканировании

Пусть вероятностный автомат $\mathcal{A}$ в текущий момент времени имеет вектор распределения состояний $\rho_0(q)$ и мы подаём на вход некоторый сигнал x. Возникает вопрос, каким будет вектор распределения состояний в следующий момент $\rho_1(q)$. Ответ на него даёт следующее предложение.

Предложение 2.1. *Для распределения $\rho_1(q)$ справедливо равенство*

$$\rho_1(q) = \sum_{r \in Q} \rho_0(r) p(x, r, q).$$

Доказательство. Пусть событие ω определено равенством

$$\omega = \{\text{вероятностный автомат после подачи входного сигнала } x \text{ находится в состоянии } q\}.$$

Очевидно, что $\rho_1(q) = \mathrm{P}(\omega)$. Рассмотрим следующие события ω_r:

$$\omega_r = \{\text{вероятностный автомат до подачи сигнала находился в состоянии } r \text{ и после подачи сигнала } x \text{ перешёл в состояние } q\}.$$

Очевидно, что выполнено равенство

$$\omega = \bigcup_{r \in Q} \omega_r,$$

поскольку в любом случае до подачи сигнала вероятностный автомат находился в каком-либо состоянии. В то же время для любых различных состояний $r, s \in Q$ верно утверждение

$$\omega_r \cap \omega_s = \varnothing,$$

поскольку до подачи сигнала вероятностный автомат не мог находиться одновременно в двух различных состояниях. Значит, из аддитивности вероятностной меры получаем, что

$$\mathrm{P}(\omega) = \mathrm{P}\Big(\bigcup_{r \in Q} \omega_r \Big) = \sum_{r \in Q} \mathrm{P}(\omega_r).$$

Рассмотрим события

$$\alpha_r = \{\text{вероятностный автомат до подачи сигнала находился в состоянии } r\},$$
$$\beta_r = \{\text{вероятностный автомат, находясь в состоянии } r, \text{ после подачи сигнала } x \text{ перешёл в состояние } q\}.$$

Из построений событий ясно, что имеет место равенство

$$\omega_r = \alpha_r \cap \beta_r.$$

В то же время нетрудно видеть, что события α_r и β_r являются независимыми (и имеют различную природу), поэтому из аксиоматики теории вероятностей получаем, что имеет место равенство

$$\mathrm{P}(\omega_r) = \mathrm{P}(\alpha_r \cap \beta_r) = \mathrm{P}(\alpha_r)\mathrm{P}(\beta_r).$$

Значит, справедливо равенство

$$\mathrm{P}(\omega) = \sum_{r \in Q} \mathrm{P}(\alpha_r)\mathrm{P}(\beta_r).$$

Однако нетрудно заметить, что

$$\mathrm{P}(\alpha_r) = \rho_0(r), \quad \mathrm{P}(\beta_r) = p(x, r, q),$$

что доказывает предложение. □

Пусть на k-м шаге имеем распределение состояний $\rho_k(q)$ и на вход вероятностного автомата поступает сигнал x_{k+1}. Тогда новое распределение получаем аналогично утверждению предложения 2.1:

$$\rho_{k+1}(q) = \sum_{r \in Q} \rho_k(r) p(x_{k+1}, r, q).$$

Отсюда получаем общую формулу для распределения $\rho_k(q)$:

$$\rho_k(q) = \sum_{r_k \in Q} \rho_{k-1}(r_k) p(x_k, r_k, q) = \ldots = \\ = \sum_{r_1, \ldots, r_k \in Q} \rho_0(r_1) p(x_1, r_1, r_2) \ldots p(x_{k-1}, r_{k-1}, r_k) p(x_k, r_k, q).$$

Как можно увидеть из данной формулы, в случае, когда все значения $p(x, q, q')$ известны, любое последующее распределение при сканировании выражается через начальное.

Предложение 2.2. *Распределение выходного сигнала на k-м шаге даётся формулой*

$$p_k(y) = \sum_{q \in Q} \rho_{k-1}(q) p(x_k, q, y).$$

Доказательство. Определим событие ω следующим образом:

$\omega = \{$вероятностный автомат на шаге с номером k при поступлении сигнала x_k выдаёт выходной сигнал $y\}$.

Тогда $p_k(y) = \mathrm{P}(\omega)$. Также определим события

$\omega_s = \{$вероятностный автомат на шаге с номером $k-1$ находился в состоянии s и при получении входного сигнала x_k выдал выходной сигнал $y\}$.

Тогда ясно, что

$$\omega = \bigcup_{s \in Q} \omega_s,$$

поскольку на шаге с номером $k-1$ вероятностный автомат должен был находиться в каком-либо состоянии, и также ясно, что для любых различных $r, s \in Q$ верно равенство

$$\omega_r \cap \omega_s = \varnothing,$$

поскольку вероятностный автомат на шаге с номером $k-1$ не мог находиться в двух различных состояниях одновременно. Значит, согласно аксиоматике теории вероятностей имеет место равенство

$$\mathrm{P}(\omega) = \sum_{s \in Q} \mathrm{P}(\omega_s).$$

Рассмотрим события

$$\alpha_s = \{\text{вероятностный автомат на шаге с номером } k-1 \text{ находился в состоянии } s\},$$

$$\beta_s = \{\text{находясь в состоянии } s \text{ при получении входного сигнала, вероятностный автомат выдал выходной сигнал } y\}.$$

Ясно, что имеет место равенство

$$\omega_s = \alpha_s \cap \beta_s$$

и что события α_s и β_s являются независимыми. Поэтому получаем равенство

$$\mathrm{P}(\omega) = \sum_{s \in Q} \mathrm{P}(\alpha_s)\mathrm{P}(\beta_s).$$

В то же время видно, что

$$\mathrm{P}(\alpha_s) = \rho_{k-1}(s), \quad \mathrm{P}(\beta_s) = p(x_k, q, y).$$

Утверждение предложения доказано. □

Таким образом, имея выходные сигналы $\{y_1, \ldots, y_m\}$, мы можем определить начальное распределение $\rho_0(q)$. В этом и заключается смысл процедуры внутреннего сканирования.

Будем считать все векторы распределения состояний $\rho_0(q), \ldots, \rho_m(q)$ векторами из $\hat{\mathbb{R}}^n$ (записанными в столбец).

Определение 2.3. Пусть $X = \{x_1, \ldots, x_k\}$, $Y = \{y_1, \ldots, y_m\}$, $Q = \{q_1, \ldots, q_n\}$ — множества входных и выходных сигналов и состояний вероятностного автомата соответственно. Для каждого входного сигнала $x_s \in X$ определим матрицы перехода Q_s и выхода Y_s. Матрица Q_s есть прямоугольная матрица размера $n \times n$, элементы которой определены следующим образом: $(Q_s)_{ij} = p(x_s, q_j, q_i)$, $i = \overline{1,n}$, $j = \overline{1,n}$. Матрица Y_s есть прямоугольная матрица размера $m \times n$, элементы которой определены следующим образом: $(Y_s)_{ij} = p(x_s, q_j, y_i)$, $i = \overline{1,m}$, $j = \overline{1,n}$.

Имеет место следующее основное утверждение данного раздела.

Предложение 2.4. *Пусть* $X = \{x_1, \ldots, x_k\}$, $Y = \{y_1, \ldots, y_m\}$, $Q = \{q_1, \ldots, q_n\}$ *— множества входных и выходных сигналов и состояний вероятностного автомата соответственно. Пусть на вход вероятностного автомата подаётся последовательность входных сигналов* $\{x_{i_1}, \ldots, x_{i_s}\}$, *где* $i_1, \ldots, i_s = \overline{1,k}$. *Также пусть* $\rho_0 \in \hat{\mathbb{R}}^n$ *— вектор распределений состояний вероятностного автомата до подачи входной последовательности сигналов* (*вектор начального состояния*). *Пусть* $\rho_s \in \hat{\mathbb{R}}^n$ *— вектор распределений состояний вероятностного автомата после подачи входной последовательности,* $\pi_s \in \hat{\mathbb{R}}^n$ *— вектор распределений выходных сигналов вероятностного автомата. Тогда для данных векторов справедливы следующие выражения, использующие матрицы, введённые в определении* 2.3:

$$\rho_s = \left(\prod_{t=s}^{1} Q_{i_t}\right)\rho_0, \quad \pi_s = \left(Y_{i_s}\prod_{t=s-1}^{1} Q_{i_t}\right)\rho_0.$$

Доказательство. Пусть $\rho_{s-1} \in \hat{\mathbb{R}}^n$ — вектор распределений состояний вероятностного автомата перед поступлением на его вход последнего сигнала x_{i_s}. Тогда согласно предложению 2.2 справедливо равенство

$$(\pi_s)_i = \sum_{j=1}^{n} p(x_{i_s}, q_j, y_i)(\rho_{s-1})_j = \sum_{j=1}^{n} (Y_{i_s})_{ij}(\rho_{s-1})_j$$

для всех $i = \overline{1,m}$, что означает в матричной записи, что $\pi_s = Y_{i_s}\rho_{s-1}$. Согласно предложению 2.1 выполнено также равенство

$$(\rho_s)_i = \sum_{j=1}^{n} p(x_{i_s}, q_j, q_i)(\rho_{s-1})_j = \sum_{j=1}^{n} (Q_{i_s})_{ij}(\rho_{s-1})_j$$

для всех $j = \overline{1,n}$, что означает в матричной записи, что $\rho_s = Q_{i_s}\rho_{s-1}$. Аналогичными рассуждениями показывается, что выполнено равенство $\rho_{s-1} = Q_{i_{s-1}}\rho_{s-2}$, где $\rho_{s-2} \in \hat{\mathbb{R}}^n$ — вектор распределений состояний вероятностного автомата перед поступлением на его вход двух последних входных сигналов. По индукции получаем выражения, приведённые в данном предложении. □

Таким образом, вектор распределения выходных сигналов на любом шаге сканирования является произведением матриц выхода и матриц перехода на начальный вектор распределения состояний. Учитывая, что все матрицы известны, можно утверждать, что процедура сканирования позволяет с некоторой точностью определить вектор начального распределения ρ_0.

Лемма 2.5. *Для любой матрицы* Y_s *все её элементы неотрицательны. Кроме того, справедливо равенство* $\sum\limits_{i=1}^{m} (Y_s)_{ij} = 1$ *при всех* $j = \overline{1,n}$.

Доказательство. По определению вероятностного автомата

$$\sum_{i=1}^{m}(Y_s)_{ij} = \sum_{i=1}^{m} p(x_s, q_j, y_i) = \sum_{i=1}^{m}\sum_{t=1}^{n} p(x_s, q_j, y_i, q_t) = 1.$$ □

Лемма 2.6. *Для любой матрицы Q_s все её элементы неотрицательны. Кроме того, справедливо равенство $\sum\limits_{i=1}^{n}(Q_k)_{ij}=1$ при всех $j=\overline{1,n}$.*

Доказательство. По определению вероятностного автомата

$$\sum_{i=1}^{n}(Q_s)_{ij}=\sum_{i=1}^{n}p(x_s,q_j,q_i)=\sum_{i=1}^{n}\sum_{t=1}^{m}p(x_s,q_j,y_t,q_i)=1. \qquad \square$$

Таким образом, все матрицы Y_s, Q_s принадлежат к одному классу матриц, называемых в данной работе стохастическими (с другим определением стохастических матриц можно ознакомиться в [2, гл. 8, § 6, определение 4]).

3. Предельные свойства стохастических матриц

Определение 3.1. Вектор $v\in\hat{\mathbb{R}}^n$ называется стохастическим, если выполнены следующие условия: $v_i\geqslant 0$ для каждого $i=\overline{1,n}$ и $\sum\limits_{i=1}^{n}v_i=1$.

Определение 3.2. Матрица A называется стохастической, если все её столбцы — стохастические векторы.

В свете введённых определений получаем из лемм 2.5 и 2.6, что матрицы Y_k и Q_k стохастические.

Следующее утверждение относится к математическому фольклору, однако для полноты картины приведём его доказательство.

Лемма 3.3. *Произведение стохастических матриц есть стохастическая матрица.*

Доказательство. Пусть A, B — стохастические матрицы, $C=AB$. Очевидно, что все элементы матрицы C неотрицательны. Возьмём любое $j=\overline{1,n}$. Тогда

$$\sum_{i=1}^{n}c_{ij}=\sum_{i=1}^{n}\Bigg(\sum_{k=1}^{n}a_{ik}b_{kj}\Bigg)=\sum_{k=1}^{n}b_{kj}\sum_{i=1}^{n}a_{ik}=\sum_{k=1}^{n}b_{kj}=1,$$

поскольку матрицы A и B стохастические. $\square$

Лемма 3.4 ([2, гл. 8, § 6, утверждение 1]). *Все значения собственных чисел стохастической матрицы по модулю не превосходят* 1. *Кроме того,* 1 *всегда является собственным значением стохастической матрицы.*

В дальнейших рассуждениях стохастические матрицы рассматриваются над алгебраически замкнутым полем $\mathbb{C}$.

Лемма 3.5. *Пусть A — стохастическая матрица. Тогда её норма* (*см. определение* 1.8) *равна* 1.

Доказательство.

$$\|Av\| = \sum_{i=1}^{n} |(Av)_i| = \sum_{i=1}^{n} \left| \sum_{j=1}^{n} a_{ij} v_j \right| \leqslant$$

$$\leqslant \sum_{i=1}^{n} \sum_{j=1}^{n} |a_{ij} v_j| = \sum_{i=1}^{n} \sum_{j=1}^{n} a_{ij} |v_j| \leqslant \sum_{i=1}^{n} \sum_{j=1}^{n} a_{ij} |v_j|.$$

Далее,

$$\sum_{i=1}^{n} \sum_{j=1}^{n} a_{ij} |v_j| = \sum_{j=1}^{n} |v_j| \sum_{i=1}^{n} a_{ij} = \sum_{j=1}^{n} |v_j| = \|v\|.$$

Значит, имеет место неравенство $\|Av\| \leqslant \|v\|$, т. е. $\|Av\|/\|v\| \leqslant 1$, откуда $\|A\| \leqslant 1$. В то же время согласно лемме 3.4 всегда существует вектор v, для которого неравенство превращается в равенство, что означает, что $\|A\| = 1$ по определению нормы. □

Изучение предельных свойств стохастических матриц связано с исследованиями характера поведения вероятностного автомата (представляющего автоматизированную систему) в том случае, когда на его вход подаются цепочки большой длины. В частности, изучаются вопросы, связанные с предельным распределением состояний вероятностного автомата в том случае, когда его время работы (длина входной цепочки) стремится к бесконечности.

Определение 3.6. Последовательность матриц $\{A_1, \ldots, A_k, \ldots\}$ сходится к матрице B (или матрица B есть предел матричной последовательности $\{A_1, \ldots, A_k, \ldots\}$), если верно утверждение, что для любого $\varepsilon > 0$ найдётся $M \in \mathbb{N}$, такое что при всех $m \in \mathbb{N}$, $m \geqslant M$, справедливо $\|A_m - B\| < \varepsilon$, где под нормой понимается норма, введённая ранее (см. определение 1.8).

Определение 3.7. Пусть A — квадратная $(n \times n)$-матрица. Матрица A имеет степенной предел, если последовательность матриц $\{A^0, A^1, A^2, \ldots, A^m, \ldots\}$ имеет предел.

Следующие утверждения являются широко известными, мы приводим их доказательство для полноты картины.

Лемма 3.8. *Пусть последовательность матриц $\{A_1, \ldots, A_k, \ldots\}$ сходится к матрице B. Тогда эта последовательность, будучи рассмотренной в другом базисе с матрицей перехода C, также сходится, и её предел равен $C^{-1}BC$.*

Доказательство. Пусть $\{B_1, \ldots, B_k, \ldots\}$ — исходная последовательность матриц, записанная в другом базисе. Поскольку справедливы выражения $B_i = C^{-1}A_iC$, получаем оценку

$$\|B_i - C^{-1}BC\| = \|C^{-1}(A_i - B)C\| \leqslant \|C\| \, \|C^{-1}\| \, \|A_i - B\|.$$

Поскольку величина $\|C\| \, \|C^{-1}\|$ является постоянной, получаем утверждение леммы. □

Лемма 3.9. *Пусть для матрицы A верно неравенство $\|A\| < \varepsilon$. Тогда для всех её элементов a_{ij} верно неравенство $|a_{ij}| < \varepsilon$.*

Доказательство. Из $\|A\| < \varepsilon$ следует, что для любого $v \neq 0$ справедливо $\|Av\| < \varepsilon\|v\|$. Возьмём в качестве вектора v базисный вектор e_j. Тогда очевидно, что $\|v\| = 1$, и Av есть j-й столбец матрицы A, норма которого строго меньше ε. Учитывая правило вычисления нормы, получаем, что все компоненты вектора Av по модулю меньше ε. □

Лемма 3.10. *Пусть последовательность стохастических матриц $\{A_1, \ldots, A_k, \ldots\}$ сходится к матрице B. Тогда матрица B также является стохастической* (*т. е. множество стохастических матриц содержит все свои предельные точки*).

Доказательство. В соответствии с определением стохастической матрицы докажем, что все элементы матрицы B неотрицательны и что сумма элементов любого столбца матрицы B равна единице.

Возьмём любые значения $i, j = \overline{1,n}$ и $\varepsilon > 0$. Тогда найдётся такое число M, что при всех $m > M$ выполнено неравенство $\|A_m - B\| < \varepsilon$. Значит, согласно лемме 3.9 справедливо неравенство $|(A_m)_{ij} - b_{ij}| < \varepsilon$. Отсюда получаем, что $b_{ij} > (A_m)_{ij} - \varepsilon \geqslant -\varepsilon$, поскольку матрица A_m является стохастической. Значит, $b_{ij} > -\varepsilon$ для любого $\varepsilon > 0$, откуда следует, что $b_{ij} \geqslant 0$. Первое утверждение доказано.

Как отмечалось выше, для любого $\varepsilon > 0$ найдётся такое число M, что при всех $m > M$ выполнено неравенство $\|A_m - B\| < \varepsilon$, откуда следует, что $|(A_m)_{ij} - b_{ij}| < \varepsilon$ при всех $i, j = \overline{1,n}$. Но тогда

$$
\begin{aligned}
&|(A_m)_{ij} - b_{ij}| < \varepsilon \implies (A_m)_{ij} - \varepsilon < b_{ij} < (A_m)_{ij} + \varepsilon \implies \\
&\implies \sum_{i=1}^{n}((A_m)_{ij} - \varepsilon) < \sum_{i=1}^{n} b_{ij} < \sum_{i=1}^{n}((A_m)_{ij} + \varepsilon) \iff \\
&\iff \sum_{i=1}^{n}(A_m)_{ij} - n\varepsilon < \sum_{i=1}^{n} b_{ij} < \sum_{i=1}^{n}(A_m)_{ij} + n\varepsilon \iff \\
&\iff 1 - n\varepsilon < \sum_{i=1}^{n} b_{ij} < 1 + n\varepsilon \iff \left|\sum_{i=1}^{n} b_{ij} - 1\right| < n\varepsilon,
\end{aligned}
$$

поскольку матрица A_m является стохастической. В силу постоянства величины n и произвольности ε получаем, что сумма элементов любого столбца матрицы B равна 1. Утверждение леммы доказано. □

Сначала напомним, при каких условиях стохастическая матрица имеет степенной предел, т. е. при каких условиях автоматизированная система практически не меняет распределения состояний при повторяющемся входном сигнале.

Теорема 3.11 ([2, гл. 8, § 7, теорема 11]). *Стохастическая матрица имеет степенной предел тогда и только тогда, когда она не имеет собственных чисел, равных по модулю* 1 *и отличных от* 1.

Рассмотрим некоторые семейства стохастических матриц, которые часто встречаются в практике моделирования автоматизированных систем и обладают свойством существования степенного предела.

Определение 3.12. Стохастическая матрица A размера $n \times n$ называется примитивной, если найдётся такая натуральная степень A^m, все элементы которой строго положительны, и слабособственной, если все её собственные значения, кроме одного, по модулю строго меньше единицы.

Доказательство следующего полезного утверждения можно найти в [2]. Данная теорема является частным случаем теоремы Перрона—Фробениуса (см., например, [2, гл. 8, § 2, теорема 2]). Согласно [2, с. 378, гл. 8, § 5, следствие] примитивная матрица неразложима (см. [2, гл. 8, § 1, определение 2]), а потому к ней применима теорема Перрона—Фробениуса.

Теорема 3.13. *Пусть стохастическая матрица A примитивна. Тогда она является слабособственной.*

Из теоремы 3.11 следует, что всякая слабособственная матрица имеет степенной предел. Теорема 3.13 показывает, что всякая примитивная (в частности, положительная) стохастическая матрица также имеет степенной предел.

Эти классы стохастических матриц, как уже было отмечено выше, достаточно часто встречаются на практике в задачах моделирования автоматизированных систем. Однако структура данных классов достаточно сложна, а именно, они не образуют даже полугруппы по умножению.

Замечание 3.14. Существуют примитивные матрицы A и B, такие что их произведение AB не имеет степенного предела.

Доказательство. Рассмотрим матрицы

$$A = \begin{pmatrix} 1/4 & 0 & 1/4 & 1 \\ 1/4 & 0 & 1/4 & 0 \\ 1/4 & 1 & 1/4 & 0 \\ 1/4 & 0 & 1/4 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 1/4 & 0 & 1/4 \\ 1 & 1/4 & 0 & 1/4 \\ 0 & 1/4 & 0 & 1/4 \\ 0 & 1/4 & 1 & 1/4 \end{pmatrix}.$$

Несложно вычислить, что

$$A^2 = \begin{pmatrix} 3/8 & 1/4 & 3/8 & 1/4 \\ 1/8 & 1/4 & 1/8 & 1/4 \\ 3/8 & 1/4 & 3/8 & 1/4 \\ 1/8 & 1/4 & 1/8 & 1/4 \end{pmatrix}, \quad B^2 = \begin{pmatrix} 1/4 & 1/8 & 1/4 & 1/8 \\ 1/4 & 3/8 & 1/4 & 3/8 \\ 1/4 & 1/8 & 1/4 & 1/8 \\ 1/4 & 3/8 & 1/4 & 3/8 \end{pmatrix},$$

$$AB = \begin{pmatrix} 0 & 3/8 & 1 & 3/8 \\ 0 & 1/8 & 0 & 1/8 \\ 1 & 3/8 & 0 & 3/8 \\ 0 & 1/8 & 0 & 1/8 \end{pmatrix}.$$

Из данных выражений видно, что матрицы A и B являются примитивными, поскольку матрицы A^2 и B^2 состоят из строго положительных элементов. Значит, согласно теореме 3.13 существуют степенные пределы матриц A и B.

Нетрудно вычислить характеристический многочлен матрицы AB:

$$\chi_{AB}(t) = t^4 - \frac{t^3}{4} - t^2 + \frac{t}{4} = t\left(t - \frac{1}{4}\right)(t^2 - 1),$$

откуда получаем, что матрица AB имеет собственное значение, равное -1 и, значит, согласно теореме 3.11 не имеет степенного предела. Утверждение доказано. □

Данный пример демонстрирует, что произведение примитивных матриц не всегда является примитивной матрицей, произведение слабособственных матриц не всегда слабособственная матрица и, более того, произведение матриц, имеющих степенные пределы, не всегда имеет степенной предел.

С прикладной точки зрения важен вопрос о положительности элементов степенного предела стохастической матрицы. Заметим для начала, что согласно лемме 3.10 степенной предел стохастической матрицы, если он существует, является стохастической матрицей.

Теорема 3.15 ([2, гл. 8, § 7, теорема 11]). *Матрица B, являющаяся степенным пределом стохастической матрицы A, состоит полностью из строго положительных элементов тогда и только тогда, когда матрица A примитивна.*

Следствие 3.16. *Если стохастическая матрица A имеет степенной предел — матрицу B — и при этом кратность единицы как собственного значения матрицы A строго больше 1, то матрица B обязательно имеет нулевые элементы.*

Доказательство. Действительно, если матрица B строго положительна, то матрица A должна быть примитивной, а значит, и слабособственной (в силу теоремы 3.13), что противоречит условию. Таким образом, матрица B обязательно содержит нулевые элементы. □

Для дальнейших рассуждений и результатов понадобится следующее определение.

Определение 3.17. Для стохастической матрицы A обозначим через $\mathcal{W}(A)$ пространство комплексных векторов v, для которых верно равенство $Av = v$. Пространство $\mathcal{W}(A)$ будем называть пространством неподвижных векторов матрицы A.

Лемма 3.18 ([2, гл. 8, § 6, теорема 10]). *Пусть A — стохастическая матрица, $\lambda = 1$ — её собственное значение. Тогда жорданова нормальная форма матрицы A не может иметь жордановых клеток, соответствующих значению λ, размер которых больше единицы.*

Лемма 3.19. *Пусть для всех элементов матрицы A размера $n \times n$ выполняется неравенство $|a_{ij}| < \varepsilon$. Тогда верно неравенство $\|A\| \leqslant n\varepsilon$.*

Доказательство. Возьмём любой вектор $v \neq 0$ и оценим $|(Av)_i|$:

$$|(Av)_i| = \left|\sum_{j=1}^{n} a_{ij}v_j\right| \leqslant \sum_{j=1}^{n} |a_{ij}v_j| = \sum_{j=1}^{n} |a_{ij}|\,|v_j| < \varepsilon \sum_{j=1}^{n} |v_j| = \varepsilon\|v\|.$$

Тогда

$$\|Av\| = \sum_{i=1}^{n} |(Av)_i| < \sum_{i=1}^{n} \varepsilon\|v\| = n\varepsilon\|v\|,$$

поэтому

$$\frac{\|Av\|}{\|v\|} < n\varepsilon,$$

откуда и получаем утверждение леммы. □

Предложение 3.20 ([2, с. 105—106]). *Пусть $J_k(\lambda)$ — жорданова клетка размера k, соответствующая числу λ, т. е.*

$$J_k(\lambda) = \begin{pmatrix} \lambda & 1 & 0 & \dots & 0 \\ 0 & \lambda & 1 & \dots & 0 \\ \vdots & \ddots & \ddots & \vdots & 1 \\ 0 & 0 & \dots & 0 & \lambda \end{pmatrix}.$$

Тогда матрица $J_k(\lambda)^m$ имеет вид

$$J_k(\lambda)^m = \begin{pmatrix} \lambda^m & C_m^1\lambda^{m-1} & C_m^2\lambda^{m-2} & \dots & C_m^{k-1}\lambda^{m-k+1} \\ 0 & \lambda^m & C_m^1\lambda^{m-1} & \dots & C_m^{k-2}\lambda^{m-k+2} \\ \vdots & \ddots & \ddots & \vdots & C_m^1\lambda^{m-1} \\ 0 & 0 & \dots & 0 & \lambda^m \end{pmatrix}, \tag{1}$$

где C_m^i — биномиальные коэффициенты.

Лемма 3.21. *Пусть $J_k(\lambda)$ — жорданова клетка размера k, соответствующая числу λ, причём $|\lambda| < 1$. Тогда матрица $J_k(\lambda)$ имеет степенной предел, равный нулевой матрице.*

Доказательство. Исходя из представления (1) и учитывая, что из того, что $|\lambda| < 1$, следует, что для всех $m_1 > m_2$ справедливо $|\lambda^{m_1}| < |\lambda^{m_2}|$, получаем, что если $B = J_k(\lambda)^m$, то ни один элемент матрицы B при $m > 2k$ не превосходит $C_m^{k-1}|\lambda^{m-k+1}| < C_m^k|\lambda^{m-k}|$ (ввиду монотонного возрастания по j биномиальных коэффициентов C_m^j при $2j < m$).

Также очевидно, что $C_m^k|\lambda^{m-k}| \to 0$ при $m \to +\infty$, поскольку C_m^k есть многочлен от m степени k, а $|\lambda^{m-k}|$ — степенная функция от m с основанием по модулю строго меньше 1.

Значит, для любого $\varepsilon > 0$ при достаточно больших значениях m модуль каждого элемента матрицы B меньше ε. По лемме 3.19 получаем утверждение леммы. □

Теорема 3.22. *Пусть матрица B есть степенной предел стохастической матрицы A. Пусть $\dim \mathcal{W}(A) = k$. Тогда существуют k стохастических векторов, порождающих пространство $\mathcal{W}$ (т. е. являющихся базисом данного пространства). Более того, эти векторы можно выбрать из числа столбцов матрицы B, при этом остальные столбцы матрицы B являются их линейной комбинацией.*

Доказательство. Пусть $v_1, \ldots, v_k$ — произвольный базис пространства $\mathcal{W}(A)$. Тогда его можно дополнить до жорданова базиса матрицы A в силу леммы 3.18, так как все векторы $v_1, \ldots, v_k$ являются собственными векторами матрицы A. Пусть J — матрица жордановой нормальной формы матрицы A. Тогда для матрицы J справедливо представление

$$J = \begin{pmatrix} I_k & 0 \\ 0 & J_0 \end{pmatrix},$$

где I_k — единичная матрица размера $k \times k$, матрица J_0 есть часть жордановой формы, соответствующей всем собственным числам матрицы A, модули которых строго меньше единицы. Матрица J_0 является блочно-диагональной, при этом согласно лемме 3.21 матрица J_0 имеет степенной предел, равный нулевой матрице. Значит, матрица B, являющаяся степенным пределом матрицы A, в жордановом базисе совпадает со степенным пределом матрицы J, равным

$$\begin{pmatrix} I_k & 0 \\ 0 & 0 \end{pmatrix}.$$

Из данного выражения очевидно следует, что выполнено равенство $B(\mathbb{C}^n) = \mathcal{W}(A)$, т. е. что для любого вектора v верно утверждение $Bv \in \mathcal{W}(A)$, поскольку, как нетрудно видеть, в жордановом базисе матрица B является проектором на пространство $\mathcal{W}(A)$. Очевидно, что данное свойство не зависит от базиса, поэтому в исходном базисе это утверждение также справедливо.

Если в качестве вектора v выбрать базисный вектор (в исходном базисе) e_j, то Be_j есть j-й столбец матрицы B. Поскольку $Be_j \in \mathcal{W}(A)$, получаем, что все столбцы матрицы B принадлежат множеству $\mathcal{W}(A)$. В то же время, поскольку $rkB = k$ (при замене базиса ранг матрицы не меняется, а в жордановом базисе это очевидно), среди столбцов матрицы B найдутся k линейно независимых, а остальные столбцы являются их линейными комбинациями. Учитывая, что $\dim \mathcal{W}(A) = k$, получаем, что эти столбцы являются базисом в пространстве $\mathcal{W}(A)$, что окончательно доказывает теорему. □

Из данной теоремы получаем очевидное следствие.

Следствие 3.23. *Если матрица A является слабособственной, то все столбцы её степенного предела равны единственному собственному стохастическому вектору.*

Полученный в теореме 3.22 результат позволяет определять, когда степенной предел стохастической матрицы содержит нулевые строки. Справедливо следующее утверждение.

Теорема 3.24. *Пусть стохастическая матрица A имеет в качестве степенного предела матрицу B. Тогда матрица B имеет нулевые строки с номерами $i_1, \ldots, i_s$ тогда и только тогда, когда у всех векторов пространства $\mathcal{W}(A)$ компоненты с номерами $i_1, \ldots, i_s$ равны нулю.*

Доказательство. Пусть матрица B имеет нулевые строки с номерами $i_1, \ldots, i_s$. По теореме 3.22 среди столбцов матрицы B можно выбрать базис

пространства $\mathcal{W}(A)$. Тогда очевидно, что у всех столбцов матрицы B, составляющих данный базис, компоненты с номерами $i_1, \ldots, i_s$ нулевые. Далее, поскольку любой вектор пространства $\mathcal{W}(A)$ является линейной комбинацией векторов базиса, для любого вектора пространства $\mathcal{W}(A)$ компоненты с номерами $i_1, \ldots, i_s$ равны нулю.

Пусть любой вектор пространства $\mathcal{W}(A)$ имеет нулевые компоненты с номерами $i_1, \ldots, i_s$. Тогда нулевые компоненты с этими же номерами будут иметь и столбцы матрицы B, являющиеся базисом пространства $\mathcal{W}(A)$. Поскольку остальные столбцы матрицы B линейно выражаются через базисные столбцы, получаем, что у всех столбцов матрицы B компоненты с номерами $i_1, \ldots, i_s$ нулевые, что и означает, что строки с данными номерами являются нулевыми.

Теорема доказана. □

Из наличия нулевой строки у степенного предела стохастической матрицы следует тот факт, что при любом начальном распределении состояний вероятностного автомата при достаточно долгой подаче одного и того же сигнала вероятность перехода в состояние, соответствующее нулевой строке, равна нулю, т. е. переходов в данное состояние практически не происходит. На самом деле верно и обратное утверждение.

Лемма 3.25. *Пусть стохастическая матрица A имеет степенной предел, равный матрице B. Пусть, кроме того, для любого стохастического вектора v вектор Bv имеет нулевые компоненты с номерами $i_1, \ldots, i_s$. Тогда матрица B имеет нулевые строки с теми же номерами.*

Доказательство. Утверждение леммы становится очевидным, если в качестве вектора v последовательно подставлять базисные векторы $e_1, \ldots, e_n$ и учитывать тот факт, что Be_j есть j-й столбец матрицы B. Таким образом получим, что все столбцы имеют нулевые компоненты с номерами $i_1, \ldots, i_s$, что эквивалентно тому, что матрица B имеет нулевые строки с номерами $i_1, \ldots, i_s$. □

Лемма 3.26. *Пусть стохастическая матрица A имеет степенной предел, равный матрице B. Пусть, кроме того, существует стохастический вектор v, такой что вектор Bv имеет нулевые компоненты с номерами $i_1, \ldots, i_s$. Тогда существует стохастический вектор, принадлежащий пространству $\mathcal{W}(A)$, который имеет нулевые компоненты с теми же номерами.*

Доказательство. Поскольку матрица B является стохастической (ввиду леммы 3.10), она переводит вектор v в некий стохастический вектор, принадлежащий пространству $\mathcal{W}(A)$ (это следует из доказательства теоремы 3.22). Утверждение доказано. □

Из условия, что существует собственный вектор матрицы A, имеющий нулевые координаты, следуют некоторые важные свойства матрицы, а именно справедливо следующее утверждение.

Теорема 3.27. *Пусть стохастическая матрица A является матрицей перехода (преобразования распределения состояний) вероятностного автомата с конечным множеством состояний $Q = \{q_1, \ldots, q_n\}$. Пусть также данная матрица имеет собственный стохастический вектор $v \in \mathcal{W}(A)$. Кроме того, пусть координаты вектора v с номерами $i_1, \ldots, i_s$ равны нулю, остальные координаты строго положительны. Пусть множества $Q_2 \in Q$ и $Q_1 \in Q$ определены равенствами $Q_2 = \{q_{i_1}, \ldots, q_{i_s}\}$, $Q_1 = Q \setminus Q_2$. Тогда вероятности перехода из любого состояния множества Q_1 в любое состояние множества Q_2 равны нулю, т. е. $p(\rho_1, \rho_2) = 0$ для всех $\rho_1 \in Q_1$, $\rho_2 \in Q_2$.*

Доказательство. Произведём перестановку векторов базиса таким образом, чтобы все нулевые элементы вектора v были расположены в конце, т. е. $v_{n-s+1} = \ldots = v_n = 0$ и $v_j > 0$ для всех $j = \overline{1, n-s}$. Данная перестановка фактически означает перенумерование элементов множества Q. В новом базисе множества Q_1 и Q_2 будут иметь вид $Q_1 = \{q_1, \ldots, q_{n-s}\}$, $Q_2 = \{q_{n-s+1}, \ldots, q_n\}$.

Будем рассматривать матрицу A в новом базисе. Очевидно, что она осталась стохастической. Тогда, если записать условие $Av = v$ в новом базисе покоординатно, для последних координат получим равенства

$$\sum_{k=1}^{n} a_{kj} v_j = v_k = 0, \quad k = \overline{n-s+1, n},$$

откуда, учитывая равенства $v_{n-s+1} = \ldots = v_n = 0$, получим

$$\sum_{k=1}^{n-s} a_{kj} v_j = 0, \quad k = \overline{n-s+1, n}.$$

Но поскольку $v_j > 0$ для всех $j = \overline{1, n-s}$, получаем, что данное равенство возможно только при выполнении условия $a_{kj} = 0$ для всех $k = \overline{n-s+1, n}$, $j = \overline{1, n-s}$.

Поскольку для матрицы перехода вероятностного автомата значение элемента a_{ij} есть вероятность перехода из состояния с номером j в состояние с номером i, получаем, что все вероятности перехода из состояний $\{q_1, \ldots, q_{n-s}\} = Q_1$ в состояния $\{q_{n-s+1}, \ldots, q_n\} = Q_2$ равны нулю, что и требовалось доказать. □

Данная теорема полезна в приложениях. Если множество Q_2 есть множество состояний автоматизированной системы, в которых уровень защищённости системы не является приемлемым («опасные состояния»), а множество Q_1 — множество «безопасных состояний», то из того, что для некоторого вектора начального распределения состояний в случае подачи одного и того же сигнала получаем такое распределение, в котором вероятность нахождения в опасных состояниях равна нулю, следует, что изначально автоматизированная система при подаче данного сигнала имеет нулевую вероятность перехода из безопасных состояний в опасные.

Таким образом, если в пределе система не переходит в опасные состояния, то она не переходит в них ни на каком шаге.

Как нетрудно видеть из доказательства данной теоремы, верно и обратное утверждение, т. е. если система не переходит из безопасных состояний в опасные, то это же утверждение имеет силу и в пределе.

Перейдём теперь к вопросу исследования предельных свойств некоторого специального семейства стохастических матриц. Интерес к данному вопросу связан с попыткой оценки предельного распределения состояний автоматизированной системы при подаче на вход различных последовательностей входных сигналов.

Пусть $\{A_1, \ldots, A_s\}$ — множество стохастических матриц размера $n \times n$. Пусть также задана бесконечная последовательность $I = \{i_1, i_2, \ldots\}$ элементов множества $\{1, \ldots, s\}$. Поставим в соответствие данной последовательности последовательность $\Pi(I) = \{\pi_1, \pi_2, \ldots\}$ матричных произведений семейства $\{A_1, \ldots, A_s\}$ по следующему правилу:

$$\pi_1 = A_{i_1}, \quad \pi_{k+1} = A_{i_{k+1}} \pi_k.$$

Рассмотрение данной последовательности произведений полностью соответствует формулам преобразования распределений состояний вероятностного автомата (предложение 2.4). Фактически π_k есть матрица перехода вероятностного автомата при поступлении на вход последовательности сигналов $i_1, \ldots, i_k$.

Зададимся вопросом о сходимости последовательности $\Pi(I)$.

Определение 3.28.

1. Последовательность $\Pi(I)$ сохраняет пространство неподвижных векторов, если для любых элементов этой последовательности их пространства неподвижных векторов совпадают, т. е. выполнено равенство

   $$\mathcal{W}(\pi_1) = \ldots = \mathcal{W}(\pi_m) = \ldots.$$

   Обозначим в этом случае $\mathcal{W}(\pi_1)$ через $\mathcal{W}(\Pi(I))$.
2. Для произвольной заданной последовательности I и произвольного натурального m определим последовательность I_m (сдвиг) как фрагмент последовательности I, начинающийся с номера m, т. е. $I_m = \{i_m, i_{m+1}, \ldots\}$, или же формально $(I_m)_k = i_{m+k-1}$. Последовательность $\Pi(I)$ равномерно сохраняет пространство неподвижных векторов, если для любого натурального m последовательность $\Pi(I_m)$ сохраняет пространство неподвижных векторов, причём все пространства $\mathcal{W}(\Pi(I_m))$ совпадают.

Вопрос о наличии предела последовательности $\Pi(I)$ не является тривиальным, о чем свидетельствуют следующие предложения.

Предложение 3.29. *Существуют такие стохастические матрицы* $\{A_1, \ldots, A_s\}$ *и последовательность* I*, что выполнено равенство*

$$\mathcal{W}(A_1) = \ldots = \mathcal{W}(A_s),$$

при этом последовательность $\Pi(I)$ *не сохраняет пространства неподвижных векторов и не имеет предела.*

Доказательство. Пусть

$$A_1 = \begin{pmatrix} 1 & 0 & 0 & 0{,}2 & 0{,}36 \\ 0 & 0{,}1 & 0{,}66 & 0{,}09 & 0{,}28 \\ 0 & 0 & 0 & 0{,}21 & 0{,}18 \\ 0 & 0{,}9 & 0{,}34 & 0{,}33 & 0{,}08 \\ 0 & 0 & 0 & 0{,}17 & 0{,}1 \end{pmatrix}, \quad A_2 = \begin{pmatrix} 1 & 0 & 0{,}17 & 0 & 0{,}24 \\ 0 & 0{,}07 & 0{,}01 & 0{,}45 & 0{,}2 \\ 0 & 0{,}93 & 0{,}02 & 0{,}55 & 0{,}2 \\ 0 & 0 & 0{,}03 & 0 & 0{,}3 \\ 0 & 0 & 0{,}77 & 0 & 0{,}06. \end{pmatrix}$$

Тогда с помощью систем компьютерной алгебры несложно вычислить, что $\mathcal{W}(A_1) = \mathcal{W}(A_2) = \langle(1,0,0,0,0)\rangle$. При этом матрица A_1A_2 имеет 1 в качестве двухкратного собственного значения и $\mathcal{W}(A_1) \subset \mathcal{W}(A_1A_2)$, т. е. после умножения произошло расширение подпространства неподвижных векторов. С помощью тех же систем можно убедиться, что матрица A_1A_2 имеет степенной предел. Обозначим его через S.

Пусть последовательность I определена следующим образом: $I = \{2,1,2,1,\ldots\}$. Очевидно, что если последовательность $\Pi(I)$ имеет предел, то он равен S, поскольку $\pi_{2m} = (A_1A_2)^m$. Также очевидно, что $\pi_{2m+1} = A_2(A_1A_2)^m$.

С помощью систем компьютерной алгебры, используя представление матрицы A_1A_2 в жордановой нормальной форме, несложно вычислить матрицу S и убедиться, что $A_2S \neq S$, что свидетельствует о том, что последовательность $\Pi(I)$ не имеет предела. □

Предложение 3.30. *Существуют такие стохастические матрицы* $\{A_1,\ldots,A_s\}$ *и последовательность* I*, что последовательность* $\Pi(I)$ *сохраняет пространство неподвижных векторов, но не сохраняет его равномерно. При этом она не имеет предела.*

Доказательство. Пусть

$$A_1 = \begin{pmatrix} 1 & 1/2 & 1/2 \\ 0 & 1/2 & 0 \\ 0 & 0 & 1/2 \end{pmatrix}, \quad A_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

Последовательность I определена следующим образом: $I = \{1,2,2,2,\ldots\}$, т. е. для элемента π_m выполнено равенство $\pi_m = A_2^{m-1}A_1$. Нетрудно видеть, что $A_2^2 = I_3$ — единичная матрица. Используя это наблюдение, мы можем существенно упростить выражение для элементов π_m, а именно

$$\pi_m = \begin{cases} A_2A_1, & \text{если } m \text{ чётно}, \\ A_1, & \text{если } m \text{ нечётно}. \end{cases}$$

Также несложно вычислить, что

$$B = A_2A_1 = \begin{pmatrix} 1 & 1/2 & 1/2 \\ 0 & 0 & 1/2 \\ 0 & 1/2 & 0 \end{pmatrix} \neq A_1,$$

откуда ясно, что последовательность $\Pi(I)$ не имеет предела.

В то же время несложно показать, что $\mathcal{W}(A_1) = \mathcal{W}(A_2A_1) = \langle(1,0,0)\rangle$, т. е. последовательность $\Pi(I)$ сохраняет пространство неподвижных векторов. Рассмотрим теперь последовательность $I_2 = \{2,2,2,\ldots\}$. Пусть $\Sigma = \Pi(I_2)$. Очевидно, что

$$\sigma_m = A_2^m = \begin{cases} A_2, & \text{если } m \text{ нечётно,} \\ I_3, & \text{если } m \text{ чётно.} \end{cases}$$

Мы видим, что последовательность $\Pi(I_2)$ не сохраняет пространства неподвижных векторов ($\mathcal{W}(\sigma_{2m+1}) = \langle(1,0,0)\rangle$, $\mathcal{W}(\sigma_{2m}) = \langle(1,0,0),(0,1,0),(0,0,1)\rangle$), а значит, исходная последовательность $\Pi(I)$ не сохраняет пространства неподвижных векторов равномерно. □

Перейдём теперь к выяснению условий, при которых последовательность $\Pi(I)$ будет иметь предел. Мы сформулируем достаточное условие сходимости.

Предварительно докажем несколько вспомогательных утверждений.

Лемма 3.31. *Пусть в пространстве $\mathbb{C}^n$ задан стандартный базис $\{e_1,\ldots,e_n\}$, т. е. базис, для координат векторов которого справедливо равенство $(e_i)_j = \delta_{ij}$, где δ_{ij} — символ Кронекера. Пусть $\{v_1,\ldots,v_k\}$ — система линейно независимых векторов. Тогда существуют такие различные базисные векторы $e_{i_1},\ldots,e_{i_{n-k}}$, что система $\{v_1,\ldots,v_k,e_{i_1},\ldots,e_{i_{n-k}}\}$ будет являться базисом в пространстве $\mathbb{C}^n$.*

Доказательство. Будем строить последовательность линейных пространств $V_1, V_2, \ldots, V_{n-k}$ следующим образом. Пусть $V_1 = \langle v_1,\ldots,v_k\rangle$. Поскольку по условию векторы $\{v_1,\ldots,v_k\}$ линейно независимы, то $\dim V_1 = k$. Также ясно, что $\dim\langle v_1,\ldots,v_k,e_1,\ldots,e_n\rangle = n$, поскольку $\{e_1,\ldots,e_n\}$ есть базис в $\mathbb{C}^n$. Каждое следующее векторное пространство получается из предыдущего путём добавления очередного базисного вектора e_i таким образом, что новая система обладает размерностью на единицу больше, чем предыдущая. Если на очередном шаге построить новое подпространство V_{l+1} не удалось, это означает, что все базисные векторы, которые не вошли в пространство V_l, т. е. не были добавлены на предыдущих шагах, линейно выражаются через векторы пространства V_l, откуда получаем, что $\dim\langle v_1,\ldots,v_k,e_1,\ldots,e_n\rangle = \dim V_l < n$. Полученное противоречие доказывает лемму. □

Определение 3.32. Пусть матрица A размера $n \times n$ обладает следующим свойством: для всех элементов матрицы справедливы неравенства $a_{ij} \geqslant 0$ и для всех $j = \overline{1,n}$ верны неравенства

$$0 < \sum_{i=1}^{n} a_{ij} \leqslant \gamma < 1.$$

Назовём такую матрицу слабостохастической.

Определим следующее характеристическое свойство слабостохастической матрицы.

Определение 3.33. Пусть матрица A размера $n \times n$ является слабостохастической. Определим число $\rho(A)$ следующим образом:

$$\rho(A) = \max_{j=\overline{1,n}} \sum_{i=1}^{n} a_{ij} < 1.$$

Лемма 3.34. *Пусть матрица A является слабостохастической. Тогда справедливо соотношение $\|A\| \leqslant \rho(A) < 1$.*

Доказательство. Для любого вектора v

$$\|Av\| = \sum_{i=1}^{n} |(Av)_i| = \sum_{i=1}^{n} \left| \sum_{j=1}^{n} a_{ij} v_j \right| \leqslant \sum_{i=1}^{n} \sum_{j=1}^{n} |a_{ij} v_j| = \sum_{i=1}^{n} \sum_{j=1}^{n} a_{ij} |v_j| \leqslant$$
$$\leqslant \sum_{i=1}^{n} \sum_{j=1}^{n} a_{ij} |v_j| = \sum_{j=1}^{n} |v_j| \sum_{i=1}^{n} a_{ij} \leqslant \rho(A) \sum_{j=1}^{n} |v_j| = \rho(A) \|v\|.$$

Значит, имеет место неравенство $\|Av\| \leqslant \rho(A)\|v\|$, т. е. $\|Av\|/\|v\| \leqslant \rho(A)$, поэтому $\|A\| \leqslant \rho(A)$. □

Определение 3.35. Пусть матрица A размера $r \times r$ удовлетворяет условиям $0 \leqslant a_{ij} \leqslant 1$ и для всех $j = \overline{1,r}$ верны неравенства $0 < \sum\limits_{i=1}^{r} a_{ij} \leqslant 1$. Назовём такую матрицу квазистохастической. (Очевидно, что если выполняются строгие равенства, то матрица является стохастической, если же строгие неравенства, то слабостохастической.)

Предложение 3.36. *Произведение квазистохастических матриц является квазистохастической матрицей.*

Доказательство. Пусть A, B — квазистохастические матрицы, $C = AB$. Очевидно, что все элементы матрицы C неотрицательны. Возьмём любое $j = \overline{1,n}$. Тогда

$$\sum_{i=1}^{n} c_{ij} = \sum_{i=1}^{n} \left(\sum_{k=1}^{n} a_{ik} b_{kj} \right) = \sum_{k=1}^{n} b_{kj} \sum_{i=1}^{n} a_{ik} \leqslant \sum_{k=1}^{n} b_{kj} \leqslant 1,$$

поскольку матрицы A и B квазистохастические. □

Лемма 3.37. *Пусть матрица A размера $r \times r$ является квазистохастической, но не является стохастической. Пусть также v — стохастический вектор длины r. Тогда если вектор Av также является стохастическим, то он обязательно содержит нулевые элементы, причём если m-я координата вектора v строго положительна, то сумма элементов m-го столбца матрицы A строго равна 1.*

Доказательство. Для любого $i = \overline{1,r}$ выполнено $(Av)_i = \sum\limits_{j=1}^{r} a_{ij} v_j$, откуда

$$\|Av\| = \sum_{i=1}^{r} (Av)_i = \sum_{i=1}^{r} \sum_{j=1}^{r} a_{ij} v_j = \sum_{j=1}^{r} v_j \left(\sum_{i=1}^{r} a_{ij} \right) \leqslant \sum_{j=1}^{r} v_j = 1.$$

Из данного неравенства видно, что если $v_j \neq 0$, то обязательно должно выполняться условие $\sum\limits_{i=1}^{r} a_{ij} = 1$, откуда следует, что если j-я координата вектора v строго положительна, то сумма элементов j-го столбца матрицы A строго равна 1. При этом если все координаты вектора v положительны, то сумма элементов в каждом столбце матрицы A равна 1, т. е. матрица A является стохастической, что противоречит условию леммы.

Таким образом, оба утверждения леммы доказаны, что и требовалось. □

Из доказательства леммы получаем, что квазистохастическая матрица не увеличивает норму вектора, при этом строго положительный стохастический вектор она обязательно переводит в положительный вектор с нормой строго меньше 1.

Следующее утверждение важно для последующих рассуждений.

Лемма 3.38. *Пусть матрица A размера $r \times r$ является квазистохастической. Пусть также вектор v является стохастическим, при этом координаты вектора $i_1, \ldots, i_m$ равны нулю, остальные координаты строго положительны. Пусть также вектор Av является стохастическим, при этом для него верны те же свойства, т. е. координаты $i_1, \ldots, i_m$ вектора Av равны нулю, остальные координаты строго положительны. Тогда единица является собственным значением матрицы A.*

Доказательство. Пусть $J = \{j_1, \ldots, j_t\} = \{1, \ldots, r\} \setminus \{i_1, \ldots, i_m\}$ — множество индексов, соответствующих положительным координатам векторов v и Av. По лемме 3.37 сумма координат столбцов матрицы A с номерами из множества J равна 1, при этом, если учесть сохранение нулевых элементов, все элементы этих столбцов в строках с номерами из множества $\{i_1, \ldots, i_m\}$ равны нулю. Действительно,

$$(Av)_{i_k} = \sum_{j=1}^{r} a_{i_k j} v_j = \sum_{j \in J} a_{i_k j} v_j = 0$$

тогда и только тогда, когда $a_{i_k j} = 0$ для всех $j \in J$, поскольку $v_j > 0$ для всех $j \in J$.

Далее рассмотрим характеристическую матрицу $B = A - \lambda E$. Пусть C — матрица, полученная из элементов пересечения строк и столбцов с номерами из множества J (главный минор матрицы B).

Тогда, как нетрудно видеть из доказанного выше, на диагонали матрицы C стоят элементы вида $a_{j_s j_s} - \lambda$, при этом матрица $C + \lambda E$ является стохастической, т. е. матрица C представляет собой характеристическую матрицу некоторой стохастической матрицы размера $|J| \times |J|$. Поскольку единица всегда является собственным числом стохастической матрицы (лемма 3.4), при $\lambda = 1$ столбцы матрицы C линейно зависимы. Поскольку все компоненты столбцов с номерами из множества J, не входящие в матрицу C, равны нулю, отсюда получаем, что и соответствующие столбцы полной матрицы B линейно зависимы с теми

же коэффициентами, что и соответствующие столбцы матрицы C. Значит, при $\lambda = 1$ матрица B является вырожденной, что означает, что единица является собственным значением матрицы A. Лемма доказана. □

Лемма 3.39. *Пусть $\{L_1, \dots, L_s\}$ — семейство квазистохастических матриц размера $r \times r$, обладающих следующим свойством. Пусть $\{i_1, \dots, i_m, \dots\}$ — произвольная бесконечная последовательность номеров, $i_m = \overline{1, r}$. Пусть единица не является собственным числом матрицы $L_{i_{m+s}} L_{i_{m+s-1}} \dots L_{i_m}$ для всех натуральных m, s. Тогда существует некоторое число $M_0 \in \mathbb{N}$, зависящее исключительно от числа r, такое что матрица $L_{i_{M_0}} L_{i_{M_0-1}} \dots L_{i_1}$ «длины» M_0 является слабостохастической. В качестве значения M_0 всегда можно взять число $M_0 = 2^r - 1$.*

Доказательство. Поскольку единица не является собственным числом матриц $L_{i_{m+s}} L_{i_{m+s-1}} \dots L_{i_m}$, в силу леммы 3.4 данные матрицы не могут являться стохастическими.

Возьмём в качестве вектора v произвольный стандартный базисный вектор. Пусть Σ — множество всех собственных подмножеств множества $\{1, \dots, r\}$. Тогда ясно, что $|\Sigma| = 2^r - 2$. Рассмотрим последовательность матричных произведений L_{i_1}, $L_{i_2} L_{i_1}$, $L_{i_3} L_{i_2} L_{i_1}, \dots$ и будем рассматривать образ вектора v при действии матрицами этой последовательности. По лемме 3.37, если на определённом шаге мы получим вектор с нормой строго меньше единицы, на всех последующих шагах будем получать вектор с нормой строго меньше единицы. В частности, если получаем нулевой вектор, то все следующие его образы также будут нулевыми. Поэтому можем считать, что на каждом шаге мы получаем вектор с хотя бы одной нулевой координатой.

Поставим каждой подпоследовательности $\{i_1, i_2, \dots, i_m\}$ в соответствие элемент $\sigma \in \Sigma$ таким образом, что множество σ есть множество номеров нулевых координат вектора $(L_{i_m} \dots L_{i_1})v$. Очевидно, что если длина последовательности больше мощности множества Σ, то мы получим две последовательности, имеющие одинаковый образ при данном соответствии, т. е. пусть последовательностям $\{i_1, i_2, \dots, i_{m_1}\}$ и $\{i_1, i_2, \dots, i_{m_2}\}$, где $m_1 < m_2$, соответствует одно множество нулевых компонент образа вектора v. Тогда вектор $u = (L_{i_{m_1}} \dots L_{i_1})v$ является стохастическим (иначе его норма была бы уже меньше 1 и можно было бы прекратить построение). Пусть матрица B определена равенством $B = L_{i_{m_2}} \dots L_{i_{m_1+1}}$. Матрица B является квазистохастической. При этом вектор Bu имеет те же номера нулевых координат, что и вектор u. Значит, по лемме 3.38 матрица B имеет собственное значение, равное единице, что противоречит условию леммы. Таким образом, любая последовательность с длиной не более мощности множества Σ переводит вектор v в вектор, содержащий строго положительные компоненты. Но тогда следующий образ этого вектора (после умножения на очередную матрицу) по лемме 3.37 имеет норму строго меньше единицы.

Поскольку $|\Sigma| = 2^r - 2$, то в качестве значения M_0 можно взять значение $|\Sigma| + 1 = 2^r - 1$. Если в качестве вектора v последовательно перебрать все базисные векторы, то мы получим, что все столбцы матрицы $L_{i_{M_0}} L_{i_{M_0-1}} \dots L_{i_1}$

имеют норму строго меньше 1, т. е. эта матрица является слабостохастической, что и требовалось доказать. □

Перейдём теперь к формулировке и доказательству достаточного условия существования предела.

Теорема 3.40. *Пусть $\{A_1, \ldots, A_s\}$ — множество стохастических матриц размера $n \times n$. Пусть также определена бесконечная последовательность $I = \{i_1, \ldots, i_m, \ldots\}$, $i_m = \overline{1, s}$. Пусть последовательность $\Pi(I)$ равномерно сохраняет пространство неподвижных векторов $\mathcal{W}$. Тогда последовательность $\Pi(I)$ сходится и для её предела C_I справедливо равенство $C_I(\mathbb{C}^n) = \mathcal{W} = C_I(\mathcal{W})$.*

Доказательство. Пусть $\dim \mathcal{W} = k$. По лемме 3.31 можно выбрать в пространстве $\mathbb{C}^n$ базис таким образом, чтобы первые k векторов нового базиса были образующими векторами пространства $\mathcal{W}$, а остальные векторы являлись подмножеством стандартного базиса в пространстве $\mathbb{C}^n$, в котором и записаны матрицы $\{A_1, \ldots, A_s\}$. Из леммы 3.8 следует, что последовательность $\Pi(I)$ имеет предел в старом базисе тогда и только тогда, когда она имеет предел в новом базисе. Так что без ограничения общности будем считать, что матрицы $\{A_1, \ldots, A_s\}$ уже рассматриваются в новом базисе.

Значит, справедливо блочно-матричное представление

$$\pi_1 = A_{i_1} = \begin{pmatrix} I_k & * \\ 0 & * \end{pmatrix},$$

где I_k — единичная матрица размера $k \times k$. Пусть

$$A_{i_2} = \begin{pmatrix} P & * \\ Q & * \end{pmatrix},$$

где P — матрица размера $k \times k$, Q — матрица размера $k \times (n-k)$ соответственно. Тогда для элемента $\pi_2 = A_{i_2} A_{i_1}$ справедливо символьное равенство

$$\pi_2 = A_{i_2} A_{i_1} = \begin{pmatrix} P & * \\ Q & * \end{pmatrix},$$

где звёздочками отмечены несущественные для текущих рассуждений элементы матриц. Поскольку последовательность $\Pi(I)$ равномерно сохраняет пространство неподвижных векторов, то $\mathcal{W}(\pi_2) = \mathcal{W}(\pi_1)$, откуда немедленно следует, что выполнены равенства $P = I_k$, $Q = 0$. Продолжая данные рассуждения, мы получим, что любая матрица A_j имеет вид

$$A_j = \begin{pmatrix} I_k & H_j \\ 0 & L_j \end{pmatrix},$$

где H_j и L_j — матрицы размеров $(n-k) \times k$ и $(n-k) \times (n-k)$ соответственно, причём матрица

$$\begin{pmatrix} H_j \\ L_j \end{pmatrix}$$

является стохастической и совпадает с частью исходной матрицы A_j. Аналогичный блочный вид имеют и все матрицы π_m.

Рассмотрим множество матриц $\{L_1, \ldots, L_s\}$. Покажем, что данное множество и любой сдвиг I_m начальной последовательности I (определённый в 3.28) удовлетворяет условиям леммы 3.39.

Действительно, если матрица $L_{i_{m+s}} L_{i_{m+s-1}} \ldots L_{i_m}$ имеет собственное число, равное единице, то матрица $A_{i_{m+s}} \ldots A_{i_m}$ имеет дополнительный к пространству $\mathcal{W}$ собственный вектор, поскольку очевидно, что имеет место символическое представление

$$A_{i_{m+s}} \ldots A_{i_m} = \begin{pmatrix} I_k & * \\ 0 & L_{i_{m+s}} \ldots L_{i_m} \end{pmatrix}.$$

Поэтому если 1 является собственным значением матрицы $L_{i_{m+s}} L_{i_{m+s-1}} \ldots L_{i_m}$, то 1 является собственным значением кратности $k+1$ матрицы $A_{i_{m+s}} \ldots A_{i_m}$ (по правилам вычисления определителя матрицы с углом нулей), т. е. $\dim \mathcal{W}(A_{i_{m+s}} \ldots A_{i_m}) = k+1$ в силу леммы 3.18. Это противоречит условию равномерного сохранения пространства неподвижных векторов для сдвига I_m.

Значит, по лемме 3.39 существует число M_0, зависящее только от размера матриц $L_1, \ldots, L_s$, такое что для любой последовательности длины M_0 матрица $L_{i_{m+M_0-1}} \ldots L_{i_m}$ является слабостохастической для всех натуральных m.

Пусть Σ — множество всевозможных произведений матриц $L_{i_{m+M_0-1}} \ldots L_{i_m}$ длины M_0 при всех значениях m. Тогда, как было показано выше, любой элемент множества Σ является слабостохастической матрицей. Поскольку множество Σ конечно (число элементов в нём, очевидно, не превосходит общего числа всевозможных произведений матриц семейства $\{L_1, \ldots, L_s\}$ длины M_0), определим постоянную γ следующим образом: $\gamma = \max\limits_{A \in \Sigma} \rho(A)$. Очевидно, в силу свойств слабостохастических матриц и конечности множества Σ, что имеет место неравенство $\gamma < 1$. Кроме того, в силу леммы 3.34 $\rho(A) \leqslant \gamma$ для любого элемента $A \in \Sigma$, откуда следует, что $\|A\| \leqslant \gamma$ для любого элемента $A \in \Sigma$.

Возьмём теперь любое $0 < \varepsilon < 1$. Тогда найдётся такое натуральное число t, что верно неравенство $\gamma^t < \varepsilon$. Пусть $N_0 = tM_0$.

Рассмотрим любую последовательность матриц $L_{i_{m+N_0-1}} \ldots L_{i_m}$ длины N_0 и оценим её норму:

$$\begin{aligned}
&\|L_{i_{m+N_0-1}} \ldots L_{i_m}\| = \\
&\quad = \|(L_{i_{m+tM_0-1}} \ldots L_{i_{m+(t-1)M_0}}) \times \\
&\quad \times (L_{i_{m+(t-1)M_0-1}} \ldots L_{i_{m+(t-2)M_0}}) \ldots (L_{i_{m+M_0-1}} \ldots L_{i_m})\| \leqslant \\
&\quad \leqslant \|L_{i_{m+tM_0-1}} \ldots L_{i_{m+(t-1)M_0}}\| \times \\
&\quad \times \|L_{i_{m+(t-1)M_0-1}} \ldots L_{i_{m+(t-2)M_0}}\| \ldots \|L_{i_{m+M_0-1}} \ldots L_{i_m}\| \leqslant \\
&\quad \leqslant \underbrace{\gamma \ldots \gamma}_{t} = \gamma^t < \varepsilon,
\end{aligned}$$

поскольку все матрицы, заключённые в скобки, являются слабостохастическими, а также ввиду свойств нормы из замечания 1.9. Это означает, что последовательность матричных произведений $\{L_{i_1}, L_{i_2}L_{i_1}, L_{i_3}L_{i_2}L_{i_1}, \ldots\}$ сходится к нулевой матрице.

Более того, справедливо следующее более сильное утверждение. Для произведения матриц длины m, $pN_0 \leqslant m < (p+1)N_0$, $p \in \mathbb{N}$, верно неравенство $\|L_{i_m} \ldots L_{i_1}\| < \varepsilon^p$. Действительно,

$$\begin{aligned}\|L_{i_m} \ldots L_{i_1}\| &= \\ &= \|(L_{i_m} \ldots L_{i_{pN_0+1}})(L_{i_{pN_0}} \ldots L_{i_{(p-1)N_0+1}}) \ldots (L_{i_{N_0}} \ldots L_{i_1}))\| \leqslant \\ &\leqslant \|L_{i_m} \ldots L_{i_{pN_0+1}}\| \, \|L_{i_{pN_0}} \ldots L_{i_{(p-1)N_0+1}}\| \ldots \|L_{i_{N_0}} \ldots L_{i_1}\| \leqslant \\ &\leqslant 1 \cdot \varepsilon \cdot \ldots \cdot \varepsilon = \varepsilon^p.\end{aligned}$$

Рассмотрим теперь последовательность матричных произведений $\{A_{i_1}, A_{i_2}A_{i_1}, A_{i_3}A_{i_2}A_{i_1}, \ldots\}$ и последовательность верхних правых угловых матриц $\{h_1, h_2, h_3, \ldots\}$. Легко проверяется следующее правило умножения блочных матриц:

$$\begin{pmatrix} I_k & H_2 \\ 0 & L_2 \end{pmatrix} \cdot \begin{pmatrix} I_k & H_1 \\ 0 & L_1 \end{pmatrix} = \begin{pmatrix} I_k & H_1 + H_2L_1 \\ 0 & L_1L_2 \end{pmatrix}.$$

Тогда по индукции легко доказать, что

$$h_m = H_{i_1} + H_{i_2}L_{i_1} + \ldots + H_{i_m}L_{i_{m-1}} \ldots L_{i_1}.$$

При этом важно отметить, что, поскольку исходные матрицы $\{A_1, \ldots, A_s\}$ являлись стохастическими, все матрицы $H_1, \ldots, H_s$ являются квазистохастическими, а значит, их норма не превосходит единицы.

Докажем, что последовательность матриц $\{h_1, h_2, h_3, \ldots\}$ имеет предел. Воспользуемся критерием Коши, справедливым и для матричных последовательностей. Докажем, что найдётся такое число $M \in \mathbb{N}$, что для всех $m_2 > m_1 > M$ выполнено $\|h_{m_2} - h_{m_1}\| < \varepsilon$. Пусть $M > N_0$. Пусть также $m_1 = p_1N_0 + q_1$, $m_2 = p_2N_0 + q_2$, $0 \leqslant q_1 < N_0$, $0 \leqslant q_2 < N_0$, $p_2 \geqslant p_1 \geqslant 1$. Тогда

$$\begin{aligned}\|h_{m_2} - h_{m_1}\| &= \|H_{m_2}L_{m_2-1} \ldots L_{i_1} + \ldots + H_{m_1+1}L_{m_1} \ldots L_{i_1}\| \leqslant \\ &\leqslant \|H_{m_2}L_{m_2-1} \ldots L_{i_1}\| + \ldots + \|H_{m_1+1}L_{m_1} \ldots L_{i_1}\| \leqslant \\ &\leqslant \|L_{m_2-1} \ldots L_{i_1}\| + \ldots + \|L_{m_1} \ldots L_{i_1}\| \leqslant N_0(\varepsilon^{p_1} + \ldots + \varepsilon^{p_2}),\end{aligned}$$

поскольку в данной сумме число слагаемых с длиной от p_1N_0 до $(p_1+1)N_0 - 1$ не более N_0, число слагаемых с длиной от $(p_1+1)N_0$ до $(p_1+2)N_0 - 1$ не более N_0 и т. д., число слагаемых с длиной от p_2N_0 до $(p_2+1)N_0 - 1$ не более N_0. Отсюда получаем требуемую оценку. Можно существенно упростить выражение в правой части оценки:

$$\begin{aligned}N_0(\varepsilon^{p_1} + \ldots + \varepsilon^{p_2}) = N_0\varepsilon^{p_1}(1 + \varepsilon + \ldots + \varepsilon^{p_2-p_1}) < N_0\varepsilon^{p_1}(1 + \varepsilon + \ldots) = \\ = N_0\varepsilon^{p_1} \sum_{m=0}^{\infty} \varepsilon^m = \frac{N_0\varepsilon^{p_1}}{1-\varepsilon} \leqslant \frac{N_0\varepsilon}{1-\varepsilon} < 2N_0\varepsilon\end{aligned}$$

при $\varepsilon < 1/2$. Таким образом, имеем неравенство $\|h_{m_2} - h_{m_1}\| < 2N_0\varepsilon = 2M_0(t\varepsilon)$. Натуральное число t мы выбрали исходя из неравенства $\gamma^t < \varepsilon$, поэтому $t > \ln\varepsilon/\ln\gamma$, т. е. достаточно взять $t = [\ln\varepsilon/\ln\gamma] + 1$, где $[x]$ означает целую часть числа x. Так как

$$\lim_{\varepsilon\to 0} \varepsilon\left(\left[\frac{\ln\varepsilon}{\ln\gamma}\right] + 1\right) = 0,$$

число $2M_0$ постоянно и не зависит от ε, то согласно критерию Коши последовательность матриц $\{h_1, h_2, \ldots\}$ сходится.

Несложно доказать также, что если имеется последовательность блочных матриц

$$\begin{pmatrix} I_k & A_n \\ 0 & B_n \end{pmatrix}$$

и последовательности $\{A_n\}$ и $\{B_n\}$ сходятся, то исходная последовательность также сходится.

Таким образом, сходимость последовательности $\Pi(I)$ доказана.

Для завершения доказательства теоремы заметим, что из того что последовательность матричных произведений $\{L_{i_1}, L_{i_2}L_{i_1}, L_{i_3}L_{i_2}L_{i_1}, \ldots\}$ сходится к нулевой матрице, следует, что матрица C_I в рассматриваемом базисе имеет нулевые строки начиная с $(k+1)$-й, т. е. имеет вид

$$\begin{pmatrix} I_k & * \\ 0 & 0 \end{pmatrix}.$$

Значит её образ есть пространство $\mathcal{W}$, откуда немедленно следует второе утверждение теоремы.

Теорема полностью доказана. □

Мы привели достаточное условие существования предела последовательности $\Pi(I)$. Как показывают результаты предложений 3.29 и 3.30, в случае невыполнения отдельных частей этого условия последовательность $\Pi(I)$ может не иметь предела.

Подобная задача рассматривалась в [5, следствие 3.3], с той разницей, что там использовалось классическое определение стохастической матрицы (которое может быть найдено, например, в [2, гл. 8, § 6, определение 4]). Эта разница оказывается весьма существенной, поскольку среди всех стандартных норм $\|\cdot\|_p$, $p \geqslant 1$, $p = \infty$, единственной нормой, значение которой для стохастических матриц с учётом определения, используемого в данной работе, не превосходит единицы, является норма $\|\cdot\|_1$, рассматриваемая нами. При этом аппарат, используемый в [5], оказывается неприменим в нашей постановке. Это приводит к тому, что формулировки достаточного условия сходимости, приведённые в [5, теорема 3.1, следствия 3.2, 3.3] и в данной работе (теорема 3.40), существенно различаются.

Сформулированное в теореме 3.40 условие, как нетрудно видеть, является достаточным, но, вообще говоря, не необходимым. Однако справедлив следующий результат.

Теорема 3.41. *Пусть $\{A_1, \ldots, A_s\}$ — множество стохастических матриц, не обязательно имеющих степенной предел. Пусть последовательность $\Pi(I)$ имеет предел — матрицу C. Пусть также для некоторого подмножества $R \subset \{1, \ldots, s\}$ верно, что любой элемент множества R встречается в последовательности I бесконечное число раз. Тогда для любого элемента $r \in R$ образ матрицы C является подмножеством пространства неподвижных векторов матрицы A_r, т. е. $C(\mathbb{C}^n) \subset \mathcal{W}(A_r)$.*

Доказательство. Возьмём любое значение $\varepsilon > 0$. Тогда, поскольку последовательность $\Pi(I)$ имеет предел, найдётся натуральное число M, такое что $\|\pi_m - C\| < \varepsilon$ для всех натуральных $m \geqslant M$. Поскольку любой элемент $r \in R$ встречается в последовательности I бесконечное число раз, найдётся такой номер m, что верно неравенство $m > M$ и, кроме того, справедливо представление $\pi_{m+1} = A_r\pi_m$ (если это не так, то матрица A_r встречается в произведениях множества $\Pi(I)$ конечное число раз). Тогда справедливы неравенства $\|A_r\pi_m - C\| < \varepsilon$, $\|\pi_m - C\| < \varepsilon$. Тогда в силу замечания 1.9

$$\|A_r\pi_m - A_rC\| \leqslant \|A_r\|\,\|\pi_m - C\| = \|\pi_m - C\| < \varepsilon.$$

Но тогда

$$\|A_rC - C\| = \|(A_r\pi_m - C) - (A_r\pi_m - A_rC)\| \leqslant \|A_r\pi_m - C\| + \|A_r\pi_m - A_rC\| < 2\varepsilon.$$

Поскольку значение ε произвольно, получаем, что $\|A_rC - C\| = 0$, поэтому $A_rC = C$. Но это значит, что для любого вектора v выполнено равенство $A_r(Cv) = Cv$, т. е. вектор Cv является собственным вектором матрицы A_r, что и утверждает теорема. □

Следствие 3.42. *Пусть $\{A_1, \ldots, A_s\}$ — множество стохастических матриц. Пусть последовательность $\Pi(I)$ имеет предел — матрицу C. Пусть все элементы множества $\{1, \ldots, s\}$ встречается в последовательности I бесконечное число раз. Тогда для любого r образ матрицы C является подмножеством пространства неподвижных векторов матрицы A_r, т. е. $C(\mathbb{C}^n) \subset \mathcal{W}(A_r)$.*

Следствие 3.43. *Пусть $\{A_1, \ldots, A_s\}$ — множество стохастических матриц. Пусть последовательность $\Pi(I)$ имеет предел — матрицу C. Пусть также для некоторого подмножества $R \subset \{1, \ldots, s\}$ верно, что любой элемент множества R встречается в последовательности I бесконечное число раз. Тогда справедливо включение $C(\mathbb{C}^n) \subset \bigcap\limits_{r\in R} \mathcal{W}(A_r)$ и, в частности, $\dim \bigcap\limits_{r\in R} \mathcal{W}(A_r) \geqslant 1$. Соответственно, если $\bigcap\limits_{r\in R} \mathcal{W}(A_r) = \{0\}$, то последовательность $\Pi(I)$ не имеет предела.*

Следствие 3.44. *Пусть $\{A_1, \ldots, A_s\}$ — множество слабособственных стохастических матриц. Пусть все элементы множества $\{1, \ldots, s\}$ встречаются в последовательности I бесконечное число раз. Пусть также найдутся такие различные матрицы A_i и A_j, что $\mathcal{W}(A_i) \neq \mathcal{W}(A_j)$. Тогда последовательность $\Pi(I)$ не имеет предела.*

Из сформулированных выше утверждение получаем следующий важный для нас результат.

Теорема 3.45. *Пусть $\{A_1, \ldots, A_s\}$ — множество стохастических матриц, являющихся матрицами перехода (преобразования распределения состояний) вероятностного автомата с конечным множеством состояний $Q = \{q_1, \ldots, q_n\}$. Пусть последовательность $\Pi(I)$ имеет предел — матрицу C. Пусть также для некоторого подмножества $R \subset \{1, \ldots, s\}$ верно, что любой элемент множества R встречается в последовательности I бесконечное число раз. Пусть v — стохастический вектор, такой что координаты вектора Cv с номерами $i_1, \ldots, i_t$ равны нулю, остальные координаты строго положительны. Пусть множества $Q_2 \in Q$ и $Q_1 \in Q$ определены равенствами $Q_2 = \{q_{i_1}, \ldots, q_{i_t}\}$ и $Q_1 = Q \setminus Q_2$. Тогда для любого $r \in R$ вероятности перехода в матрице A_r из любого состояния множества Q_1 в любое состояние множества Q_2 равны нулю, т. е. $p(x_r, \rho_1, \rho_2) = 0$ для любых $\rho_1 \in Q_1$, $\rho_2 \in Q_2$.*

Доказательство. Согласно теореме 3.41 вектор Cv есть собственный вектор матриц $\{A_r\}_{r \in R}$. Для завершения доказательства осталось применить теорему 3.27. □

Данная теорема, как и её «одномерный» аналог (теорема 3.27), полезна в приложениях. Если множество Q_2 есть множество состояний автоматизированной системы, в которых уровень защищённости системы не является приемлемым («опасные состояния»), а множество Q_1 — множество «безопасных состояний», то из того факта, что для некоторого вектора начального распределения состояний в случае подачи некоторой последовательности, приводящей к стабилизации распределения состояний, получаем такое распределение, в котором вероятность нахождения в опасных состояниях равна нулю, следует, что изначально автоматизированная система при подаче любого из сигналов данной последовательности, повторяющегося в ней бесконечное число раз, имеет нулевую вероятность перехода из безопасных состояний в опасные.

Таким образом, грубо описывая данный результат, можно сказать, что если в пределе система не переходит в опасные состояния, то она не переходит в них ни на каком шаге.

4. Сканирование автоматизированных систем

Как уже отмечалось выше, под процессом сканирования автоматизированной системы (или вероятностного автомата $\mathcal{A}$) понимается процесс передачи на вход системы заранее заданной последовательности входных сигналов $\{x_1, \ldots, x_m\}$ и получения последовательности выходных сигналов $\{y_1, \ldots, y_m\}$. При этом в том случае, когда больше про вероятностный автомат ничего неизвестно, данный процесс называется *внешним сканированием*. Также при решении задач анализа защищённости автоматизированной системы рассматривается процесс

внутреннего сканирования, при котором считается известным распределение вероятностей перехода $p(x, q, y, q')$.

Имея выходные сигналы $\{y_1, \ldots, y_m\}$, мы пытаемся определить начальное распределение состояний вероятностного автомата ρ_0. В этом и заключается процедура внутреннего сканирования.

Определение 4.1. Процедура сканирования называется эффективной, если она позволяет определить вектор начального состояния ρ_0 с любой наперёд заданной точностью (по векторной норме) при любом векторе ρ_0.

В дальнейшем мы будем исследовать возможность построения эффективной политики сканирования. Для начала же приведём формальную модель и метод определения начального вектора.

Построение политики эффективного сканирования является весьма сложной задачей. Более того, она практически неразрешима в общем случае, когда о матрицах Y_k и Q_k (данные матрицы были введены в определении 2.3) практически ничего не известно.

В реальной ситуации для автоматизированной системы справедливо неравенство $|Y| < |Q|$. Однако после внедрения комплексной системы защиты информации производится полный контроль состояний автоматизированной системы и её переходов с применением целого набора различных средств защиты, функционирующих на различных рубежах. Фактически применение средств защиты расширяет множество выходных сигналов за счёт появления так называемых «внутренних сигналов», обеспечивающих трассировку состояний (активный аудит). Также в реальности рассматриваются не все состояния, а некоторые классы эквивалентности (в общем случае описать данные классы не представляется возможным). Поэтому мы будем считать, что после применения средств защиты и аудита справедливо равенство $|Y| = |Q|$. На самом деле, как уже отмечалось выше, при внутреннем сканировании зачастую по прямым или косвенным признакам автоматизированной системы возможно получить данные о текущем состоянии системы, так что можно считать что все матрицы Y_k являются обратимыми матрицами.

Тогда мы сводим задачу моделирования сканирования к следующей постановке.

Пусть $\{\xi_i\}_{i=1}^{\infty}$ — последовательность случайных величин, имеющих дискретное распределение, являющихся выходными сигналами вероятностного автомата. При этом ξ_i принимает значения из множества $\{y_1, \ldots, y_n\} = Y$ с вероятностями $\{p_1^i, \ldots, p_n^i\}_{i=1}^{\infty}$. Множество входных сигналов вероятностного автомата конечно. Обозначим его через $X = \{x_1, \ldots, x_k\}$. На вход вероятностного автомата подаётся последовательность сигналов $I = \{x_{i_1}, x_{i_2}, \ldots, x_{i_m}\}$. Пусть вектор начального (в момент начала процедуры сканирования) распределения состояний вероятностного автомата обозначен через ρ, это n-мерный стохастический вектор (ввиду равенства $|Q| = |Y|$).

Используя равенство (2.4), нетрудно получить формулы для векторов распределения случайных величин ξ_i: $p^1 = Y_{i_1}\rho$, $p^2 = Y_{i_2}Q_{i_1}\rho, \ldots$, $p^m =$

$= Y_{i_m} Q_{i_{m-1}} \dots Q_{i_1} \rho$, причём вектор ρ неизвестен, значения $\{y_1, \dots, y_n\}$ и матрицы переходов и выходов $\{Q_i\}_{i=1}^k$, $\{Y_i\}_{i=1}^k$ считаются известными. Данная модель описывает процесс внутреннего сканирования автоматизированной системы.

Сформулируем теперь задачу эффективного сканирования в новой постановке. Пусть в результате эксперимента (проведения внутреннего сканирования) были получены значения выходных сигналов вероятностного автомата $\{z_1, \dots, z_m\}$ как реализации соответствующей последовательности случайных величин $\{\xi_i\}_{i=1}^m$. Необходимо оценить условия, при которых имеется возможность построения по данному набору значений оценки для вектора ρ, близкой к нему по норме, введённой в определении 1.8.

Для построения алгоритма эффективного сканирования необходимо доказать несколько предварительных утверждений.

Лемма 4.2. *Для последовательности случайных величин $\{\xi_i\}_{i=1}^m$ для любого натурального s выполняется свойство $\mathrm{E}|\xi_i^s| < C(s)$, где $C(s)$ — некая положительная константа, не зависящая от i, а зависящая исключительно от степени момента (величины s).*

Доказательство. Справедливо неравенство

$$\mathrm{E}|\xi_i^s| = \sum_{j=1}^n |y_j^s| p_j^i \leqslant \sum_{j=1}^n |y_j^s| = C(s).$$

Как нетрудно видеть, величина в правой части неравенства не зависит от номера i. При доказательстве данного утверждения существенно использован тот факт, что все случайные величины принимают одно множество значений. □

Лемма 4.3. *Для любых неотрицательных чисел a и b имеет место неравенство $(a+b)^4 \leqslant 8(a^4 + b^4)$.*

Доказательство. Неравенство $(a+b)^4 \leqslant 8(a^4+b^4)$ справедливо тогда и только тогда, когда справедливо неравенство $((a+b)/2)^4 \leqslant (a^4+b^4)/2$. Данное неравенство выполняется ввиду выпуклости вниз функции $f(x) = x^4$. □

Лемма 4.4. *Для последовательности случайных величин $\{\xi_i\}_{i=1}^m$ для любого натурального s выполняется свойство $\mathrm{E}|\xi_i^s - \mathrm{E}(\xi_i^s)|^4 < C$, где C — некая положительная константа, не зависящая от i, т. е. четвёртый центральный момент величины ξ_i^s равномерно ограничен.*

Доказательство. Поскольку для любых чисел a и b верно неравенство $|a-b| \leqslant |a| + |b|$, то имеем

$$|\xi_i^s - \mathrm{E}(\xi_i^s)| \leqslant (|\xi_i^s| + |\mathrm{E}(\xi_i^s)|).$$

Тогда в силу леммы 4.3 справедливо неравенство

$$|\xi_i^s - \mathrm{E}(\xi_i^s)|^4 \leqslant (|\xi_i^s| + |\mathrm{E}(\xi_i^s)|)^4 \leqslant 8(|\xi_i^{4s}| + |\mathrm{E}(\xi_i^s)|^4) \leqslant 8(|\xi_i^{4s}| + (\mathrm{E}|\xi_i^s|)^4),$$

поскольку для любой случайной величины η верно неравенство $|\mathrm{E}\eta| \leqslant \mathrm{E}|\eta|$ (см. [4, гл. 2, § 6, утверждение 3.C]. Таким образом, получаем, что

$$\mathrm{E}|\xi_i^s - \mathrm{E}(\xi_i^s)|^4 \leqslant 8(\mathrm{E}|\xi_i^{4s}| + (\mathrm{E}|\xi_i^s|)^4) \leqslant 8(C(4s) + C(s)^4) = D(s)$$

по лемме 4.2. При этом видно, что значение $D(s)$ не зависит от i, что и требовалось доказать. □

Справедлив следующий результат (усиленный закон больших чисел в форме Кантелли, см. [4, гл. 4, § 3, теорема 1]. Пусть задана последовательность случайных величин $\xi_1, \xi_2, \ldots$, все случайные величины имеют конечный четвёртый момент, при этом центральный четвёртый момент равномерно ограничен: существует такое число C, что для любого i выполнено $\mathrm{E}|\xi_i - \mathrm{E}\xi_i|^4 \leqslant C$. Тогда справедливо следующее утверждение:

$$\frac{\xi_1 + \ldots + \xi_m - \mathrm{E}(\xi_1 + \ldots + \xi_m)}{m} \to 0 \quad \text{(п. н.)}.$$

Как известно [4, гл. 2, § 10, теорема 2], из сходимости с вероятностью 1 следует сходимость по вероятности, т. е. для любых $\varepsilon_1, \varepsilon_2 > 0$ найдётся $K(\varepsilon_1, \varepsilon_2)$, такое что для всех $k > K(\varepsilon_1, \varepsilon_2)$

$$\mathrm{P}\left(\left|\frac{\xi_1 + \ldots + \xi_k - \mathrm{E}(\xi_1 + \ldots + \xi_k)}{k}\right| > \varepsilon_1\right) < \varepsilon_2. \tag{2}$$

На основании леммы 4.4 мы получаем, что для последовательности $\{\xi_i^s\}$ справедлив усиленный закон больших чисел (2). Значит, для любых $\varepsilon_1, \varepsilon_2 > 0$ и любого $s = \overline{1,n}$ найдётся $M_s(\varepsilon_1, \varepsilon_2)$, такое что для всех $m > M_s(\varepsilon_1, \varepsilon_2)$

$$\mathrm{P}\left(\left|\frac{\xi_1^s + \ldots + \xi_m^s - \mathrm{E}(\xi_1^s + \ldots + \xi_m^s)}{m}\right| > \varepsilon_1\right) < \varepsilon_2.$$

Обозначим через $\alpha_s(m)$ событие

$$\left\{\omega \in \Omega\colon \left|\frac{(\xi_1^s + \ldots + \xi_m^s)(\omega) - \mathrm{E}(\xi_1^s + \ldots + \xi_m^s)}{m}\right| > \varepsilon_1\right\}.$$

Пусть

$$M(\varepsilon_1, \varepsilon_2) = \max_{s=\overline{1,n}} M_s(\varepsilon_1, \varepsilon_2). \tag{3}$$

Если взять $m > M$, то получим, что $\mathrm{P}(\alpha_s(m)) < \varepsilon_2$ для всех $s = \overline{1,n}$.

Пусть событие $\beta(m)$ определено равенством

$$\beta(m) = \left\{\omega \in \Omega\colon \forall s = \overline{1,n}\ \omega \notin \alpha_s(m)\right\}.$$

Тогда, как нетрудно видеть,

$$\beta(m) = \Omega \setminus \bigcup_{s=\overline{1,n}} \alpha_s(m).$$

Значит, из аксиоматики теории вероятностей следует, что

$$\mathrm{P}(\beta(m)) = 1 - \mathrm{P}\Big(\bigcup_{s=\overline{1,n}} \alpha_s(m)\Big).$$

Для любых двух событий A и B имеет место равенство (см. [4, гл. 2, § 1, свойства меры]) $\mathrm{P}(A\cup B) = \mathrm{P}(A)+\mathrm{P}(B)-\mathrm{P}(AB)$, откуда следует, что $\mathrm{P}(A\cup B) \leqslant \leqslant \mathrm{P}(A) + \mathrm{P}(B)$. Но тогда получаем, что

$$\mathrm{P}\Big(\bigcup_{s=\overline{1,n}} \alpha_s(m)\Big) \leqslant \sum_{s=1}^{n} \mathrm{P}(\alpha_s(m)),$$

откуда следует полезное неравенство

$$\mathrm{P}(\beta(m)) \geqslant 1 - \sum_{s=1}^{n} \mathrm{P}(\alpha_s(m)).$$

Если $m > M$, то

$$\mathrm{P}(\beta(m)) \geqslant 1 - \sum_{s=1}^{n} \mathrm{P}(\alpha_s(m)) \geqslant 1 - \sum_{s=1}^{n} \varepsilon_2 = 1 - n\varepsilon_2. \tag{4}$$

Перейдём теперь к построению политики эффективного сканирования.

Вычислим теоретические значения моментов порядка $s = \overline{1,n}$ для случайных величин $\{\xi_t\}_{t=1}^{m}$:

$$\mathrm{E}\xi_t^s = \sum_{j=1}^{n} y_j^s (Y_{i_t} Q_{i_{t-1}} \dots Q_{i_1}\rho)_j.$$

При этом при $t = 1$ под значением выражения $Q_{i_{t-1}} \dots Q_{i_1}$ понимается единичная матрица. Тогда

$$\frac{1}{m}\sum_{t=1}^{m} \mathrm{E}\xi_t^s = \frac{1}{m}\sum_{t=1}^{m}\sum_{j=1}^{n} y_j^s (Y_{i_t}(Q_{i_{t-1}} \dots Q_{i_1})\rho)_j =$$

$$= \frac{1}{m}\sum_{j=1}^{n} y_j^s \sum_{t=1}^{m} Y_{i_t}((Q_{i_{t-1}} \dots Q_{i_1})\rho)_j = \sum_{j=1}^{n} y_j^s \left(\left(\frac{1}{m}\sum_{t=1}^{m} Y_{i_t} Q_{i_{t-1}} \dots Q_{i_1}\right)\rho\right)_j.$$

Обозначим матрицы

$$\frac{1}{m}\sum_{t=1}^{m} Y_{i_t} Q_{i_{t-1}} \dots Q_{i_1}$$

через S_m. Тогда очевидно, что все матрицы S_m являются стохастическими, как нормированная сумма стохастических матриц. Перепишем полученное ранее выражение с учётом введённых обозначений:

$$\frac{1}{m}\sum_{t=1}^{m} \mathrm{E}\xi_t^s = \sum_{j=1}^{n} y_j^s (S_m\rho)_j.$$

Пусть $y^\theta(m)$ — вектор-столбец размера n, определённый покоординатно следующим образом:

$$y^\theta(m)_s = \frac{1}{m}\sum_{t=1}^{m} \mathrm{E}\xi_t^s, \quad s = \overline{1,n}.$$

Также определим матрицу V по правилу $V_{sj} = y_j^s$, где s обозначает строку, j — столбец, $s = \overline{1,n}$, $j = \overline{1,n}$. Тогда для вектора нормированных теоретических моментов справедливо матричное равенство

$$y^\theta(m) = VS_m\rho \iff S_m\rho = V^{-1}y^\theta(m). \tag{5}$$

Теперь становится понятной методология определения вектора ρ. Основная проблема заключается в том, что вектор $y^\theta(m)$ нам неизвестен. Однако нам известно его приближение.

Определим вектор практических моментов $y^\pi(m)$ размера n покоординатно следующим образом:

$$y^\pi(m)_s = \frac{1}{m}\sum_{t=1}^{m}\xi_t^s, \quad s = \overline{1,n}.$$

Лемма 4.5. *Для любых положительных значений ε, γ найдётся такое натуральное число M, что для всех натуральных $m > M$ верно неравенство*

$$\mathrm{P}(\|y^\theta(m) - y^\pi(m)\| < \varepsilon) > 1 - \gamma.$$

Доказательство. Пусть $\varepsilon_1 = \varepsilon/n$, $\varepsilon_2 = \gamma/n$. Возьмём $M = M(\varepsilon_1, \varepsilon_2)$ (см. определение (3)). Тогда в силу неравенства (4) получаем утверждение

$$\mathrm{P}(\forall s = \overline{1,n}\ |y^\theta(m)_s - y^\pi(m)_s| < \varepsilon_1) > 1 - n\varepsilon_2,$$

откуда следует, что

$$\mathrm{P}\left(\forall s = \overline{1,n}\ |y^\theta(m)_s - y^\pi(m)_s| < \frac{\varepsilon}{n}\right) > 1 - \gamma.$$

Поскольку

$$\|y^\theta(m) - y^\pi(m)\| = \sum_{s=1}^{n}|y^\theta(m)_s - y^\pi(m)_s| < \sum_{s=1}^{n}\frac{\varepsilon}{n} = \varepsilon,$$

то получаем, что

$$\mathrm{P}(\|y^\theta(m) - y^\pi(m)\| < \varepsilon) \geqslant \mathrm{P}\left(\forall s = \overline{1,n}\ |y^\theta(m)_s - y^\pi(m)_s| < \frac{\varepsilon}{n}\right) > 1 - \gamma,$$

что и требовалось доказать. □

Это означает, что при проведении сканирования мы имеем возможность заменить вектор теоретических моментов на вектор практических моментов, причём сделать это возможно с любой заданной точностью. Тогда, учитывая равенство (5), можно попытаться вычислить вектор распределения ρ: $S_m\rho \approx V^{-1}y^\pi(m)$, $m \to \infty$.

Очевидно, что если матрица S_m не является обратимой, то однозначно определить вектор ρ не удастся, поэтому если все матрицы S_m необратимы начиная с некоторого номера M_0, то политика сканирования не является эффективной. Значит, у матричной последовательности $\{S_m\}$ имеется бесконечная подпоследовательность обратимых матриц. Не ограничивая общности, можем считать,

что последовательность S_m состоит из обратимых матриц, поскольку мы всегда имеем возможность расширить рассматриваемое множество входных сигналов и рассматривать «комплексные сигналы», являющиеся некоторыми заданными последовательностями элементарных сигналов. Тогда можем записать выражение для вектора ρ следующим образом: $\rho \approx S_m^{-1}V^{-1}(y^\pi(m))$.

Если последовательность S_m^{-1} (определённая только для тех m, для которых матрица S_m обратима) не является сходящейся, то в общем случае нельзя утверждать, что политика сканирования является эффективной. В то же время если имеется сходимость, то политика сканирования является эффективной, что доказывается в следующей теореме.

Теорема 4.6. *Пусть последовательность матриц S_m^{-1} сходится к некоторой матрице T. Пусть вектор ρ_m определён равенством $\rho_m = S_m^{-1}V^{-1}(y^\pi(m))$. Тогда для любых $\varepsilon, \gamma > 0$ найдётся такое натуральное M, что при всех $m > M$ верно неравенство $\mathrm{P}(\|\rho - \rho_m\| < \varepsilon) > 1 - \gamma$.*

Доказательство. Так как последовательность S_m^{-1} сходится к матрице T, существует такое натуральное число M_1, что при всех $m > M_1$ верно неравенство $\|S_m^{-1} - T\| < 1$. Тогда для всех $m > M_1$ выполняется неравенство

$$\|S_m^{-1}\| = \|T + (S_m^{-1} - T)\| \leqslant \|T\| + \|S_m^{-1} - T\| \leqslant \|T\| + 1.$$

Согласно лемме 4.5 для любых $\varepsilon_1, \gamma > 0$ найдётся такое натуральное число M_2, что для всех $m > M_2$ верно неравенство $\mathrm{P}(\|y^\theta(m) - y^\pi(m)\| < \varepsilon_1) > 1 - \gamma$. Пусть $\varepsilon_1 = \varepsilon/((\|T\| + 1)\|V^{-1}\|)$. Тогда имеет место неравенство

$$\begin{aligned}\|\rho - \rho_m\| &= \|S_m^{-1}V^{-1}(y^\theta(m)) - S_m^{-1}V^{-1}(y^\pi(m))\| \leqslant \\ &\leqslant \|S_m^{-1}V^{-1}\|\,\|y^\theta(m) - y^\pi(m)\| \leqslant \|S_m^{-1}\|\,\|V^{-1}\|\,\|y^\theta(m) - y^\pi(m)\|.\end{aligned}$$

Пусть $m \in \mathbb{N}$ таково, что $m > \max(M_1, M_2)$. Тогда справедливо неравенство

$$\|\rho - \rho_m\| \leqslant (\|T\| + 1)\|V^{-1}\|\varepsilon_1 = \varepsilon$$

с вероятностью не менее чем $1 - \gamma$.

Теорема доказана. □

Таким образом, если последовательность матриц S_m^{-1} сходится, то политика сканирования гарантированно является эффективной.

Лемма 4.7. *Пусть последовательность обратимых матриц $\{A_i\}$ сходится к обратимой матрице B. Тогда последовательность обратных матриц $\{A_i^{-1}\}$ также является сходящейся и её предел равен B^{-1}.*

Доказательство. Докажем сначала, что нормы всех матриц $\{A_i^{-1}\}$ являются ограниченными в совокупности, т. е. найдётся такое число C, что $\|A_i^{-1}\| \leqslant C$ для всех натуральных i. Пусть это не так. Тогда для любого $C > 0$ найдётся такое натуральное число m, что $\|A_m^{-1}\| > C$, причём значения m возрастают по мере возрастания значения C. Это значит, что для всех $C > 0$ найдутся натуральное число m и вектор $v \neq 0$, такие что $\|A_m^{-1}v\| > C\|v\|$. Так как матрица A_m является обратимой, а значит, она является матрицей полного ранга, то

найдётся вектор $u \neq 0$, такой что $v = A_m u$. Тогда неравенство можно записать следующим образом:

$$\|A_m^{-1}(A_m u)\| > C\|A_m u\| \iff \|A_m u\| < \frac{1}{C}\|u\|.$$

Далее,

$$\|Bu\| = \|A_m u + (B - A_m)u\| \leqslant \|A_m u\| + \|(B - A_m)u\| \leqslant \|A_m u\| + \|B - A_m\|\,\|u\|.$$

Возьмём любое $\varepsilon > 0$. Поскольку последовательность $\{A_m\}$ сходится, то найдётся такое число $M \in \mathbb{N}$, что для всех натуральных $m > M$ $\|A_m - B\| < \varepsilon/2$. Также найдутся число $C > 2/\varepsilon$, натуральное число $m > M$ и вектор $u \neq 0$, такие что

$$\|A_m u\| < \frac{1}{C}\|u\| < \frac{\varepsilon}{2}\|u\|.$$

Тогда

$$\|Bu\| \leqslant \|A_m u\| + \|B - A_m\|\,\|u\| < \frac{\varepsilon}{2}\|u\| + \frac{\varepsilon}{2}\|u\| = \varepsilon\|u\|.$$

Итак, мы получили, что для любого $\varepsilon > 0$ найдётся вектор $u \neq 0$, такой что $\|Bu\| < \varepsilon\|u\|$. Так как матрица B обратима, найдётся вектор v, такой что $u = B^{-1}v$ и $v \neq 0$. Тогда $\|B(B^{-1}v)\| < \varepsilon\|B^{-1}v\|$, поэтому $\|B^{-1}v\| > (1/\varepsilon)\|v\|$.

Пусть $0 < \varepsilon < 1/\|B^{-1}\|$. Тогда получаем, что найдётся вектор $v \neq 0$, такой что

$$\|B^{-1}v\| > \frac{1}{\varepsilon}\|v\| > \|B^{-1}\|\,\|v\|,$$

что противоречит определению нормы. Полученное противоречие доказывает тот факт, что нормы матриц $\{A_i^{-1}\}$ являются ограниченными в совокупности и найдётся число C, такое что $\|A_i^{-1}\| \leqslant C$ для всех натуральных i.

Перейдём теперь к доказательству утверждения леммы. Имеет место равенство $B^{-1} - A_m^{-1} = A_m^{-1}(A_m - B)B^{-1}$, откуда получаем неравенство

$$\|B^{-1} - A_m^{-1}\| = \|A_m^{-1}(A_m - B)B^{-1}\| \leqslant$$
$$\leqslant \|A_m^{-1}\|\,\|A_m - B\|\,\|B^{-1}\| \leqslant C\|B^{-1}\|\,\|A_m - B\|.$$

Поскольку значение $C\|B^{-1}\|$ постоянно, а значение $\|A_m - B\|$ стремится к нулю ввиду сходимости последовательности $\{A_m\}$, получаем, что значение $\|B^{-1} - A_m^{-1}\|$ стремится к нулю при m, стремящемся к бесконечности. Утверждение доказано. □

Лемма 4.8. *Пусть имеется последовательность обратимых стохастических матриц, таких что последовательность $\{A_i^{-1}\}$ сходится к некоторой матрице B. Тогда матрица B обратима, последовательность матриц $\{A_i\}$ является сходящейся, причём её предел равен матрице B^{-1}.*

Доказательство. Так как последовательность $\{A_i^{-1}\}$ сходится к матрице B, то для любого $\varepsilon > 0$ найдётся натуральное число M, такое что $\|A_m^{-1} - B\| < \varepsilon$ для всех натуральных $m > M$. Но тогда имеет место неравенство

$$\|E - A_m B\| = \|A_m(A_m^{-1} - B)\| \leqslant \|A_m\|\,\|A_m^{-1} - B\| < \varepsilon,$$

поскольку матрицы A_m стохастические, а значит, их норма равна 1. Итак, получаем, что $\|E-A_mB\| < \varepsilon$. Пусть матрица B не является обратимой, значит, имеет нетривиальное ядро, т. е. найдётся вектор $v \neq 0$, такой что $Bv = 0$. Но тогда $\|(E - A_mB)(v)\| \leqslant \|E - A_mB\|\,\|v\| < \varepsilon\|v\|$. С другой стороны, $(E - A_mB)v = v - A_m(Bv) = v$, откуда получаем, что $\|(E - A_mB)v\| = \|v\| < \varepsilon\|v\|$, что неверно при $\varepsilon < 1$. Полученное противоречие доказывает, что предположение о наличии таких векторов v неверно и, значит, матрица B является обратимой.

Оставшаяся часть утверждения леммы следует из леммы 4.7.

Лемма доказана. □

Объединяя леммы 4.7 и 4.8, получаем следующий результат.

Теорема 4.9. *Пусть имеется последовательность стохастических матриц $\{A_i\}$. Последовательность $\{A_i^{-1}\}$ сходится тогда и только тогда, когда последовательность $\{A_i\}$ сходится к обратимой матрице.*

Лемма 4.10. *Пусть последовательность обратимых матриц $\{A_i\}$ сходится к необратимой матрице B. Тогда нормы матриц $\{A_i^{-1}\}$ стремятся к бесконечности.*

Доказательство. Если матрица B необратима, то найдётся такой вектор $v \neq 0$, что $Bv = 0$. Возьмём произвольное $\varepsilon > 0$. Тогда, поскольку последовательность $\{A_i\}$ сходится к B, найдётся такое натуральное число M, что для всех натуральных $m > M$ верно неравенство $\|A_m-B\| < \varepsilon$. Тогда $\|(A_m-B)v\| \leqslant \leqslant \|A_m-B\|\,\|v\| < \varepsilon\|v\|$. С другой стороны, $\|(A_m-B)v\| = \|A_mv\|$, поэтому имеет место неравенство $\|A_mv\| < \varepsilon\|v\|$. Так как матрица A_m обратима, она является полноранговой, а значит, найдётся такой ненулевой вектор u, что $v = A_m^{-1}u$. Тогда верно неравенство $\|A_m(A_m^{-1}u)\| < \varepsilon\|A_m^{-1}u\|$, поэтому $\|A_m^{-1}u\| > (1/\varepsilon)\|u\|$, следовательно, $\|A_m^{-1}\| > 1/\varepsilon$, откуда в силу произвольности ε следует утверждение леммы. □

Из утверждений теоремы 4.9 и леммы 4.10 и доказательства теоремы 4.6 получаем, что эффективная политика сканирования существует тогда и только тогда, когда последовательность матриц S_m сходится к обратимой матрице.

Лемма 4.11. *Пусть $\{A_i\}_{i=1}^{\infty}$ — последовательность стохастических матриц. Пусть $\{B_i\}_{i=1}^{\infty}$ — последовательность матриц, сходящаяся к матрице B. Рассматривается последовательность*

$$C_m = \frac{1}{m}\sum_{i=1}^{m} A_iB_i.$$

Пусть последовательность C_m сходится к матрице C. Тогда последовательность

$$D_m = \frac{1}{m}\sum_{i=1}^{m} A_iB$$

также сходится к матрице C.

Доказательство. Возьмём произвольное $\varepsilon > 0$. Поскольку последовательность B_i сходится к матрице B, то найдётся такое натуральное число M_1, что $\|B_m - B\| < \varepsilon/3$ для всех натуральных $m > M_1$. Рассмотрим разность $C_m - D_m$:

$$C_m - D_m = \frac{1}{m}\sum_{i=1}^{m} A_i(B_i - B) = \frac{1}{m}\sum_{i=1}^{M_1} A_i(B_i - B) + \frac{1}{m}\sum_{i=M_1+1}^{m} A_i(B_i - B).$$

Пусть матрица T определена равенством

$$T = \sum_{i=1}^{M_1} A_i(B_i - B).$$

Заметим, что матрица T не зависит от m. Используя свойства нормы из замечания 1.9, получаем оценку

$$\begin{aligned}\|C_m - D_m\| &\leqslant \left\|\frac{1}{m}\sum_{i=1}^{M_1} A_i(B_i - B)\right\| + \left\|\frac{1}{m}\sum_{i=M_1+1}^{m} A_i(B_i - B)\right\| \leqslant \\ &\leqslant \frac{1}{m}\|T\| + \frac{1}{m}\sum_{i=M_1+1}^{m} \|A_i(B_i - B)\| \leqslant \frac{1}{m}\|T\| + \frac{1}{m}\sum_{i=M_1+1}^{m} \|A_i\|\,\|B_i - B\| \leqslant \\ &\leqslant \frac{1}{m}\|T\| + \frac{1}{m}\sum_{i=M_1+1}^{m} \|B_i - B\| \leqslant \frac{1}{m}\|T\| + \frac{1}{m}\left((m - M_1)\frac{\varepsilon}{3}\right) < \frac{1}{m}\|T\| + \frac{\varepsilon}{3}.\end{aligned}$$

При получении данной оценки существенно использован тот факт, что матрицы A_i стохастические, а значит, согласно лемме 3.5 выполнено равенство $\|A_i\| = 1$. Поскольку последовательность C_m сходится к матрице C, найдётся такое натуральное число M_2, что $\|C_m - C\| < \varepsilon/3$ для всех натуральных $m > M_2$. Также очевидно, что найдётся такое натуральное число M_3, что для всех натуральных $m > M_3$ справедливо $(1/m)\|T\| < \varepsilon/3$, т. е. $m > 3\|T\|/\varepsilon$.

Возьмём теперь любое $m > \max(M_1, M_2, M_3)$. Тогда

$$\|D_m - C\| = \|(D_m - C_m) + (C_m - C)\| \leqslant \|C_m - D_m\| + \|C_m - C\| < \frac{\varepsilon}{3} + \frac{\varepsilon}{3} + \frac{\varepsilon}{3} = \varepsilon,$$

поэтому последовательность D_m сходится к матрице C. Утверждение доказано. □

Лемма 4.12. *Пусть $\{A_i\}$ — последовательность матриц, B — матрица. Пусть последовательность A_iB сходится к обратимой матрице C. Тогда матрица B обратима.*

Доказательство. Пусть утверждение леммы неверно и матрица B не является обратимой. Тогда найдётся вектор $v \neq 0$, такой что $Bv = 0$. Поскольку последовательность A_iB сходится к матрице C, для любого $\varepsilon > 0$ существует натуральное число N, такое что $\|A_nB - C\| < \varepsilon$ для любых натуральных $n > N$. Пусть $n > N$. Тогда

$$\|(A_nB - C)v\| \leqslant \|A_nB - C\|\,\|v\| < \varepsilon\|v\|$$

по свойству нормы. С другой стороны,

$$\|(A_nB - C)v\| = \|A_n(Bv) - Cv\| = \|Cv\|.$$

Так как матрица C обратима, найдётся вектор w, такой что $v = C^{-1}w$. Тогда получаем неравенство $\|Cv\| < \varepsilon\|v\|$, т. е. $\|C^{-1}w\| > \frac{1}{\varepsilon}\|w\|$, что невозможно при $\varepsilon < \frac{1}{\|C^{-1}\|}$. Полученное противоречие показывает, что таких векторов v не существует, что означает, что матрица B обратима. □

Вернёмся к построению эффективной политики сканирования. Следующий результат является одним из ключевых в области исследования возможности построения эффективных политик сканирования.

Теорема 4.13. *Пусть последовательность S_m сходится к обратимой матрице. Пусть также сходится последовательность $B_t = Q_{i_{t-1}} \dots Q_{i_1}$ и последовательность I содержит каждый из сигналов $x_1, \dots, x_k$ бесконечное число раз. Тогда все матрицы переходов вероятностного автомата $\{Q_i\}_{i=1}^k$ являются единичными матрицами, т. е. вероятностный автомат является вырожденным.*

Доказательство. Рассмотрим последовательность $A_t = Y_{i_t}$. Согласно лемме 2.5 данная последовательность состоит из стохастических матриц. Пусть последовательность B_t сходится к матрице B, последовательность S_m сходится к обратимой матрице S. Как нетрудно видеть из построения матриц S_m, выполнено равенство

$$S_m = \frac{1}{m}\sum_{t=1}^{m} A_tB_t.$$

Рассмотрим последовательность

$$T_m = \left(\frac{1}{m}\sum_{t=1}^{m} A_t\right)B.$$

Согласно лемме 4.11 последовательность T_m сходится к матрице S. Значит, учитывая, что по условию теоремы матрица S обратима, и применяя к последовательности T_m лемму 4.12, получаем, что матрица B является обратимой.

Но тогда в силу следствия 3.42 получаем, что для любого $i = \overline{1,k}$ любой вектор является собственным вектором матрицы Q_i со значением 1 (так как матрица B обратима, то её образ есть всё пространство $\mathbb{C}^n$), что означает, что матрица Q_i является единичной. □

Таким образом, мы видим, что существование предела последовательности $Q_{i_{t-1}} \dots Q_{i_1}$, с одной стороны, является «хорошим» знаком, поскольку это означает, что распределение состояний вероятностного автомата стабилизируется во времени, но, с другой стороны, в силу теоремы 4.13 это означает, что в этом случае построение эффективной политики сканирования невозможно.

Приведённые выше утверждения показывают, что построить эффективную политику сканирования достаточно сложно и не всегда возможно. Именно поэтому на практике для проведения эффективного сканирования и анализа защищённости учитывают многие неформализуемые эмпирические соображения.

Литература

[1] Бухараев Р. Г. Основы теории вероятностных автоматов. — М.: Наука, 1985.

[2] Гантмахер Ф. Р. Теория матриц. — М.: Наука, 1966.

[3] Маркус М., Минк Х. Обзор по теории матриц и матричных неравенств. — М.: Едиториал УРСС, 2004.

[4] Ширяев А. Н. Вероятность-1. Вероятность-2. — М.: МЦНМО, 2004.

[5] Bru R., Elsner L., Neumann M. Convergence of infinite products of matrices and inner-outer iteration schemes // Electron. Trans. Numer. Anal. — 1994. — Vol. 2. — P. 183—193.