Научная статья
УДК 004.056.5; 004.822; DOI: 10.61260/2218-13X-2025-2-102-115

РАЗРАБОТКА ДИСКРЕТНОЙ МОДЕЛИ ОЦЕНКИ ЭФФЕКТИВНОСТИ ФУНКЦИОНИРОВАНИЯ ЗНАЧИМЫХ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ В УСЛОВИЯХ ИНФРАСТРУКТУРНОГО ДЕСТРУКТИВИЗМА

✉**Долженков Сергей Сергеевич;**
Максимова Елена Александровна.
МИРЭА – Российский технологический университет, Москва, Россия
✉***dolzhenkov@mirea.ru***

Аннотация. Представлены результаты исследования в области оценки эффективности функционирования значимых объектов критической информационной инфраструктуры в условиях инфраструктурного деструктивизма с применением разработанной универсальной дискретной Q-модели, основанной на вычислениях узлов цепей Маркова. Эффективным функционированием значимых объектов считается такое состояние системы, при котором значение показателя инфраструктурного деструктивизма находится в допустимом диапазоне. Разработанная модель исследована в условиях инфраструктурного деструктивизма в частных ситуациях с дифференцированным количеством эффективно функционирующих объектов. По результатам установлены новые закономерности моделирования оценки эффективности функционирования объектов критической информационной инфраструктуры. Значение показателя инфраструктурного деструктивизма служит индикатором эффективности функционирования объектов, то есть данный показатель и разработанную модель оценки можно использовать в качестве элемента в системе управления информационной безопасностью.

Ключевые слова: межобъектное взаимодействие, инфраструктурный деструктивизм, объект критической информационной инфраструктуры, дискретная Q-модель, уязвимости программного кода, цепи Маркова, эффективное функционирование

Для цитирования: Долженков С.С., Максимова Е.А. Разработка дискретной модели оценки эффективности функционирования значимых объектов критической информационной инфраструктуры в условиях инфраструктурного деструктивизма // Науч.-аналит. журн. «Вестник С.-Петерб. ун-та ГПС МЧС России». 2025. № 2. С. 102–115. DOI: 10.61260/2218-13X-2025-2-102-115.

Scientific article

DEVELOPMENT OF A DISCRETE MODEL FOR ASSESSING THE EFFICIENCY OF FUNCTIONING OF SIGNIFICANT OBJECTS OF CRITICAL INFORMATION INFRASTRUCTURE IN THE CONDITIONS OF INFRASTRUCTURE DESTRUCTIVISM

✉**Dolzhenkov Sergey S.;**
Maksimova Elena A.
MIREA – Russian technological university, Moscow, Russia
✉***dolzhenkov@mirea.ru***

Abstract. The article presents the results of a study in the field of assessing the efficiency of functioning of significant objects of critical information infrastructure under conditions of infrastructural destructiveness using the developed universal discrete Q-model based on calculations of Markov chain nodes.

The efficient functioning of significant objects is considered to be such a state of the system in which the value of the indicator of infrastructural destructiveness is in the acceptable range. The developed model was studied under conditions of infrastructural destructiveness in special cases with a differentiated number of effectively functioning objects. Based on the results, new patterns were established in modeling the assessment of the efficiency of functioning of critical information infrastructure objects. The value of the indicator of infrastructural destructiveness serves as an indicator of the efficiency of functioning of objects, that is, this indicator and the developed assessment model can be used as an element in the information security management system.

Keywords: inter-object interaction, infrastructural destructiveness, critical information infrastructure object, discrete Q-model, program code vulnerabilities, Markov chains, effective functioning

For citation: Dolzhenkov S.S., Maksimova E.A. Development of a discrete model for assessing the effectiveness of the functioning of significant objects of critical information infrastructure in the context of infrastructural destructiveness // Scientific and analytical journal «Vestnik Saint-Petersburg university of State fire service of EMERCOM of Russia». 2025. № 2. P. 102–115. DOI: 10.61260/2218-13X-2025-2-102-115.

Введение

Эффективность функционирования значимых объектов критической информационной инфраструктуры (ОКИИ) определяется множеством показателей, индикаторов и критериев, одним из которых выступает показатель инфраструктурного деструктивизма (ИД).

ИД – результат функционирования критической информационной инфраструктуры (КИИ) при активных межобъектных и межсубъектных связях определенного характера, выявление феномена саморазрушения субъекта критической информационной инфраструктуры (СКИИ) как системы [1]. Явление ИД порождается деструктивным воздействием (ДВ) внутри системы от реализации взаимодействия объектов внутри неё. В случае КИИ ИД проявляется на СКИИ от активного взаимодействия его ОКИИ: информационных систем, автоматизированных систем управления и информационно-телекоммуникационных сетей [2].

На рис. 1 изображена среда СКИИ, в которой функционируют два ОКИИ с потенциальными угрозами на уровне программного кода [3]. В результате ДВ угроз инфраструктурного генеза (ИГ) происходит явление ИД.

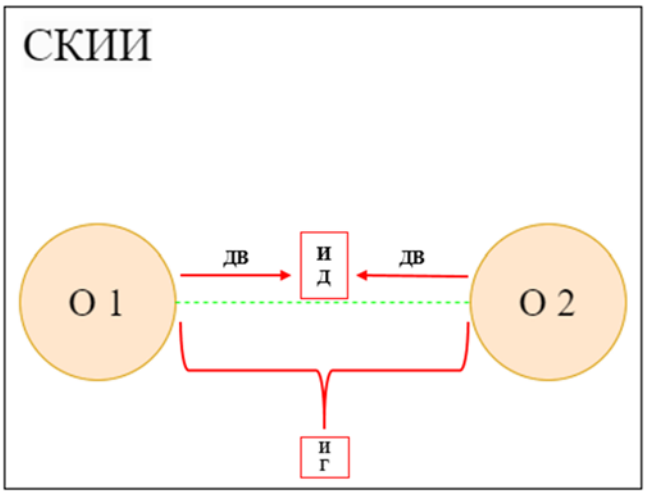

Рис. 1. **Схема зарождения ИД**

Принимая во внимание актуальность поддержания эффективности функционирования ОКИИ необходимо учитывать показатель ИД и удерживать его в допустимом диапазоне [4]. Таким образом, минимальное значение диапазона – практически полное устранение явления ИД –

повлечет за собой существенные затраты на инвестиции в систему управления информационной безопасностью, что является не самым выгодным вложением для коммерческих компаний [5]. Максимальное значение диапазона обусловлено полным игнорированием показателя ИД, последствием которого может стать полное саморазрушении СКИИ как системы. Допуск такого сценария невозможен [6].

Универсальная модель

Для определения значения ИД разработана универсальная дискретная Q-модель (рис. 2), основанная на вычислении звеньев цепи Маркова с заданными параметрами. Она принимает на вход следующие данные: матрица перехода системы в состояние за один шаг (A), вектор начальных вероятностей (P_0) – стартовая точка нахождения системы на нулевом шаге, количество шагов (n) [7]. Элементами модели (Sn) являются случаи, когда количество ОКИИ, равное n, функционирует эффективно, то есть общее состояние системы выше предела инфраструктурного деструктивизма [8].

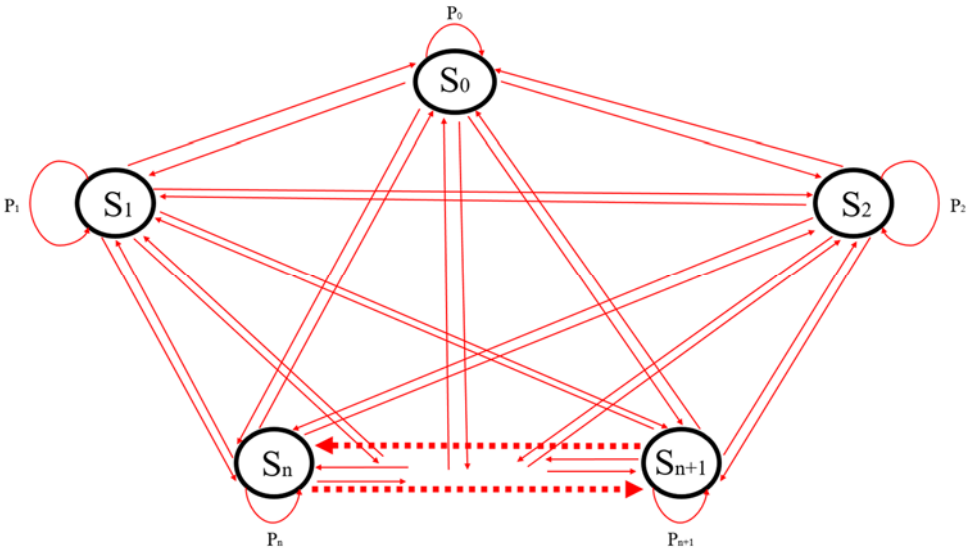

Рис. 2. **Универсальная дискретная Q-модель**

Для формализации разработанной модели введены обозначения:
A – матрица перехода системы в состояние за один шаг (1);
n – количество шагов перехода системы;
P_0 – вектор начальных вероятностей на нулевом шаге.

$$A = \begin{bmatrix} A11 & \cdots & A1i \\ \vdots & \ddots & \vdots \\ Ai1 & \cdots & Aij \end{bmatrix} \quad (1)$$

Если в каждой строке содержатся вероятности событий, которые образуют полную группу, то сумма элементов каждой строки матрицы равна единице:

$$\sum_{j=1}^{N} A_{ij}(n) = 1.$$

Вероятности состояния системы за n шагов определяются произведением матрицы перехода A на вектор начальных вероятностей P_0 [9]:

$$(P_1 = P_0 \times A;\ P_2 = P_1 \times A;\ P_n = P_{n-1} \times A);\ (A_m = A^n;\ P_n = P_0 \times A^n).$$

Частное моделирование

Далее рассмотрены частные ситуации функционирования значимых ОКИИ в зависимости от количества эффективно функционирующих объектов:

1. S_1 – только один объект функционирует эффективно.
2. S_2 – только два объекта функционируют эффективно.
3. S_3 – три объекта функционируют эффективно.
4. S_4 – все объекты функционируют эффективно [10].

Частная ситуация 1. Только один объект функционирует эффективно.

Рассматриваемая ситуация подразумевает два состояния системы – ни один из объектов не функционирует эффективно (S_0), один объект функционирует эффективно (S_1) (рис. 3).

Рис. 3. **Общий вид всевозможных связей функционирования одного объекта**

Формализация частной ситуации функционирования одного объекта имеет следующий вид:

$$A = \begin{pmatrix} 0.25 & 0.75 \\ 0.15 & 0.85 \end{pmatrix}.$$

На рис. 4 изображен частный вид функционирования одного объекта с учетом матрицы перехода системы.

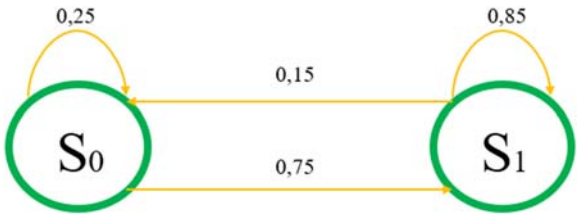

Рис. 4. **Частный вид функционирования одного объекта**

$P_0 = (1, 0)$ – вектор начальных вероятностей. В табл. 1 приведен вектор вероятности функционирования одного объекта за пять шагов.

Таблица 1

Вектор вероятности перехода за пять шагов функционирования одного объекта

Шаг	S_0	S_1	Переход
P_0	1	0	Вектор начальных вероятностей
P_1	0,25	0,75	$P_0 \times A = P_0 \times A^1$
P_2	0,175	0,825	$P_1 \times A = P_0 \times A^2$
P_3	0,1675	0,8325	$P_2 \times A = P_0 \times A^3$
P_4	0,1667	0,8333	$P_3 \times A = P_0 \times A^4$
P_5	0,1667	0,8333	$P_4 \times A = P_0 \times A^5$

На рис. 5 представлен график вероятностей перехода системы из одного объекта за пять шагов. Визуализирована вероятность нахождения системы в точках с учетом вектора начальных вероятностей.

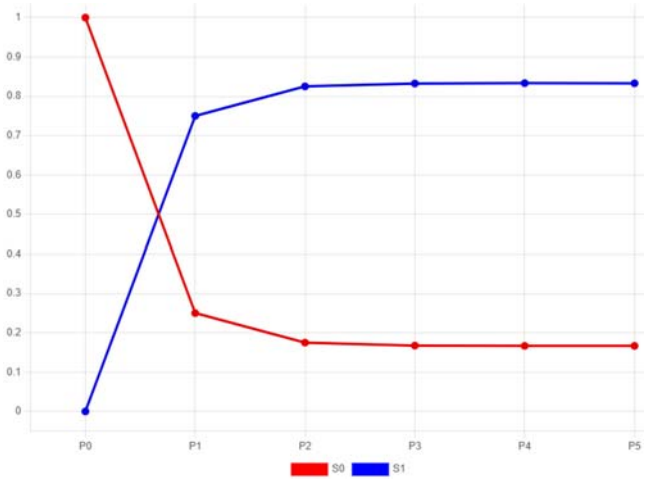

Рис. 5. **График вероятностей перехода системы из одного объекта за пять шагов**

Частная ситуация 2. Два объекта функционируют эффективно.

Рассматриваемая ситуация подразумевает три состояния системы: ни один из объектов не функционирует эффективно (S_0), один объект функционирует эффективно (S_1), два объекта функционируют эффективно (S_2) (рис. 6).

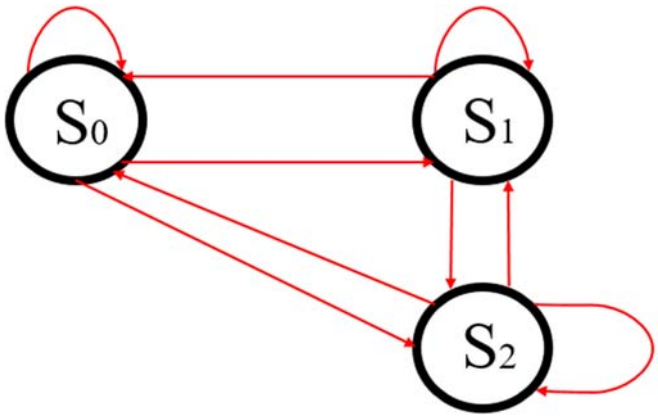

Рис. 6. **Общий вид всевозможных связей функционирования двух объектов**

Формализация частной ситуации функционирования двух объектов имеет следующий вид:

$$A = \begin{pmatrix} 0.25 & 0.75 & 0 \\ 0.15 & 0.3 & 0.55 \\ 0.2 & 0.45 & 0.35 \end{pmatrix}.$$

На рис. 7 изображен частный вид функционирования двух объектов с учетом матрицы перехода системы.

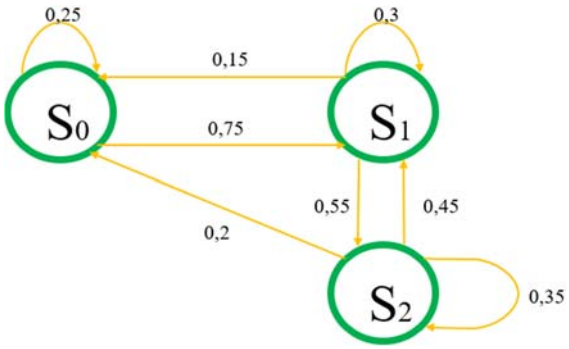

Рис. 7. **Частный вид функционирования двух объектов**

$P_0 = (1, 0, 0)$ – вектор начальных вероятностей. В табл. 2 приведен вектор вероятности функционирования двух объектов за пять шагов.

Таблица 2

Вектор вероятности перехода за пять шагов функционирования двух объектов

Шаг	S_0	S_1	S_2	Переход
P_0	1	0	0	Вектор начальных вероятностей
P_1	0,25	0,75	0	$P_0 \times A = P_0 \times A^1$
P_2	0,175	0,4125	0,4125	$P_1 \times A = P_0 \times A^2$
P_3	0,1881	0,4406	0,3712	$P_2 \times A = P_0 \times A^3$
P_4	0,1874	0,4403	0,3723	$P_3 \times A = P_0 \times A^4$
P_5	0,1874	0,4402	0,3725	$P_4 \times A = P_0 \times A^5$

На рис. 8 представлен график вероятностей перехода системы из двух объектов за пять шагов. Визуализирована вероятность нахождения системы в точках с учетом вектора начальных вероятностей.

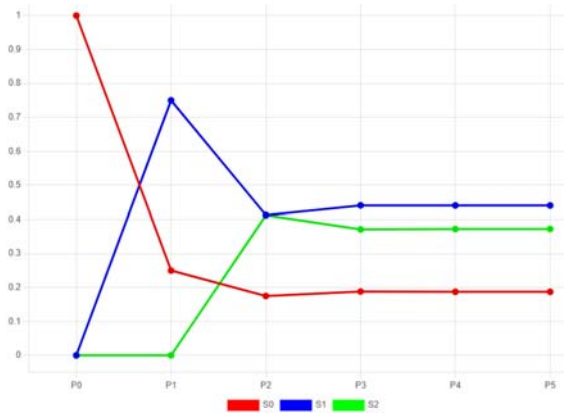

Рис. 8. **График вероятностей перехода системы из двух объектов за пять шагов**

Частная ситуация 3. Три объекта функционируют эффективно.

Рассматриваемая ситуация подразумевает четыре состояния системы: ни один из объектов не функционирует эффективно (S_0), один объект функционирует

эффективно (S_1), два объекта функционируют эффективно (S_2) и три объекта функционируют эффективно (S_3) (рис. 9).

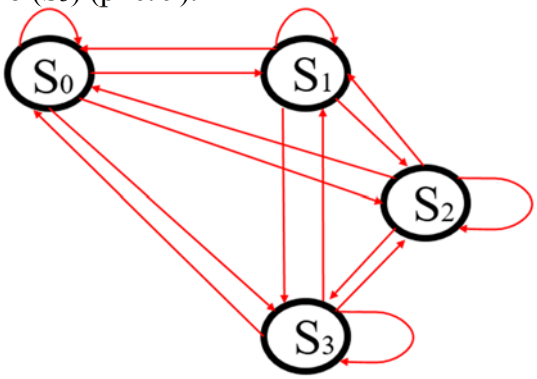

Рис. 9. **Общий вид всевозможных связей функционирования трёх объектов**

Формализация частной ситуации функционирования трёх объектов имеет следующий вид:

$$A = \begin{pmatrix} 0.25 & 0.75 & 0 & 0 \\ 0.15 & 0.3 & 0.55 & 0 \\ 0.1 & 0.45 & 0.35 & 0.1 \\ 0.15 & 0 & 0.15 & 0.7 \end{pmatrix}.$$

На рис. 10 изображен частный вид функционирования трёх объектов с учетом матрицы перехода системы.

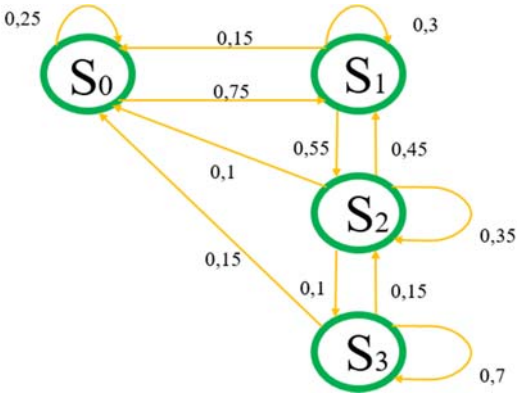

Рис. 10. **Частный вид функционирования трёх объектов**

P_0 = (1, 0, 0, 0) – вектор начальных вероятностей. В табл. 3 приведен вектор вероятности функционирования трёх объектов за пять шагов.

Таблица 3

Вектор вероятности перехода за пять шагов функционирования трёх объектов

Шаг	S_0	S_1	S_2	S_3	Переход
P_0	1	0	0	0	Вектор начальных вероятностей
P_1	0,25	0,75	0	0	$P_0 \times A = P_0 \times A^1$
P_2	0,175	0,4125	0,4125	0	$P_1 \times A = P_0 \times A^2$
P_3	0,1469	0,4406	0,3712	0,0413	$P_2 \times A = P_0 \times A^3$
P_4	0,1461	0,4094	0,3785	0,066	$P_3 \times A = P_0 \times A^4$
P_5	0,1457	0,4027	0,3675	0,084	$P_4 \times A = P_0 \times A^5$

На рис. 11 представлен график вероятностей перехода системы из трёх объектов за пять шагов. Визуализирована вероятность нахождения системы в точках с учетом вектора начальных вероятностей.

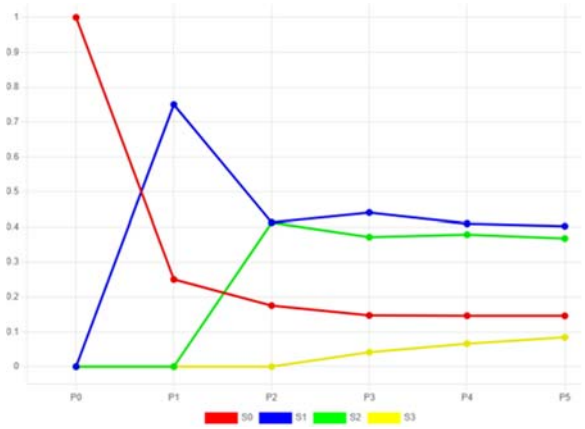

Рис. 11. **График вероятностей перехода системы из трёх объектов за пять шагов**

Частная ситуация 4. Четыре объекта функционируют эффективно.

Рассматриваемая ситуация подразумевает пять состояний системы: ни один из объектов не функционирует эффективно (S_0), один объект функционирует эффективно (S_1), два объекта функционируют эффективно (S_2), три объекта функционируют эффективно (S_3), четыре объекта функционируют эффективно (S_4) (рис. 12).

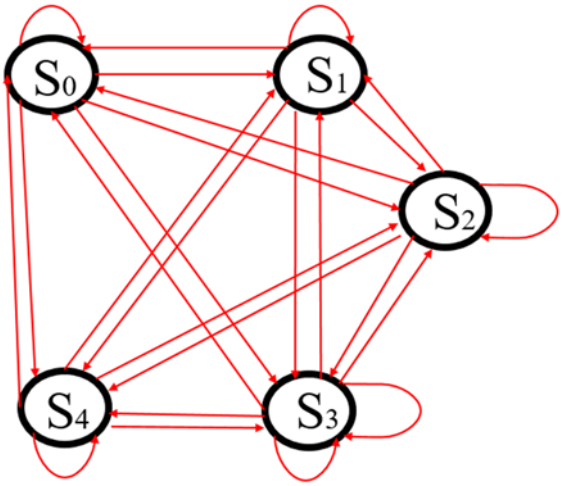

Рис. 12. **Общий вид всевозможных связей функционирования четырёх объектов**

Формализация частной ситуации функционирования четырёх объектов имеет следующий вид:

$$A = \begin{pmatrix} 0.2 & 0.7 & 0 & 0 & 0.1 \\ 0.15 & 0.3 & 0.55 & 0 & 0 \\ 0.1 & 0.45 & 0.35 & 0.1 & 0 \\ 0.15 & 0 & 0.15 & 0.6 & 0.1 \\ 0.2 & 0 & 0 & 0.3 & 0.5 \end{pmatrix}.$$

На рис. 13 изображен частный вид функционирования четырех объектов с учетом матрицы перехода системы.

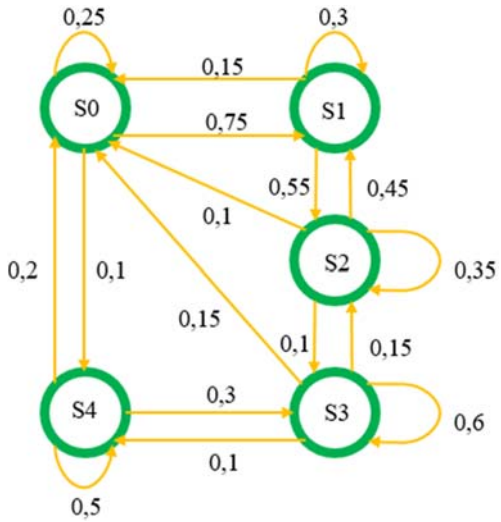

Рис. 13. **Частный вид функционирования четырех объектов**

P_0 = (1, 0, 0, 0, 0) – вектор начальных вероятностей. В табл. 4 приведен вектор вероятности функционирования четырех объектов за 5 шагов.

Таблица 4

Вектор вероятности перехода за пять шагов функционирования четырёх объектов

Шаг	S_0	S_1	S_2	S_3	S_4	Переход
P_0	1	0	0	0	0	Вектор начальных вероятностей
P_1	0,2	0,7	0	0	0,1	$P_0 \times A = P_0 \times A^1$
P_2	0,165	0,35	0,385	0,03	0,07	$P_1 \times A = P_0 \times A^2$
P_3	0,1425	0,3938	0,3318	0,0775	0,0545	$P_2 \times A = P_0 \times A^3$
P_4	0,1433	0,3672	0,3443	0,096	0,0493	$P_3 \times A = P_0 \times A^4$
P_5	0,1424	0,3654	0,3368	0,1068	0,0486	$P_4 \times A = P_0 \times A^5$

На рис. 14 представлен график вероятностей перехода системы из четырёх объектов за 5 шагов. Визуализирована вероятность нахождения системы в точках с учетом вектора начальных вероятностей.

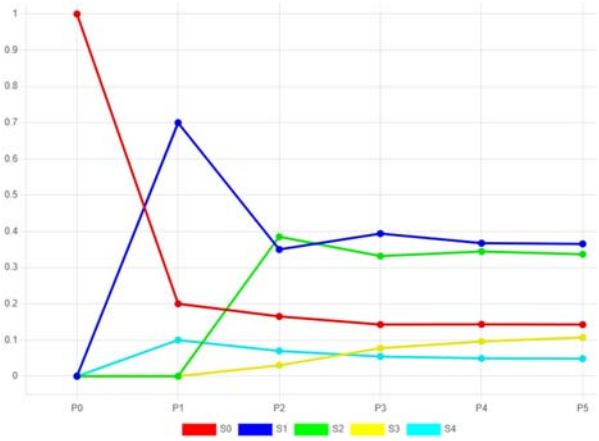

Рис. 14. **График вероятностей перехода системы из четырех объектов за пять шагов**

Метрика инфраструктурного деструктивизма

В настоящее время нет единой метрики оценки ИД инфраструктурного генеза. Аналогичным образом отсутствует практика оценивания эффективности функционирования значимых ОКИИ, в которой отражаются и учитываются значения показателя ИД [11]. Авторами предложена собственная метрика, основанную на матрице перехода системы и векторе вероятности перехода [12].

Для апробирования модели выделены следующие значимые ОКИИ в условиях ИД и их соответствие состояниям на узлах цепей Маркова из Частной ситуации 4 (табл. 5).

Таблица 5

Значимые ОКИИ в условиях ИД

Значимый ОКИИ	S_0	S_1	S_2	S_3	S_4
Информационно – телекоммуникационная сеть предприятия	–	+	+	+	+
Автоматизированная система управления и учета клиентов предприятия	–	–	+	+	+
Информационная система работы с документами отдела кадров	–	–	–	+	+
Информационная система работы с документами бухгалтерии	–	–	–	–	+
Комментарий	Ни один из объектов не функц. эффективно	Только один объект в системе функц. эффективно	Только два объекта в системе функц. эффективно	Только три объекта в системе функц. эффективно	Все объекты функц. эффективно

Удержание положительного состояния S_4 требует работы экспертной группы или дополнительных исследований.

Метрика оценки ИД (Метрика) может быть записана следующим образом:

$$M = \sum_{P0}^{Pn} Sn,$$

где S_n – оптимальное состояние системы, P_0 и P_n – сумма вероятностей за все шаги перехода системы [13].

Предлагаемое решение

Из вышеизложенного следует гипотеза: для эффективного функционирования значимых ОКИИ показатель ИД должен находиться в оптимальном (умеренном) значении возможного диапазона. Качественная метрика показателя ИД представлена в табл. 6 [14].

Таблица 6

Качественная метрика показателя ИД

Значение ИД	0,15–0,24	0,25–0,48	0,49–0,74	0,75–0,99
Показатель	Минимальный	Умеренный	Высокий	Максимальный

Предположим, что в рамках одного субъекта функционируют четыре ОКИИ посредством обмена данными: бухгалтерские отчеты, данные отпусков сотрудников для отдела кадров и конфиденциальная информация, например, коммерческая. В таком сценарии вероятны сбои информационных потоков, несанкционированный доступ. Как в большинстве случаев ОКИИ представляют собой микросервисы, связанные общим сервером и базами данных [15].

В результате Метрика представляется в следующем виде:

$$\mathrm{M} = \sum_{P0}^{P5} S4 = 0.33.$$

Анализируя полученное значение показателя ИД можно говорить об эффективном функционировании объектов, поскольку оно является умеренным. Умеренный показатель говорит о том, что система работает эффективно и в ближайшее время не потребует инвестиций в обслуживание или модернизацию. Более того, есть небольшой запас «прочности» вплоть до значения показателя 0,48 [16].

Заключение

Разработанная модель подтверждает гипотезу об оценке эффективного функционирования значимых ОКИИ посредством показателя ИД. Нахождение значения показателя ИД при помощи цепей Маркова обосновывает актуальность и востребованность применения дискретной Q-модели. Рассмотренные в работе частные ситуации можно использовать в дальнейшем изучении эффективного функционирования объектов в условиях ИД [17].

Кроме того, возможно использование разработанной дискретной модели оценки эффективности в модернизации системы управления рисками информационной безопасности: учет значения показателя ИД в планировании инвестиционной политики информационной безопасности организации, что благоприятно скажется на деятельности любой коммерческой компании [18].

Применение оценки эффективности объектов, основанной на значении показателя ИД, оказалось достаточно удачным – как для типизации, так и для его интерпретации человеком.

Предложенная формализация показала свою жизнеспособность, хотя для полноценного математического аппарата необходимы дополнительные исследования и подходы вне сферы информационной безопасности.

Список источников

1. Максимова Е.А. Модели и методы оценки информационной безопасности субъекта критической информационной инфраструктуры при деструктивных воздействиях инфраструктурного генеза: дисс. ... д-ра техн. наук. М., 2022. 448 с.

2. Федеральный закон Российской Федерации от 2 июля 2013 г. № 187-ФЗ // Патенты и лицензии. Интеллектуальные права. 2013. № 8. С. 60–65.

3. Долженков С.С., Максимова Е.А. Исследование антропоморфических видов организации межобъектного взаимодействия на уровне субъекта критической информационной инфраструктуры // Науч.-аналит. журн. «Вестник С.-Петерб. ун-та ГПС МЧС России». 2025. № 1. С. 94–108. DOI: 10.61260/2218-130X-2025-1-94-108.

4. Долженков С.С., Максимова Е.А. Риск-менеджмент, как средство реализации методологии поддержки процессов управления информационной безопасностью субъектов критической информационной инфраструктуры при деструктивных воздействиях инфраструктурного генеза // Актуальные проблемы прикладной математики, информатики и механики: сб. трудов Междунар. науч. конф. Воронеж, 2023. С. 1538–1539.

5. Долженков С.С. Оптимизация системы менеджмента информационной безопасности объектов критической информационной инфраструктуры // Студенческая наука для развития информационного общества: материалы XX Всерос. науч.-техн. конф. Ставрополь, 2023. С. 124–130. EDN EYGAVD.

6. Taneski V., Heričko M., Brumen B. Impact of security education on password change // 38th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO). 2015. P. 1350–1355.

7. Куркчи М.В., Доронина Ю.В. Анализ достоверности имитационной модели технической системы на основе цепи Маркова // Интеллектуальные информационные системы: сб. трудов Междунар. науч.-практ. конф. Воронеж, 2019 г. С. 35–39.

8. Castro J.L., Delgado M. Fuzzy systems with defuzzification are universal approximators // IEEE Transactions on Systems, Man and Cybernetics. Part B (Cybernetics). 1996. Vol. 26. Iss. 1. P. 149–152.

9. Убодоев В.В. Дискретные цепи Маркова // Успехи современной науки и образования. 2016. Т. 7. № 11. С. 96–99.

10. Арикова К.Г., Максимова Е.А. Численное прогнозирование количества DDOS-атак и их мощности // Кибербезопасность: технические и правовые аспекты защиты информации: сб. науч. трудов III Ежегодной национальной науч.-практ. конф. Москва, 2024. С. 258–264.

11. Rinaldi S.M., Peerenboom J.P., Kelly T.K. Identifying, understanding and analyzing critical infrastructure interdependencies // IEEE control systems magazine. 2001. Vol. 21. №. 6. P. 11–25.

12. Modeling Software Vulnerabilities with Vulnerability Cause Graphs / D. Byers [et al.] // 22nd IEEE International Conference on Software Maintenance. 2006. P. 411–422.

13. Marimuthu K., Gopinath M. Production of Sugarcane Forecasting using ARIMAX Model // Scopus. International Journal of Innovative Technology and Exploring Engineering. 2019. Vol. 8. Iss. 12S.

14. Русаков А.М. Комплекс антропоморфических моделей поведенческого анализа процессов для обнаружения эффектов инфраструктурного деструктивизма // Инженерный вестник Дона. 2024. № 11 (119). С. 391–404.

15. Доктрина информационной безопасности Российской Федерации: Указ Президента Рос. Федерации от 05 дек. 2016 г. № 646. Доступ из инф.-правового портала «Гарант».

16. Буйневич М.В., Израилов К.Е. Антропоморфический подход к описанию взаимодействия уязвимостей в программном коде. Часть 2. Метрика уязвимостей // Защита информации. Инсайд. 2019. № 6 (90). С. 61–65.

17. Аналитический обзор методов проектирования систем безопасности в телемедицинских системах / М.А. Лапина [и др.] // Труды Института системного программирования РАН. 2024. Т. 36. № 5. С. 191–218. DOI: 10.15514/ISPRAS-2024-36(5)-14.

18. Retraction Note: Electric power industry development in the Russian Federation considering the structural trends of the world economy / V.V. Bezpalov [et al.] // Environment, Development and Sustainability. 2023. DOI: 10.1007/s10668-023-03999-z.

References

1. Maksimova E.A. Modeli i metody ocenki informacionnoj bezopasnosti sub"ekta kriticheskoj informacionnoj infrastruktury pri destruktivnyh vozdejstviyah infrastrukturnogo geneza: diss. ... d-ra tekhn. nauk. M., 2022. 448 s.

2. Federal'nyj zakon Rossijskoj Federacii ot 2 iyulya 2013 g. № 187-FZ // Patenty i licenzii. Intellektual'nye prava. 2013. № 8. S. 60–65.

3. Dolzhenkov S.S., Maksimova E.A. Issledovanie antropomorficheskih vidov organizacii mezhob"ektnogo vzaimodejstviya na urovne sub"ekta kriticheskoj informacionnoj infrastruktury // Nauch.-analit. zhurn. «Vestnik S.-Peterb. un-ta GPS MCHS Rossii». 2025. № 1. S. 94–108. DOI: 10.61260/2218-130X-2025-1-94-108.

4. Dolzhenkov S.S., Maksimova E.A. Risk-menedzhment, kak sredstvo realizacii metodologii podderzhki processov upravleniya informacionnoj bezopasnost'yu sub"ektov kriticheskoj informacionnoj infrastruktury pri destruktivnyh vozdejstviyah infrastrukturnogo geneza // Aktual'nye problemy prikladnoj matematiki, informatiki i mekhaniki: sb. trudov Mezhdunar. nauch. konf. Voronezh, 2023. S. 1538–1539. EDN DNWVWZ.

5. Dolzhenkov S.S. Optimizaciya sistemy menedzhmenta informacionnoj bezopasnosti ob"ektov kriticheskoj informacionnoj infrastruktury // Studencheskaya nauka dlya razvitiya informacionnogo obshchestva: materialy HX Vseros. nauch.-tekhn. konf. Stavropol', 2023. S. 124–130. EDN EYGAVD.

6. Taneski V., Heričko M., Brumen B. Impact of security education on password change // 38th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO). 2015. P. 1350–1355.

7. Kurkchi M.V., Doronina Yu.V. Analiz dostovernosti imitacionnoj modeli tekhnicheskoj sistemy na osnove cepi Markova // Intellektual'nye informacionnye sistemy: sb. trudov Mezhdunar. nauch.-prakt. konf. Voronezh, 2019 g. S. 35–39.

8. Castro J.L., Delgado M. Fuzzy systems with defuzzification are universal approximators // IEEE Transactions on Systems, Man and Cybernetics. Part B (Cybernetics). 1996. Vol. 26. Iss. 1. P. 149–152.

9. Ubodoev V.V. Diskretnye cepi Markova // Uspekhi sovremennoj nauki i obrazovaniya. 2016. T. 7. № 11. S. 96–99.

10. Arikova K.G., Maksimova E.A. Chislennoe prognozirovanie kolichestva DDOS-atak i ih moshchnosti // Kiberbezopasnost': tekhnicheskie i pravovye aspekty zashchity informacii: sb. nauch. trudov III Ezhegodnoj nacional'noj nauch.-prakt. konf. Moskva, 2024. S. 258–264.

11. Rinaldi S.M., Peerenboom J.P., Kelly T.K. Identifying, understanding and analyzing critical infrastructure interdependencies // IEEE control systems magazine. 2001. Vol. 21. №. 6. P. 11–25.

12. Modeling Software Vulnerabilities with Vulnerability Cause Graphs / D. Byers [et al.] // 22nd IEEE International Conference on Software Maintenance. 2006. P. 411–422.

13. Marimuthu K., Gopinath M. Production of Sugarcane Forecasting using ARIMAX Model // Scopus. International Journal of Innovative Technology and Exploring Engineering. 2019. Vol. 8. Iss. 12S.

14. Rusakov A.M. Kompleks antropomorficheskih modelej povedencheskogo analiza processov dlya obnaruzheniya effektov infrastrukturnogo destruktivizma // Inzhenernyj vestnik Dona. 2024. № 11 (119). S. 391–404.

15. Doktrina informacionnoj bezopasnosti Rossijskoj Federacii: Ukaz Prezidenta Ros. Federacii ot 05 dek. 2016 g. № 646. Dostup iz inf.-pravovogo portala «Garant».

16. Bujnevich M.V., Izrailov K.E. Antropomorficheskij podhod k opisaniyu vzaimodejstviya uyazvimostej v programmnom kode. Chast' 2. Metrika uyazvimostej // Zashchita informacii. Insajd. 2019. № 6 (90). S. 61–65.

17. Analiticheskij obzor metodov proektirovaniya sistem bezopasnosti v telemedicinskih sistemah / M.A. Lapina [i dr.] // Trudy Instituta sistemnogo programmirovaniya RAN. 2024. T. 36. № 5. S. 191–218. DOI: 10.15514/ISPRAS-2024-36(5)-14.

18. Retraction Note: Electric power industry development in the Russian Federation considering the structural trends of the world economy / V.V. Bezpalov [et al.] // Environment, Development and Sustainability. 2023. DOI: 10.1007/s10668-023-03999-z.

Информация о статье:
Статья поступила в редакцию: 14.02.2025; одобрена после рецензирования: 01.04.2025; принята к публикации: 05.04.2025
Information about the article:
The article was submitted to the editorial office: 14.02.2025; approved after review: 01.04.2025; accepted for publication: 05.04.2025

Информация об авторах:
Долженков Сергей Сергеевич, аспирант кафедры КБ-4 «Интеллектуальные системы информационной безопасности» института кибербезопасности и цифровых технологий МИРЭА – Российского технологического университета (119454, Москва, пр. Вернадского, д. 78), e-mail: dolzhenkov@mirea.ru, https://orcid.org/0009-0004-8621-3994, SPIN-код: 1759- 7373
Максимова Елена Александровна, заведующий кафедрой КБ-4 «Интеллектуальные системы информационной безопасности» института кибербезопасности и цифровых технологий МИРЭА – Российского технологического университета (119454, Москва, пр. Вернадского, д. 78, стр. 4), доктор технических наук, доцент, e-mail: maksimova@mirea.ru, https://orcid.org/0000-0001-8788-4256, SPIN-код: 6876-5558

Information about authors:
Dolzhenkov Sergey S., postgraduate student of the department KB-4 «Intelligent systems of information security» of the institute of cybersecurity and digital technologies of the MIREA – Russian university of technology (119454, Moscow, Vernadsky ave., 78), e-mail: dolzhenkov@mirea.ru, https://orcid.org/0009-0004-8621-3994, SPIN: 1759-7373
Maksimova Elena A., head of the department KB-4 «Intelligent systems of information security» of the institute of cybersecurity and digital technologies of the MIREA – Russian university of technology (119454, Moscow, Vernadsky ave., 78), doctor of technical sciences, associate professor, e-mail: maksimova@mirea.ru, https://orcid.org/0000-0001-8788-4256, SPIN: 6876-5558