Инженерный вестник Дона, №11 (2021)
ivdon.ru/ru/magazine/archive/n11y2021/7284

Риск пребывания автоматизированной информационной системы специального назначения в критическом состоянии

О.В. Петрова, А.А. Поздняков, А.В. Уваров

Краснодарское высшее военное училище имени генерала армии С.М. Штеменко

Аннотация: В статье авторы предлагают рассмотреть способ оценки риска возможного пребывания автоматизированной информационной системы специального назначения в критическом состоянии в условиях воздействия DDOS-атаки, учитывающий в качестве эмпирической составляющей не только интенсивность нагрузки на систему, но и параметры, используемые в модели системы защиты с полным перекрытием.
Ключевые слова: автоматизированная информационная система, оценка защищенности, система массового обслуживания, риск.

Одной из основных форм формального описания систем защиты традиционно считается модель системы защиты с полным перекрытием, в которой рассматривается взаимодействие «области угроз», «защищаемой области» – области ресурсов автоматизированной информационной системы специального назначения (далее АИС СН), и «системы защиты» – механизмов безопасности автоматизированной информационной системы. Система безопасности должна иметь, по крайней мере, одно средство для обеспечения безопасности на каждом возможном пути воздействия нарушителя на информационную систему. В модели определяется объект, требующий защиты, оцениваются средства обеспечения безопасности и их вклад в обеспечение безопасности всей системы. С каждым объектом, требующим защиты, связывается некоторое множество действий, к которым может прибегнуть нарушитель.

Используя модель оценки защищенности АИС СН в условиях воздействия DDOS-атак, которая обладает основным и резервными каналами, где оценка защищенности вычисляется через вероятностные показатели пребывания системы во множестве реализуемых состояний в результате

осуществления DDOS-атак [1-3], оценим риск ее возможного пребывания в критическом состоянии.

Согласно модели системы защиты с полным перекрытием, множество отношений «объект-угроза» образует двудольный граф, представленный на рисунке 1, в котором ребро (t_i, o_j) существует тогда и только тогда, когда t_i является средством получения доступа к объекту o_j [4].

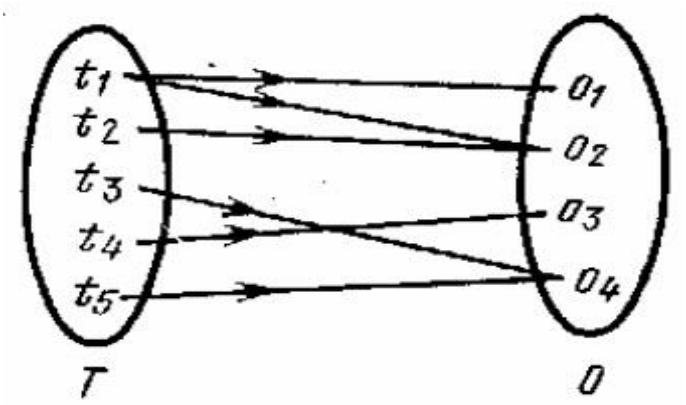

Рис. 1. – Двудольный граф множества отношений «объект-угроза»

Связь между угрозами и объектами не является связью типа «один к одному» — угроза может распространяться на любое число объектов, а объект может быть уязвим со стороны более чем одной угрозы. Цель защиты состоит в том, чтобы «перекрыть» каждое ребро данного графа и воздвигнуть барьер для доступа по этому пути [4].

В идеальном случае каждое средство защиты $m_k \in M$ должно устранять некоторое ребро (t_i, o_j). В действительности m_k выполняет функцию «барьера», обеспечивая некоторую степень сопротивления попыткам проникновения. Набор M средств обеспечения безопасности преобразует двудольный граф в трехдольный, представленный на рисунке 2 [4].

Ребра указывают на соответствующие связи между угрозами, средствами защиты и множеством объектов защиты. Система обеспечения безопасности описывается в виде пятикортежного набора $S = \{O, T, M, V, B\}$, где O — набор защищаемых объектов; T — набор угроз; M — набор средств

обеспечения безопасности; V — набор уязвимых мест — отображение T×O на набор упорядоченных пар $V_i = (t_i, o_j)$, представляющих собой пути проникновения в систему; B — набор барьеров — отображение $V \times M$ или $T \times O \times M$ на набор упорядоченных троек $b_i = (t_i, o_j, m_k)$, представляющих собой точки, в которых требуется осуществлять защиту в системе [4].

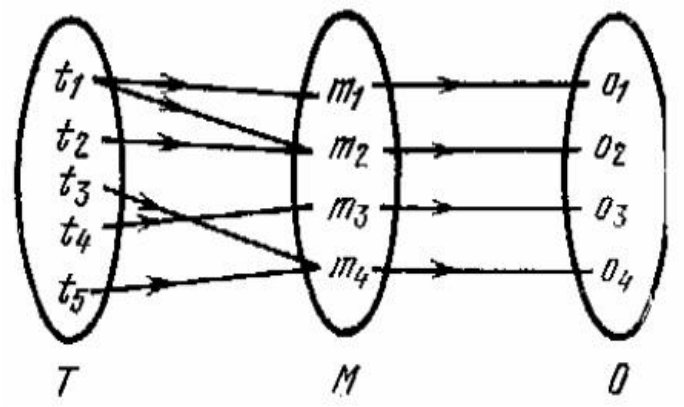

Рис. 2. – Трехдольный граф множества отношений «объект-средство обеспечения безопасности-угроза»

В идеале каждый механизм защиты должен исключать соответствующий путь реализации угрозы $V_i = (t_i, o_j)$. В действительности механизмы защиты обеспечивают лишь некоторую степень сопротивляемости угрозам безопасности. В связи с этим, в качестве характеристик элемента набора барьеров $b_i = (t_i, o_j, m_k)$ может рассматриваться (Z_i, L_i, R_i), где

Z_i – вероятность появления угрозы;

L_i – величина ущерба при удачном осуществлении угрозы в отношении защищаемых объектов (уровень серьёзности угрозы);

$1\text{-}R_i$ – степень сопротивляемости механизма защиты m_k, характеризующаяся вероятностью его преодоления [4].

Прочность барьера $b_i = (t_i, o_j, m_k)$ характеризуется величиной риска пребывания автоматизированной информационной системы в незащищенном состоянии $Risk_i$, связанного с возможностью осуществления угрозы

безопасности t_i в отношении объекта АИС СН o_j, при использовании механизма защиты m_k. Эта величина определяется по формуле [4]:

$$Risk_i = Z_i * L_i * (1 - R_i) \ . \quad (1)$$

Рассмотрим модель оценки защищенности АИС СН в условиях воздействия DDOS-атак, которая обладает основным и одним резервным каналом. Оценка защищенности вычисляется через вероятностные показатели пребывания АИС СН после осуществления DDOS-атак в каждом из возможных состояний. Данная модель представлена графом состояний на рисунке 3, где X_0 – свободны все каналы; X_1 – занят первый канал; X_2 – заняты оба канала [1, 2]:

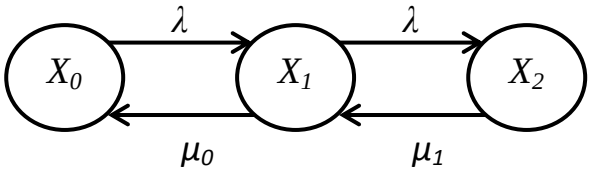

Рис. 3. – Модель оценки защищенности АИС СН с одним резервным каналом

P_0 – вероятность пребывания системы в состоянии X_0, P_1 – в состоянии X_1, P_2 – в состоянии X_2, вычисляемые по формулам [1,3]:

$$P_0 = \frac{\mu_1\mu_0}{\mu_1\mu_0 + \mu_1\lambda + \lambda^2}, \quad (2)$$

$$P_1 = \frac{\mu_1\lambda}{\mu_1\mu_0 + \mu_1\lambda + \lambda^2}, \quad (3)$$

$$P_2 = \frac{\lambda^2}{\mu_1\mu_0 + \mu_1\lambda + \lambda^2}. \quad (4)$$

Рассчитаем значения вероятностей пребывания системы во всех состояниях с учетом изменения значений интенсивности DDOS-атаки при фиксированных значениях интенсивностей обработки заявок всеми

каналами для системы массового облуживания с 1 резервным каналом по формулам (2-4). Результаты представлены в таблице № 1.

Таблица № 1

Вероятности пребывания АИС СН с 1 резервным каналом во всех состояниях

Интенсивность входящего потока	Интенсивность обработки		P_0	P_1	P_2
	1–й канал	2–й канал			
Изменение интенсивности входящего потока					
0,2	0,2	0,2	0,33333	0,33333	0,33333
0,3	0,2	0,2	0,21053	0,31579	0,47368
0,4	0,2	0,2	0,14286	0,28571	0,57143
0,5	0,2	0,2	0,10256	0,25641	0,64103
0,6	0,2	0,2	0,07692	0,23077	0,69231
Изменение интенсивности обработки 1-го канала					
0,2	0,2	0,2	0,33333	0,33333	0,33333
0,2	0,3	0,2	0,42857	0,28571	0,28571
0,2	0,4	0,2	0,5	0,25	0,25
0,2	0,5	0,2	0,55556	0,22222	0,22222
0,2	0,6	0,2	0,6	0,2	0,2
Изменение интенсивности обработки 2-го канала					
0,2	0,2	0,2	0,33333	0,33333	0,33333
0,2	0,2	0,3	0,375	0,375	0,25
0,2	0,2	0,4	0,4	0,4	0,2
0,2	0,2	0,5	0,41667	0,41667	0,16667
0,2	0,2	0,6	0,42857	0,42857	0,14286

Рассмотрим процесс функционирования АИС СН в условиях воздействия DDOS-атак, используя подход модели системы защиты с полным перекрытием, и синтезируем способ оценки риска возможного пребывания АИС СН в критическом состоянии.

Под степенью сопротивляемости механизма защиты m_i, характеризующейся вероятностью его преодоления, будем понимать величину $(1\text{-}R_i)$, равную сумме вероятностей пребывания системы во всех состояниях, предшествующих незащищенному состоянию, что будет соответствовать возможности реализации увеличения интенсивности

атакующих запросов, или увеличению интенсивности DDOS-атаки при условии знания о возможности обработки информации всеми предшествующими каналами, т.е.

$$R_i = .\sum_{0}^{1} P_i = (1 - P_2) . \quad (5)$$

В качестве вероятности появления угрозы Z_i рассмотрим вероятность того, что система массового обслуживания окажется в последнем незащищенном состоянии, т.е. наблюдается критическое состояние работы всей системы.

L_i – величина ущерба при удачном осуществлении угрозы в отношении защищаемых объектов (уровень серьёзности угрозы), определяется специалистами по информационной безопасности в соответствии с критериями оценки, иными словами, данную величину целесообразно определять с помощью экспертных оценок [5, 6]. Подобный подход вносит дополнительный параметр, содержащий неопределенность. В качестве оценки данного параметра можно ввести величину, равную отношению интенсивности потока запросов к среднему геометрическому интенсивности обработки этих запросов каждым каналом:

$$L_i = \frac{\lambda}{\sqrt[2]{\prod_{i=0}^{1} \mu_i}} . \quad (6)$$

Данное отношение изменяется прямо пропорционально интенсивности DDOS-атаки, что подчеркивает важность атакуемого объекта с ростом значения интенсивности запросов, и соответственно обратно пропорционально интенсивности их обработки, которая напрямую зависит от технической реализации каналов.

В данных условиях величину риска пребывания автоматизированной информационной системы в незащищенном состоянии $Risk_i$ при использовании механизма защиты m_i можно вычислить по формуле (1).

В условиях сделанных допущений и предположений, рассмотрим изменение значения параметра риска с учетом изменения значений интенсивности обработки запасных каналов при фиксированном значении потока заявок для системы массового обслуживания с одним резервным каналом. Для этого найдем значения выходных параметров по формулам (5, 6) при расчете с использованием синтезированного способа. Результаты представлены в таблице № 2.

Таблица № 2

Выходные параметры АИС СН с 1 резервным каналом при расчете с использованием предложенного способа

Интенсивность входящего потока	Интенсивность обработки		Z_1	L_1	R_1	$Risk_1$
	1–й канал	2–й канал				
Изменение интенсивности входящего потока						
0,2	0,2	0,2	0,33333	1	0,66667	0,11111
0,3	0,2	0,2	0,47368	1,5	0,52632	0,33657
0,4	0,2	0,2	0,57143	2	0,42857	0,65306
0,5	0,2	0,2	0,64103	2,5	0,35897	1,02728
0,6	0,2	0,2	0,69231	3	0,30769	1,43787
Изменение интенсивности обработки 1-го канала						
0,2	0,2	0,2	0,33333	1	0,66667	0,11111
0,2	0,3	0,2	0,28571	0,8165	0,71429	0,06665
0,2	0,4	0,2	0,25	0,70711	0,75	0,04419
0,2	0,5	0,2	0,22222	0,63246	0,77778	0,03123
0,2	0,6	0,2	0,2	0,57735	0,8	0,02309
Изменение интенсивности обработки 2-го канала						
0,2	0,2	0,2	0,33333	1	0,66667	0,11111
0,2	0,2	0,3	0,25	0,8165	0,75	0,05103
0,2	0,2	0,4	0,2	0,70711	0,8	0,02828
0,2	0,2	0,5	0,16667	0,63246	0,83333	0,01757
0,2	0,2	0,6	0,14286	0,57735	0,85714	0,01178

Теперь рассмотрим модель оценки защищенности АИС СН в условиях воздействия DDOS-атак, которая обладает основным защищенным каналом передачи информации и двумя запасными. Применение трех независимых

каналов повышает информационную связность АИС СН с удаленными пользователями, и, следовательно, доступность АИС СН, устойчивость ее безотказного функционирования. Данной модели соответствует граф состояний, представленный на рисунке 4 [2].

Учитывается следующее допущение – все каналы в системе включаются и освобождаются последовательно, где определены состояния системы: X_0 – свободны все каналы; X_1 – занят первый (основной) канал; X_2 – заняты первые 2 канала (основной и первый резервный); X_3 – заняты все 3 канала (основной и два резервных) [2].

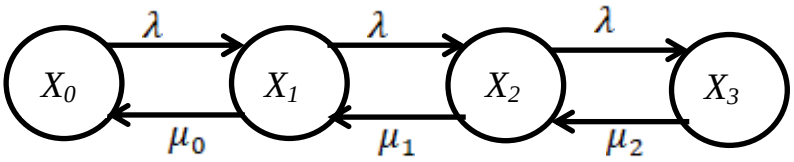

Рис. 4. – Модель оценки защищенности АИС СН с двумя резервными каналами

P_0 – вероятность нахождения системы в состоянии X_0; P_1 – вероятность нахождения системы в состоянии X_1; P_2 – вероятность нахождения системы в состоянии X_2; P_3 – вероятность нахождения системы в состоянии X_3, которые вычисляются по формулам [2, 3]:

$$P_0 = \frac{\mu_0\mu_1\mu_2}{\mu_0\mu_1\mu_2 + \lambda\mu_1\mu_2 + \lambda^2\mu_2 + \lambda^3}, \quad (7)$$

$$P_1 = \frac{\lambda\mu_1\mu_2}{\mu_0\mu_1\mu_2 + \lambda\mu_1\mu_2 + \lambda^2\mu_2 + \lambda^3}, \quad (8)$$

$$P_1 = \frac{\lambda\mu_1\mu_2}{\mu_0\mu_1\mu_2 + \lambda\mu_1\mu_2 + \lambda^2\mu_2 + \lambda^3}, \quad (9)$$

$$P_3 = \frac{\lambda^3}{\mu_0\mu_1\mu_2 + \lambda\mu_1\mu_2 + \lambda^2\mu_2 + \lambda^3}. \quad (10)$$

Рассчитаем значения вероятностей пребывания системы во всех состояниях с учетом изменения значений интенсивности DDOS-атаки для

системы массового обслуживания с двумя резервными каналами по формулам (7-10). Результаты представлены в таблице № 3.

Таблица № 3

Вероятности пребывания АИС СН с 2 резервными каналами во всех состояниях

Интенсивность входящего потока	Интенсивность обработки			P_0	P_1	P_2	P_3
	1–й канал	2–й канал	3–й канал				
Изменение интенсивности входящего потока							
0,2	0,2	0,2	0,2	0,25	0,25	0,25	0,25
0,3	0,2	0,2	0,2	0,12308	0,18462	0,27692	0,41538
0,4	0,2	0,2	0,2	0,06667	0,13333	0,26667	0,53333
0,5	0,2	0,2	0,2	0,03941	0,09852	0,24631	0,61576
0,6	0,2	0,2	0,2	0,025	0,075	0,225	0,675
Изменение интенсивности обработки 1-го канала							
0,2	0,2	0,2	0,2	0,25	0,25	0,25	0,25
0,2	0,3	0,2	0,2	0,33333	0,22222	0,22222	0,22222
0,2	0,4	0,2	0,2	0,4	0,2	0,2	0,2
0,2	0,5	0,2	0,2	0,45455	0,18182	0,18182	0,18182
0,2	0,6	0,2	0,2	0,5	0,16667	0,16667	0,16667
Изменение интенсивности обработки 2-го канала							
0,2	0,2	0,2	0,2	0,25	0,25	0,25	0,25
0,2	0,2	0,3	0,2	0,3	0,3	0,2	0,2
0,2	0,2	0,4	0,2	0,33333	0,33333	0,16667	0,16667
0,2	0,2	0,5	0,2	0,35714	0,35714	0,14286	0,14286
0,2	0,2	0,6	0,2	0,375	0,375	0,125	0,125
Изменение интенсивности обработки 3-го канала							
0,2	0,2	0,2	0,2	0,25	0,25	0,25	0,25
0,2	0,2	0,2	0,3	0,27273	0,27273	0,27273	0,18182
0,2	0,2	0,2	0,4	0,28571	0,28571	0,28571	0,14286
0,2	0,2	0,2	0,5	0,29412	0,29412	0,29412	0,11765
0,2	0,2	0,2	0,6	0,3	0,3	0,3	0,1

Рассмотрим процесс функционирования АИС СН с двумя резервными каналами в условиях воздействия DDOS-атак, используя способ оценки риска возможного пребывания АИС СН в критическом состоянии и уточним некоторые ранее введенные параметры.

Степень сопротивляемости механизма защиты m_i, характеризующейся вероятностью его преодоления $(1\text{-}R_i)$ [6-8], будем рассчитывать, исходя из соотношения:

$$R_i = .\sum_{0}^{2} P_i = (1 - P_3). \tag{11}$$

В качестве вероятности появления угрозы:

$$L_i = \frac{\lambda}{\sqrt[3]{\prod_{i=0}^{2} \mu_i}}. \tag{12}$$

В данных условиях найдем значения выходных параметров по формулам (11, 12) и рассмотрим изменение значения параметра риска, с учетом изменения значений интенсивности обработки запасных каналов [9, 10], при фиксированном значении потока заявок для системы массового обслуживания с двумя резервными каналами. Результаты представлены в таблице № 4.

Таблица № 4

Выходные параметры АИС СН с 2 резервными каналами, при расчете с использованием предложенного способа

Интенсивность входящего потока	Интенсивность обработки			Z_1	L_1	R_1	$Risk_1$
	1–й канал	2–й канал	3–й канал				
1	2	3	4	5	6	7	8
Изменение интенсивности входящего потока							
0,2	0,2	0,2	0,2	0,25	1	0,75	0,0625
0,3	0,2	0,2	0,2	0,41538	1,5	0,58462	0,25882
0,4	0,2	0,2	0,2	0,53333	2	0,46667	0,56889
0,5	0,2	0,2	0,2	0,61576	2,5	0,38424	0,94791
1	2	3	4	5	6	7	8
0,6	0,2	0,2	0,2	0,675	3	0,325	1,36688
Изменение интенсивности обработки 1-го канала							
0,2	0,2	0,2	0,2	0,25	1	0,75	0,0625
0,2	0,3	0,2	0,2	0,22222	0,87358	0,77778	0,04314
0,2	0,4	0,2	0,2	0,2	0,7937	0,8	0,03175

1	2	3	4	5	6	7	8
0,2	0,5	0,2	0,2	0,18182	0,73681	0,81818	0,02436
0,2	0,6	0,2	0,2	0,16667	0,69336	0,83333	0,01926
Изменение интенсивности обработки 2-го канала							
0,2	0,2	0,2	0,2	0,25	1	0,75	0,0625
0,2	0,2	0,3	0,2	0,2	0,87358	0,8	0,03494
0,2	0,2	0,4	0,2	0,16667	0,7937	0,83333	0,02205
0,2	0,2	0,5	0,2	0,14286	0,73681	0,85714	0,01504
0,2	0,2	0,6	0,2	0,125	0,69336	0,875	0,01083
Изменение интенсивности обработки 3-го канала							
0,2	0,2	0,2	0,2	0,25	1	0,75	0,0625
0,2	0,2	0,2	0,3	0,18182	0,87358	0,81818	0,02888
0,2	0,2	0,2	0,4	0,14286	0,7937	0,85714	0,0162
0,2	0,2	0,2	0,5	0,11765	0,73681	0,88235	0,0102
0,2	0,2	0,2	0,6	0,1	0,69336	0,9	0,00693

Из таблиц 2 и 4 видно, что при изменении значений интенсивностей величина риска возможного пребывания АИС СН в критическом состоянии изменяется: при увеличении интенсивности DDOS-атаки и фиксированных значениях интенсивности обработки заявок каналами – растет; при фиксированном значении интенсивности входящего потока и увеличении значений интенсивностей обработки заявок каналами – убывает. Это указывает на адекватное реагирование предложенного способа на изменение расчетных параметров.

Использование предложенного способа оценки риска возможного пребывания АИС СН в критическом состоянии позволяет моделировать входящие в состав АИС СН средства защиты информации в условиях воздействия DDOS-атак, учитывая как эмпирические значения, полученные в результате измерений или моделирования, так и теоретическую базу параметров, конкретизированных входными данными с исключением экспертных знаний.

При синтезе двух моделей был устранен недостаток неопределенности части входных параметров, учитывающих значения, основанные на экспертных оценках.

Литература

1. Максименко В.Н., Ясюк Е.В. Основные подходы к анализу и оценке рисков информационной безопасности // Экономика и качество систем связи, 2017, №2. URL: cyberleninka.ru/article/n/osnovnye-podhody-k-analizu-i-otsenke-riskov-informatsionnoy-bezopasnosti

2. Королев И.Д., Петрова О.В., Овчаренко И.О. Модель системы защиты многоканальных автоматизированных комплексов от DDoS–атак с учетом освобождения по мере обработки каналов // Инженерный вестник Дона, 2019, № 7. URL: ivdon.ru/ru/magazine/archive/N7y2019/6080

3. Вентцель Е.С, Овчаров Л.А. Теория вероятностей. М.: Высшая школа, 2001. 575 с.

4. Королев И.Д., Петрова О.В., Овчаренко И.О. Моделирование системы защиты многоканальных автоматизированных комплексов // Вестник Российского нового университета, 2019. URL: vestnik-rosnou.ru/сложные-системы-модели-анализ-и-управление-complex-systems-models-analysis-management/2019/1/3

5. Королев И.Д., Петрова О.В., Крюков Д.М., Колесников В.Л. Способ оценки защищенности автоматизированной информационной системы специального назначения от DDoS-атак на основе теоретико-эмпирического подхода // Инженерный вестник Дона, 2021, №1. URL: ivdon.ru/ru/magazine/archive/n1y2021/6779

6. Суханов А.И. Оценки защищенности информационных систем // Журнал научных публикаций аспирантов и докторантов, 2008. URL: jurnal.org/articles/2008/inf33.html

7. Privault, N. Understanding Marcov Chains. Examples and Applications // Springer, 2018. 372 p.

8. Cobb, G.W. What is Markov Chain Monte Carlo and Why it Matters // CRC Press, 2021. 200 p.

9. Metcalfe, A., D. Green, T. Greenfield and M. Mansor. Statistics in Engineering // CRC Press, 2019. 792 p.

10. Xin-She Yang and Xing-Shi He. Mathematical Foundations of Nature Inspired Algorithms // Springer, 2019. 107 p.

References

1. Maksimenko V.N., Yasyuk E.V. Ekonomika i kachestvo sistem svyazi, 2017, №2. URL: cyberleninka.ru/article/n/osnovnye-podhody-k-analizu-i-otsenke-riskov-informatsionnoy-bezopasnosti

2. Korolev I.D., Petrova O.V., Ovcharenko I.O. Inzhenernyy vestnik Dona, 2019, № 7. URL: ivdon.ru/ru/magazine/archive/N7y2019/6080

3. Venttsel' E.S, Ovcharov L.A. Teoriya veroyatnostey [probability theory]. Moskow, 2001. 575 p.

4. Korolev I.D., Petrova O.V., Ovcharenko I.O. Vestnik Rossiyskogo novogo universiteta, 2019. URL: vestnik-rosnou.ru/slozhnye-sistemy-modeli-analiz-i-upravlenie-complex-systems-models-analysis-management/2019/1/3

5. Korolev I.D., Petrova O.V., Kryukov D.M., Kolesnikov V.L. Inzhenernyy vestnik Dona, 2021, №1. URL: ivdon.ru/ru/magazine/archive/n1y2021/6779

6. Sukhanov A.I. Zhurnal nauchnykh publikatsiy aspirantov i doktorantov, 2008. URL: jurnal.org/articles/2008/inf33.html

7. Privault, N. Understanding Marcov Chains. Examples and Applications. Springer, 2018. 372 p.

8. Cobb, G.W. What is Markov Chain Monte Carlo and why it Matters. CRC Press, 2021. 200 p.

9. Metcalfe, A., D. Green, T. Greenfield and M. Mansor. Statistics in Engineering. CRC Press, 2019. 792 p.

10. Xin-She Yang and Xing-Shi He. Mathematical Foundations of Nature Inspired Algorithms. Springer, 2019. 107 p.