УДК 519.832 DOI: 10.26102/2310-6018/2019.27.4.028

ПРАКТИЧЕСКИЕ АСПЕКТЫ ПРИМЕНЕНИЯ ТЕОРИИ ИГР К ОЦЕНКЕ БЕЗОПАСНОСТИ СИСТЕМЫ

Л.В. Степанов[1,2], А.С. Кольцов[1], А.В. Паринов[1], Д.В. Паринов[3], Б.А. Соловьев[3]
[1]ФКОУ ВО Воронежский институт ФСИН России, Воронеж, Россия
[2]ФГБОУ ВО Российский экономический университет им. Г.В. Плеханова, Воронежский филиал, Воронеж, Россия
[3]ФГАОУ ВО Российский университет транспорта, Москва, Россия
[1]e-mail: stepanovlv@yandex.ru

Резюме: В работе рассматривается практическое применение теоретико-игрового подхода в задаче оценки безопасности систем. Одним из факторов, определяющих жизнь и деятельность любой системы, является её безопасность. Понятие безопасности применимо к организационно-экономическим, инженерно-техническим, биологическим и любым другим видам систем. Состояние безопасности системы определяется множеством внешних и внутренних факторов. К числу внутренних факторов можно отнести уязвимости присущие данной системе, а к числу внешних - множество угроз, способных потенциально воздействовать на данную систему. Обстоятельство противоборства между угрозами с одной стороны, и уязвимостями (мероприятиями по устранению уязвимостей) с другой, делает обоснованным применение для оценки безопасности системы методов теории игр. Параметры угроз и уязвимостей наряду с количественным могут иметь качественное описание, что ограничивает возможность применения математических методов. По данной причине эти параметры необходимо формализовать в числовой вид. Для решения данной проблемы в работе предлагается использовать попарное сравнение лингвистических конструкций. Полученные формализованные значения можно использовать при построении матрицы игры.Особенностью предлагаемого в работе подхода является возможность его реализации в виде алгоритмического и программного обеспечения, которое позволит автоматизировать работу аналитиков ответственных за формирование тактики и стратегии обеспечения безопасности любого учреждения или организации. Это обстоятельство отражает практическую полезность предложенной методики.

Ключевые слова: система безопасности, угрозы безопасности, уязвимости системы, мероприятия по противодействию угрозам, линейное программирование, теория игр.

Для цитирования: Степанов Л.В., Кольцов А.С., Паринов А.В., Паринов Д.В., Соловьев Б.А. Практические аспекты применения теории игр к оценке безопасности системы. *Моделирование, оптимизация и информационные технологии.* 2019;7(4). Доступно по: https://moit.vivt.ru/wp-content/uploads/2019/11/StepanovSoavtori_4_19_1.pdf DOI: 10.26102/2310-6018/2019.27.4.028

PRACTICAL ASPECTS OF APPLICATION OF THEORY OF GAMES TO THE ASSESSMENT OF SYSTEM SECURITY

L.V. Stepanov[1,2], A.S. Koltsov[1], A.V. Parinov[1], D.V. Parinov[3], B.A. Soloviev[3]
[1]Voronezh Institute of the Federal Penitentiary Service of Russia, Voronezh, Russia
[2] Plekhanov Russian University of Economics, Voronezh, Russia
[3]Federal State Institution of Higher Education «Russian University of Transport» Russian Federation, Moscow

Abstract: The paper considers the practical application of the game-theoretic approach to the task of assessing the security of systems. One of the factors determining the life and activity of any system is

its safety. The concept of security is applicable to organizational, economic, engineering, biological and any other types of systems. The security status of the system is determined by many external and internal factors. Among the internal factors include the vulnerabilities inherent in this system, and among the external ones there are many threats that could potentially affect this system. The circumstance of the confrontation between threats on the one hand, and vulnerabilities (measures to eliminate vulnerabilities) on the other, makes it reasonable to use game theory methods to assess the security of a system.The parameters of threats and vulnerabilities, along with quantitative ones, can have a qualitative description, which limits the possibility of using mathematical methods. For this reason, these parameters must be formalized in a numerical form. To solve this problem, it is proposed to use a pairwise comparison of linguistic constructions. The obtained formalized values can be used to construct the game matrix.A feature of the approach proposed in the work is the possibility of its implementation in the form of algorithmic and software that will automate the work of analysts responsible for the formation of tactics and strategies for ensuring the security of any institution or organization. This fact reflects the practical usefulness of the proposed methodology.

Keywords: security system, security threats, system vulnerabilities, measures to counter threats, linear programming, game theory.

For citation: Stepanov L.V., Koltsov A.S., Parinov A.V., Parinov D.V., Soloviev B.A. Practical aspects of application of theory of games to the assessment of system security. *Modeling, Optimization and Information Technology*. 2019;7(4). Available from: https://moit.vivt.ru/wp-content/uploads/2019/11/StepanovSoavtori_4_19_1.pdf DOI: 10.26102/2310-6018/2019.27.4.028 (In Russ).

Введение

Угрозы и уязвимости находится в определенной взаимосвязи. Однако эту взаимную зависимость нельзя считать полностью определенной и четко формализовать [1]. Например, одним из видов угроз информационной безопасности инфокоммуникационной системы является вредоносное программное обеспечение. Эту угрозу можно рассматривать, как внешний фактор по отношению к информационным ресурсам и их источником в организации. С целью противодействия данному виду угроз в организации могут использоваться антивирусные программные продукты. Однако, их наличие полностью уязвимость от вредоносного программного обеспечения не устраняет хотя бы по причине того, что антивирусные базы обновляются после выявления вредоносных программ с определенной сигнатурой кода и остаётся определённое время для негативного воздействия на инфокоммуникационную систему. С другой стороны, использование каких-либо программных средств высокой эффективности противодействия в принципе не способно полностью ликвидировать угрозу вредоносного воздействия [1].

Ситуация существенно усложняет тем, что одна уязвимость системы может приводить к актуализации сразу нескольких видов угроз и наоборот. Например, угроза проникновения на территорию охраняемого объекта может зависеть от двух уязвимостей: надежности инженерных средств и конструкций, а также эффективности технических средств, которые применяются на охраняемом объекте. То есть одна угроза связана с двумя уязвимостями. С другой стороны, использование интегрированных систем безопасности в учреждении способно исключить или минимизировать риск проникновения злоумышленника на территорию охраняемого объекта, а также защитить информационные ресурсы в этом учреждении. Таким образом, одна уязвимость связана с двумя видами угроз [1].

Еще одним проблемным вопросом является то, что угрозы и уязвимости могут иметь параметры, многие из которых невозможно представить в количественной (числовой) форме. Подобная ситуация характерна не только для биологических или социально-экономических, но и инженерно-технических систем. Так в представленных

выше примерах состояние защищенности информационных ресурсов невозможно описать количественно. В этих условиях для описания параметров часто применяют качественную (нечисловую) форму [2, 3].

Все перечисленные обстоятельства делают обоснованным применение подходов, позволяющих учесть данную множественность и неопределенность.

Подход к формализации качественных характеристик системы «угроза-уязвимость»

Пусть H и A множества угроз и уязвимостей безопасности системы:

$$H = \{H_j\},\ j = \overline{1,m}\ ,\ A = \{A_i\},\ i = \overline{1,n} \tag{1}$$

где H_j – j-ая угроза безопасности; A_i – i-ая уязвимость системы.

Тогда H_j определим как:

$$H_j = \{h_j^y\},\ y = \overline{1, w_j}, \tag{2}$$

где h^y_j – y-я характеристика j-ой угрозы, то есть действие или событие способное понизить уровень безопасности системы; w_j – число характеристик j-ой угрозы.

Аналогично можно описать уязвимости системы:

$$A_i = \{a_i^z\},\ z = \overline{1, v_i}, \tag{3}$$

где v_i – число характеристик i-ой уязвимости.

Предположим, что характеристики всех угроз и уязвимостей имеют только качественное описание.

Для h^y может быть задана равномерная шкала, содержащая множество лингвистических конструкций L^y, описывающих h^y для рассматриваемого объекта безопасности:

$$L^y = \{l_b\}^y, b = \overline{1,r}, \tag{4}$$

где r – число лингвистических конструкций y-ой характеристик угрозы.

Предположим, что в качестве угрозы безопасности системы выступает вредоносное программное обеспечение, шкала описания для которого может быть составлена конструкциями: «очень опасное», «опасное», «мало опасное», «неопасное».

Для формализации лингвистических конструкций L^y нужно поставить в соответствие каждому l_b некоторую оценку:

$$SH = \{op : sh_u\}, u = \overline{1, dl}, \tag{5}$$

где dl – количество степеней предпочтительности.

При выборе соответствующей оценки необходимо учитывать равномерность шкалы. Сами весовые значения роли не играют. В зависимости от требований точности описания шкала значений может быть любой длины, достаточной для точного описания значений параметра.

Предположим, что степень предпочтительности может быть охарактеризована тремя значениями.

Таблица 1 - Шкала сравнения

Уровень *op*	Степень предпочтительности *sh*
Равнозначность	1
Превышение	3
Значительное превышение	5

Можно построить матрицу попарного сравнения используемых для описания лингвистических конструкций:

$$SR = \begin{vmatrix} sr_{11} & \dots & sr_{1b} & \dots sr_{1r} \\ \dots & \dots & \dots & \dots \dots \\ sr_{b1} & \dots & sr_{bb} & \dots sr_{br} \\ \dots & \dots & \dots & \dots\dots \\ sr_{r1} & \dots & sr_{rb} & \dots sr_{rr} \end{vmatrix}, \quad (6)$$

где

$$sr = \begin{cases} sh, l_b \succ l_{b'}, \\ \dfrac{1}{sh}, l_b \prec l_{b'}, \\ 1, l_b = l_{b'}. \end{cases} \quad (7)$$

В системе (7) символом «$\prec$» обозначается превосходство одной лингвистической конструкции над другой, используемой для описания значения параметра.

Для используемого примера матрица *SR* будет иметь вид, представленный в Таблице 2.

Таблица 2 - Матрица попарного сравнения

	очень опасное	*опасное*	*мало опасное*	*неопасное*
очень опасное	1	3	3	5
опасное	1/3	1	3	3
мало опасное	1/3	1/3	1	3
неопасное	1/5	1/3	1/3	1

Если бы шкала сравнения имела большую длину, то степени предпочтительности над и под диагональю можно было бы выразить точнее.

Для числовой формализации каждой лингвистической конструкции нужно определить сумму элементов строк матрицы *SR* и сумму $Sum_{общ}$ всех элементов этой матрицы и выполнить нормализацию:

$$Sum_b = \sum_{b'=1}^{r} sr_{bb'}, b = \overline{1, r}, \quad (8)$$

$$o_b = \frac{Sum_b}{Sum_{общ}}. \quad (9)$$

где *b* и *b'* – индексы строки и столбца соответственно матрицы *SR*.

Для примера угрозы со стороны вредоносного программного обеспечения и Таблицы 2 получим вектор нормализованных значений.

Таблица 3 - Нормализованные значения

очень опасное	*опасное*	*мало опасное*	*неопасное*
0,44	0,29	0,19	0,08

Рассмотренный подход необходимо применить ко всем качественным характеристикам из исходных множеств угроз и уязвимостей *H* и *A*. Важно отметить, что для отдельных угроз и уязвимостей и их характеристик могут быть заданы разные множества лингвистических конструкций и шкал степеней предпочтительности. При этом сама методика формализации изменений не претерпевает.

В случае наличия угроз и уязвимостей, характеристики которых имеют количественное выражение их значения необходимо нормализовать [2, 3].

Теоретико-игровой подход к оценке состояния безопасности системы

В силу того, что обеспечение безопасности любой системы связано с противодействием негативному влиянию на неё, для оценки уровня защищенности этой системы предлагается использовать теоретико-игровой подход. Явно выраженный антагонистический характер угроз по отношению к уязвимостям, а также описанная выше неоднозначность взаимосвязи между угрозами и уязвимостями являются основанием для выбора методов матричных игр [4, 5].

По причине основательной проработанности всех базовых положений теории игр и с учетом наличия большого количества практических примеров её применения для различных сфер практической деятельности человека рассмотрим прикладной аспект матричных игр на конкретном примере [2, 4, 5].

Сформулируем постановку задачи. Предположим, что в распоряжении злоумышленника имеется четыре программно-технических средства способных оказать негативное влияние на безопасность инфокоммуникационной система учреждения. В процессе анализа системы безопасности учреждения были выявлены три уязвимости этой системы. Каждое из программно-технических средств имеет следующий ряд параметров: стоимость, степень деструктивного действия и некоторый совокупный показатель, характеризующий трудоемкость применения злоумышленником программно-технического средства по отношению к учреждению. С позиции учреждения для ликвидации каждый уязвимости могут быть предприняты определенные мероприятия, которые также характеризуются параметрами: стоимость, эффективность противодействия и некоторый совокупный параметр, отражающий затратность реализация этих мероприятий для учреждения. Причём для ликвидации каждой отдельной уязвимости используется только одно определенное мероприятие. Необходимо оценить последствия реализации угроз безопасности инфокоммуникационной системы учреждения с учётом существующих уязвимостей и возможности реализации мероприятий по их устранению.

В сформулированной постановке задачи стоимостной показатель имеет количественное выражение, а другие параметры могут быть охарактеризованы только качественно.

Исходные данные для постановки задачи представлены в Табличной форме.

Таблица 3 - Параметры угроз безопасности системы

Угроза	Стоимость	Степень деструктивного действия	Трудоемкость применения злоумышленником
1	1500	средняя	высокая
2	2000	высокая	средняя
3	800	низкая	низкая

Таблица 4 - Параметры уязвимостей системы

Уязвимость/ Мероприятие	Стоимость	Эффективность противодействия	Затратность мероприятия
1	2500	средняя	высокая
2	1000	низкая	низкая
3	6000	высокая	средняя

В результате нормализация количественных значений и формализации качественных характеристик получим следующие результаты оценки угроз и уязвимостей.

Таблица 5 - Формализация параметров угроз безопасности

Угроза	Оценка стоимости	Оценка деструктивности	Оценка трудоемкости
1	0,35	0,31	0,58
2	0,47	0,58	0,31
3	0,19	0,11	0,11

Таблица 6 - Формализация параметров уязвимостей системы

Уязвимость/ Мероприятие	Оценка стоимости	Оценка эффективность противодействия	Оценка затрат на мероприятия
1	0,26	0,31	0,58
2	0,11	0,11	0,11
3	0,63	0,58	0,31

На следующем этапе возникает задача расчёта интегральной оценки каждой угрозы и уязвимости. Предположим, что каждый параметр имеет равную значимость, тогда совокупная оценка может определяться, как сумма значений её параметров. Однако в рассматриваемом примере для угроз безопасности значение параметра деструктивности должно вносить положительный, а стоимость и трудоемкость отрицательные вклад в интегральную оценку. Аналогичная ситуация связана с параметрами уязвимостей системы. С учётом данного обстоятельства могут быть рассчитаны следующие интегральные оценки.

Таблица 7 - Совокупная оценка угроз безопасности системы

Угроза	Совокупная оценка
1	-0,61
2	-0,20
3	-0,19

Таблица 8 - Совокупная оценка уязвимостей системы

Уязвимость/Мероприятие	Совокупная оценка
1	-0,53
2	-0,11
3	-0,37

С позиции теоретико-игрового подхода угрозы и уязвимости могут быть рассмотрены как стратегии взаимодействующих сторон. При этом, угрозы как стратегии злоумышленника, а уязвимости как стратегии системы безопасности учреждения.

Полученные совокупные оценки позволяют перейти к построению матрицы игрового взаимодействия.

Таблица 9 - Матричная игра

$A_i \setminus B_j$	B_1	B_2	…	B_m
A_1	a_{11}	a_{12}	…	a_{1m}
A_2	a_{21}	a_{21}	…	a_{2m}
…	…	…	…	…
A_n	a_{n1}	a_{n2}	…	a_{nm}

Способ определения значения элемента a_{ij} определяется для каждой задачи исходя из её постановки. Для рассматриваемого примера предлагается определять значение матрицы игры как разность между совокупными оценками уязвимостей и угроз соответственно.

Таблица 10 - Матрица игры

	Уязвимость/Мероприятие		
Угроза	-0,53	-0,11	-0,37
-0,61	0,09	0,51	0,25
-0,20	-0,33	0,10	-0,17
-0,19	-0,34	0,08	-0,18

С целью проверки возможности поиска решения матричной игры в чистых стратегиях необходимо применить минимаксный и максиминный подходы к строкам и столбцам матрица игры соответственно. Такой вариант обоснован тем, что учреждению целесообразно стремиться к выбору наилучшей стратегии из наихудших возможных, а злоумышленнику наоборот.

Таблица 11 - Поиск седловой точки

	Уязвимость/Мероприятие				
Угроза	-0,53	-0,11	-0,37		
-0,61	0,09	0,51	0,25	**0,51**	
-0,20	-0,33	0,10	-0,17	**0,10**	
-0,19	-0,34	***0,08***	-0,18	**0,08**	**0,08**
	-0,34	**0,08**	**-0,18**		
			0,08		

Для данной матрицы игры значение минимакса и максимина совпали, то есть игровое взаимодействие имеет седловую точку, которая является решением данной игры.

Обязательным этапом решения любых задач на основе применения теоретико-игрового подхода является интерпретация полученных результатов. Согласно теории игр отклонение злоумышленником от применения третьего вида программно-

технических средств будет вести к необоснованному возрастанию затрат на применение другого вида вредоносного воздействия. Для учреждения второй комплекс мероприятий по устранению уязвимостей также следует считать оптимальным. При отклонении учреждения от данной стратегии могут возрастать затраты на мероприятия по устранению уязвимостей или снижаться их эффективность по отношению к действиям злоумышленника. Положительное значение найденного решения, равное 0,08 показывает, что в совокупности параметры выбранного комплекса мероприятий по устранению уязвимостей системы безопасности учреждения превосходят совокупное значение параметров оптимальной угрозы. При этом, если рассмотреть весь интервал значений матрицы (от -0,33 до 0,51), то найденное значение лежит над границей «выгодно для учреждения/выгодно для злоумышленника» в области «выгодно для учреждения». Рассматриваемая матрица имеет более высокие значения, например, 0,51. Это значение соответствует второму комплексу мероприятий, но первому виду угроз и «выгодно» для учреждения, но «не выгодно» для злоумышленника. Выбор злоумышленником первой стратегии нельзя считать рациональным, так как этот комплекс вредоносных воздействий имеет более высокую стоимость и трудоемкость применения, что при средней деструктивности действия нельзя считать оправданным. Анализ и сравнение других вариантов также покажут нецелесообразность отклонения от найденной оптимальной стратегии для злоумышленника и для учреждения.

Кроме рассмотренного возможен второй вариант, при котором решение в чистых стратегиях отсутствует. В этой ситуации осуществляется поиск решения в смешанных стратегиях. Одним из способов нахождения решения является применение линейного программирования. Рассмотрим для примера следующую матрицу игры.

Таблица 12 – Пример матрицы игры

	Уязвимость/Мероприятие				Min	Max
Угроза	0,09	-0,33	-0,34	0,09	-0,34	**0,08**
	0,51	0,10	0,08	0,51	0,08	
	0,25	-0,17	0,09	0,25	-0,17	
	0,51	0,10	0,08	0,51	0,08	
Max	0,51	0,10	0,09	0,51		
Min	**0,09**					

В соответствии с принципом равенства минимакса и максимина седловая точка отсутствует, а решение должно находиться в диапазоне от 0,08 до 0,09.

Формализация задачи линейного программирования будет иметь вид:

$$x_1 + x_2 + x_3 + x_4 \to \min;$$

$$\begin{cases} 0,09x_1 + 0,51x_2 + 0,25x_3 + 0,51x_4 \geq 1; \\ -0,33x_1 + 0,10x_2 - 0,17x_3 + 0,10x_4 \geq 1; \\ -0,34x_1 + 0,08x_2 + 0,09x_3 + 0,08x_4 \geq 1; \\ 0,09x_1 + 0,51x_2 + 0,25x_3 + 0,51x_4 \geq 1; \end{cases} \quad (10)$$

$$x_1 \geq 0; \quad x_2 \geq 0; \quad x_3 \geq 0; \quad x_4 \geq 0.$$

$$y_1 + y_2 + y_3 + y_4 \to \max;$$
$$\begin{cases} 0,09y_1 - 0,33y_2 - 0,34y_3 + 0,09y_4 \le 1; \\ 0,51y_1 + 0,10y_2 + 0,08y_3 + 0,51y_4 \le 1; \\ 0,25y_1 - 0,17y_2 + 0,09y_3 + 0,25y_4 \le 1; \\ 0,51y_1 + 0,10y_2 + 0,08y_3 + 0,51y_4 \le 1; \end{cases} \quad (11)$$
$$y_1 \ge 0; \quad y_2 \ge 0; \quad y_3 \ge 0; \quad y_4 \ge 0.$$

Применив надстройку «Поиск решения» в Excel могут быть получены результаты, представленные на Рисунке 1.

Уязвимости/Мероприятия						***Угрозы***				
x1	x2	x3	x4	**F(x)**		y1	y2	y3	y4	**F(y)**
0	0,2346	0,6562	11,413	**12,3**		0	0,4129	11,891	0	**12,3**
0,09	0,51	0,25	0,51	6,0811		0,09	-0,33	-0,34	0,09	-4,196
-0,33	0,10	-0,17	0,10	1		0,51	0,10	0,08	0,51	1
-0,34	0,08	0,09	0,08	1		0,25	-0,17	0,09	0,25	1
0,09	0,51	0,25	0,51	6,0811		0,51	0,10	0,08	0,51	1
V	**p1**	**p2**	**p3**	**p4**		**V**	**p1**	**p2**	**p3**	**p4**
0,081	**0**	**0,019**	**0,053**	**0,928**		**0,081**	**0**	**0,034**	**0,966**	**0**

Рисунок 1 – Смешанные стратегии матричной игры

Решение игры *V* равно 0,081, что соответствует сделанному ранее предположению. Значение p1, p2, p3 и p4 соответствуют вероятностям выбора стратегии каждым из игроков. Наиболее вероятной является третья угроза, а наиболее эффективным четвёртое мероприятие по ликвидации уязвимостей. Решение в смешанных стратегиях позволяет определить комплекс мер противодействия сразу нескольким угрозам. Так, в рассматриваемом варианте задачи могут быть использованы совместно второе, третье и четвёртое мероприятие по устранению уязвимостей системы безопасности.

Заключение

В реальных условиях угрозы и уязвимости могут характеризоваться большим количеством параметров. Невзирая на то, что теория матричных игр не требует сложных и ресурсозатратных вычислений выполнить формализацию большого количества отдельных параметров может быть затруднительно. В этих условиях предлагается выполнить экспертную оценку каждой пары «угрозы-уязвимость» по аналогии с принципом формирования матрицы попарных сравнений рассмотренном выше. Для повышения точности сравнения может быть предложена школа большой длины и достаточное количество лингвистических конструкций способных учесть все необходимые аспекты сопоставление угроз и уязвимостей. Перед формированием такой матрицы необходимо определиться с какой точки зрения рассматривается взаимодействие в системе (с позиции злоумышленника или с позиции системы безопасности учреждения). С учетом этого должна быть охарактеризована каждая пара «угроза-уязвимость». Получив матрицу игры, можно воспользоваться рассмотренным

выше способом формализации лингвистических экспертных оценок, а затем осуществить поиск решения матричной игры в чистых или смешанных стратегиях.

ЛИТЕРАТУРА

1. Степанов Л.В., Десятов Д.Б., Кравченко А.С. Концепция обеспечения информационной безопасности телекоммуникационный сетей на основе искусственных иммунных систем. *Актуальные проблемы прикладной математики, информатики и механики: сборник трудов Международной научно-технической конференции*, Воронеж, 18–20 декабря 2017 г. Воронеж: «Научно-исследовательские публикации», 2017;:898-909.
2. Степанов Л.В., Десятов Д.Б., Сальникова А.Ю. *Аспекты применения теории игр к формализации систем. Актуальные проблемы деятельности подразделений УИС* Воронеж, 23 мая 2019 г. Воронеж: «Научная книга», 2019;:93-96
3. Степанов Л.В., Паринов А. В., Коротких Л.П. Формализация угроз информационной безопасности и комплексное оценивание эффективности защиты информации. *Вестник Воронежского института ФСИН России*. 2017;(4):156-162 (ВАК)
4. Дюбин Г.Н., Суздаль В.Г. *Введение в прикладную теорию игр.* Под ред. Н.Н. Воробьева -М.: Наука, 1981;:336.
5. Степанов Л.В. Теоретико-игровые модели выбора и принятия решений в задачах распределения ресурсов технологических систем: диссертация. канд. техн, наук. -В. 1998;:166.

REFERENCES

1. Stepanov L.V., Desyatov D.B., Kravchenko A.S. Kontseptsiya obespecheniya informatsionnoy bezopasnosti telekommunikatsionnyy setey na osnove iskusstvennykh immunnykh sistem. Aktual'nye problemy prikladnoy matematiki, informatiki i mekhaniki: sbornik trudov Mezhdunarodnoy nauchno-tekhnicheskoy konferentsii, Voronezh, 18–20 dekabrya 2017 g. Voronezh: «Nauchno-issledovatel'skie publikatsii», 2017;:898-909.
2. Stepanov L.V., Desyatov D.B., Sal'nikova A.Yu. Aspekty primeneniya teorii igr k formalizatsii sistem. Aktual'nye problemy deyatel'nosti podrazdeleniy UIS Voronezh, 23 maya 2019 g. Voronezh: «Nauchnaya kniga», 2019;:93-96
3. Stepanov L.V., Parinov A. V., Korotkikh L.P. Formalizatsiya ugroz informatsionnoy bezopasnosti i kompleksnoe otsenivanie effektivnosti zashchity informatsii. Vestnik Voronezhskogo instituta FSIN Rossii. 2017;(4):156-162 (VAK)
4. Dyubin G.N., Suzdal' V.G. Vvedenie v prikladnuyu teoriyu igr. Pod red. N.N. Vorob'eva - M.: Nauka, 1981;:336.
5. Stepanov L.V. Teoretiko-igrovye modeli vybora i prinyatiya resheniy v zadachakh raspredeleniya resursov tekhnologicheskikh sistem: dissertatsiya. kand. tekhn, nauk. -V. 1998;:166.

ИНОРМАЦИЯ ОБ АВТОРЕ / INFORMATION ABOUT THE AUTHOR

Степанов Леонид Викторович, профессор кафедры информационных технологий в экономике ФГБОУ ВО «Российский экономический университет имени Г.В. Плеханова» Воронежский филиал, доктор технических наук, доцент.

Leonid V. Stepanov, professor of the department of information technologies in the economy of Plekhanov Russian University of Economics, doctor of technical sciences, associate professor

Кольцов Андрей Сергеевич, профессор кафедры технических комплексов охраны и связи Воронежского института ФСИН России, канд. технических наук, доцент.

Andrey S. Koltsov, professor of the department technical complexes of safety and communication of the Voronezh institute of Russian Federal Penitentiary Service, candidate of technical sciences, associate professor

Паринов Андрей Владимирович, начальник кафедры технических комплексов охраны и связи Воронежского института ФСИН России, канд. технических наук, доцент

Andrey V. Parinov, head of chair technical complexes of safety and communication of the Voronezh institute of Russian Federal Penitentiary Service, candidate of technical sciences, associate professor

Соловьев Богдан Анатольевич, доцент Федерального государственного автономного образовательного учреждения высшего образования "Российский университет транспорта", к.э.н., доцент.

Bogdan A. Solovyov, associate professor Federal State Institution of Higher Education «Russian University of Transport», candidate of economic sciences, associate professor

Паринов Денис Владимирович, доцент Федерального государственного автономного образовательного учреждения высшего образования "Российский университет транспорта" к.э.н., доцент

Denis V. Parinov, associate professor Federal State Institution of Higher Education «Russian University of Transport», candidate of economic sciences, associate professor